One Identity Manager and Epic Integration 9.1.2

Administration Guide for Connecting to Epic Target System

Copyright 2025 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

Refer to our 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.

EPC Module Administration Guide for Connecting to Epic Target System
Updated - 11 January 2025, 02:35
Version - 9.1.2

Contents

Managing an Epic health care system ... **1**
Architecture overview ... 1
One Identity Manager users for managing an Epic health care system ... 2
Setting up synchronization with an Epic health care system ... **4**
Setting up the synchronization server ... 5
Creating a synchronization project for initial synchronization of an Epic health care system ... 8
Displaying synchronization results ... 16
Customizing synchronization configuration ... 17
Updating Schemas ... 17
Post-processing outstanding objects ... 18
Help for the analysis of synchronization issues ... 21
Deactivating synchronization ... 21
Basic Data for managing an Epic health care system ... **23**
Account definition for Epic User Account ... 24
Creating Account Definitions - Master data for an Account Definition ... 25
Creating manage level - Master data for manage level ... 27
Master data for a manage level ... 28
Creating mapping rules for IT operating data ... 29
Entering IT operating data ... 31
Modifying IT operating data ... 32
Assigning account definition to employees ... 33
Assigning account definitions to departments, cost centers, and locations ... 34
Assigning an account definition to business roles ... 34
Assigning account definitions to all employees ... 35
Assigning account definitions directly to employees ... 35
Assigning account definitions to system roles ... 36
Adding account definitions in the IT Shop ... 36
Assigning account definitions to a target system ... 38
Deleting an account definition ... 38
Password policies for Epic User Account ... 40
Predefined password policies ... 41
Applying password policies ... 42
Editing password policies ... 43
General master data for a password policy ... 44

Policy settings 44
Character classes for passwords on page 45
Custom scripts for password requirements 46
Script for checking a password on page 47
Script for generating a password 48
Excluded list for passwords 49
Checking Passwords 49
Initial password for Epic User Account 50
Email notification about login data 50
Target system managers 51
Editing a server 54
Master data for jobserver 54
Specifying server functions 56
Epic EMP template 58
Editing EMP template 59
Assigning the EMP template to Epic User 59
Assigning EMP template directly to the Epic User 60
Assigning EMP template to the department, cost center, and locations 60
Assigning EMP template to the business roles 61
Assigning EMP template to the IT shop 62
Deleting EMP template 62
Epic SubTemplate 64
Editing the Sub template 65
Assigning the Sub template to Epic User 65
Assigning the Sub template directly to the Epic User 66
Assigning SubTemplate to the department, cost center, and locations 66
Assigning Sub template to the business roles 67
Assigning SubTemplate to IT shop 68
Deleting the Sub template 69
Epic Connection 70
General Master Data for Epic Connection 70
Assign Epic EMPTemplate Matrix Property Mapping 71
Define Search criteria for Employee assignment 71
View Epic Security Matrix for EMPTemplate 72
Assign Epic SubTemplate Matrix Property Mapping 72
View Epic Security Matrix for SubTemplate 72
Configure settings for SubTemplate Index 73
Epic EMP User Accounts 74

Linking user account to employees ... 78
Editing master data for user account ... 78
General master data for Epic User Account ... 79
Demographic data for Epic User Account ... 82
Password data for Epic User Account ... 83
Template data for Epic User Account ... 84
Additional tasks for managing Epic User Account ... 85
Overview of Epic User Account ... 85
Managing IdentityIDs for Epic User Account ... 85
Managing External Identifiers for Epic User Account ... 86
Managing Epic User Account Managers ... 86
Managing Demographics for Epic User Account ... 87
Automatic assignments of persons to Emp user accounts ... 87
Editing search criteria for automatic employee assignment ... 89
Disabling Epic User Account ... 91
Deleting and restoring Epic EMP user accounts ... 93
Setting External User ID on Epic EMP user creation ... 93

Security Matrix ... 94
Security Matrix for EMP template ... 94
Configuring SecurityMatrix for EMPTemplate ... 94
Importing SecurityMatrix for EMPTemplate ... 95
Importing the matrix using CSV import Synchronization Project ... 95
Importing the matrix directly into One Identity Manager Table ... 97
Viewing the EMPTemplate Security Matrix ... 97
Assignment of the EMPTemplate to Epic user accounts ... 97
Security Matrix for SubTemplate ... 98
Configuring SecurityMatrix for SubTemplate ... 98
Importing SecurityMatrix for SubTemplate ... 98
Importing the matrix using CSV import Synchronization Project ... 99
Importing the matrix directly into One Identity Manager Table ... 100
Viewing the SubTemplate Security Matrix ... 101
Assignment of the SubTemplate to Epic user accounts ... 101
Customizing Security Matrix ... 101

Appendix: Configuration parameters for managing Epic health care system ... 103

Appendix: Default project template for Epic ... 106

About us ... 107
Contacting us ... 107

Technical support resources 107

Managing an Epic health care system

One Identity Manager Epic health care system module provides the ability to connect to Epic health care systems and help manage the health care system identities and their access policies from One Identity Manager. Identity and Access Governance processes such as attesting, Identity Audit, user account management and system entitlements, IT Shop, or report subscriptions can be used for Epic health care systems. The integration provides a one stop shop for managing Epic health care identities, their access policies and ensures a strong identity governance.

One Identity Manager provides company employees with the necessary user accounts. You can use different mechanisms to connect employees to their user accounts. You can also manage user accounts independently of employees.

Architecture overview

To access Epic health care system data, the Epic health care system connector is installed on a synchronization server. The synchronization server ensures that the data is compared between the One Identity Manager database and Epic health care system. The Epic health care system connector uses the Epic web services for accessing Epic health care system data.

At a high level, the Epic health care module provides the following two features leveraging the Epic web services

- **Provisioning**: Provision Epic EMP user accounts along with their entitlements (EMPTemplate and SubTemplate) created in One Identity Manager on to the target Epic health care system.
- **Synchronization**: Synchronize Epic EMP user accounts along with their entitlements including Epic EMPTemplates and SubTemplates into One Identity Manager.

One Identity Manager users for managing an Epic health care system

The following users are used in Epic health care system administration.

Table 1: Users used in Epic health care system administration

Users	Task
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role • Administrate application roles for individual target systems types • Specify the target system manager • Set up other application roles for target system managers if required • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators • Do not assume any administrative tasks within the target system
Target system managers	Target system managers must be assigned to **Target systems | Epic** or a sub-application role. Users with this application role • Assume administrative tasks for the target system • Create, change or delete target system objects, like user accounts • Edit password policies for the target system • Prepare EMPTemplate and SubTemplate for adding to the IT Shop • 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	• Create customized permissions groups for application roles for role-based login to administration tools in **Designer** as required • Create system users and permissions groups for nonrole-based login to administration tools in **Designer** as required • Enable or disable additional configuration parameters in **Designer** as required • Create custom processes in **Designer** as required • Create and configures schedules as required • Create and configure password policies as required
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role • Assign to IT Shop structures
Product owner for the IT Shop	Product owners must be assigned to the **Request & Fulfillment | IT Shop | Product owner** application role or a child application role. Users with this application role • Approve through requests • Edit service items and service categories under their management
Administrators for Organizations	Administrators must be assigned to the application role **Identity Management | Organizations | Administrators**. Users with this application role • Assign to departments, cost centers and locations
Business roles administrators	Administrators must be assigned to the application role **Identity Management | Business roles | Administrators**. Users with this application role • Assign to business roles

2

Setting up synchronization with an Epic health care system

Epic health care system prerequisites

The following are the Epic health care system prerequisites

Epic version supported: May 2019, August 2020, May 2020, February 2020, November 2020, Feb 2021, May 2021, August 2021.

> NOTE: Prior Epic versions should also be supported but not officially tested against those versions.

Epic web services: Epic's SOAP 1.1 version of web services should be enabled and accessible. Epic system's Personnel management and demographics (user) web services should be enabled for access

Epic web services credentials: Valid credentials that has access to the Epic web services

Client ID: Valid Epic Client ID that has access to the Epic's personnel management and demographics (user) web services. One Identity's Production and Non-Production Epic Client IDs can be used if they are enabled for accessing the Epic web services. One Identity's Epic Client IDs can be found in the **EPCEpicConfig.xml** file in One Identity Manager workstation.

EMP User, EMPTemplate and SubTemplate reports: The master list of all EMP users, EMPTemplates and SubTemplates need to be exported from Epic in to separate CSV files and provided to Epic connector. Please contact Epic on how to automate the report generation process.

Epic EMP Items need to be un-locked: Epic EMP user attributes that need to be managed from One Identity Manager need to be un-locked by Epic's Data Courier team. The list of attributes along with the EMP item number are provided in the section Epic EMP User Accounts. Un-lock the EMP user items that you want serviced from One Identity Manager.

For more information about report format, see

- Epic EMP template
- Epic SubTemplate
- Epic EMP User Accounts

To load One Epic EMP users, EMPTemplates and SubTemplates into the One Identity Manager database for the first time

1. Make sure Epic health care system prerequisites are met
2. The **One Identity Manager** components for managing Epic health care system are available if the **TargetSystem | Epic configuration parameter** is set.
   - Check whether the configuration parameter is set in the **Designer**. Otherwise, set the configuration parameter and compile the database.
   - Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as Job server in **One Identity Manager**.

   NOTE: Ensure that the Job server has the machine role of Epic and job server function of Epic connector.
4. Create a synchronization project with the **Synchronization Editor**.

For more information, see

- Setting up the synchronization server
- Creating a synchronization project for initial synchronization of an Epic health care system
- Deactivating synchronization
- Customizing synchronization configuration
- Configuration parameters for managing Epic health care system
- Default project template for Epic

Setting up the synchronization server

To set up synchronization with an Epic health care system, a server must be available with the following software installed on it

- Windows operating system

  Versions supported

  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
  - Microsoft .NET Framework Version 4.8 or later

- Windows PowerShell version 5.0 or later

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

- **One Identity Manager Service**, **Epic** connector
- Install **One Identity Manager** components with the installation wizard.
  1. Select installation modules with existing database.
  2. Select the machine role **Server | Job server | Epic**.

All **One Identity Manager Service** actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

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

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

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

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

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

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

1. Start the program **Server Installer** on your administrative workstation.
2. Enter the valid connection credentials for the **One Identity Manager** database on the **Database connection** page.
3. Specify the server on which you want to install **One Identity Manager Service** on the **Server properties** page.

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

- OR -

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

Enter the following data for the Job server.

Table 2: Job Server Properties

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

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

4. Select **Epic** on the **Machine roles** page.
5. Select **Epic** connector on the **Server functions** page.
6. Check the **One Identity Manager Service** configuration on the **Service settings** page.

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

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

    NOTE: This page is only displayed when the database is encrypted.

11. Enter the service's installation data on the Service access page.

Table 3: Installation Data

Data	Description
Computer	Server on which to install and start the service from. ***To select a server***

	Enter a name for the server. - OR - Select a entry from the list.
Service Account	User account data for the **One Identity Manager Service**. ***To enter a user account for the One Identity Manager Service*** Set the option Local system account. This starts the **One Identity Manager Service** under the **NT AUTHORITY\SYSTEM** account. - OR - Enter user account, password and password confirmation.
Installation account	Data for the administrative user account to install the service. ***To enter an administrative user account for installation*** Enable Advanced. | Enable Current user. This uses the user account of the current user. - OR - Enter user account, password and password confirmation.

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

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

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

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

Creating a synchronization project for initial synchronization of an Epic health care system

Use **Synchronization Editor** to configure synchronization between the **One Identity Manager** database and Epic health care system. The following describes the steps for initial configuration of a synchronization project. 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.

The following information is required for setting up a synchronization project.

Table 4: Information Required for Setting up a Synchronization Project

Data	Explanation
Client Name	Client name who is using Epic
Environment Name	Epic instance's environment being connected to. Example: TEST, PROD
Connection display	Provide a display name for the Epic connection
Client ID	Valid Epic Client ID for authenticating against the Epic web services. For more information, see Epic health care system prerequisites for using One Identity Client ID. NOTE: Production Client ID must be used to connect to Epic's Production environment and Non-Production Client ID must be used to connect to Epic's Non-Production environments
Username	User that has access to the Epic web services • If the username is an EMP user account, then prefix the username with **emp:** Example: If username is webServiceAccount, then enter the username as emp:webServiceAccount • If the username is an Active directory user account then prefix the username with **windows:** Example: If username is webServiceAccount, then enter the username as windows:webServiceAccount
Password	Password of the user who has access to the Epic web services
Audit user id	Epic EMP user id that should be used for auditing the web service calls being made. The user needs to be active. IMPORTANT:The EMP user id supplied should be the External ID of the user. NOTE:It is highly recommended that an exclusive Epic EMP service account is created and used as the Audit user id
Audit user password	Audit user password needs to be supplied only on Epic versions prior to Epic 2018
Personnel Management Webservice URL	Epic's Personnel management web services URL. NOTE: Only one connection is allowed to a particular Epic environment. So the Personnel Management

	Webservice URL needs to be unique across synchronization projects.
Demographic (User) Webservice URL	Epic's demographics (User) web services URL NOTE: Only one connection is allowed to a particular Epic environment. So the Demographics (User) Webservice URL needs to be unique across synchronization projects.
CSV import directory	The directory from which the Epic EMP User, EMPTemplate and SubTemplate CSV reports should be fetched. This directory can be local folder or a network share. IMPORTANT: Important If local folder is used, make sure to set up the local folder on the synchronization server and One Identity Manager workstation. If network shared path is used provide the UNC path to the network share.
CSV import directory Credential	If the CSV import directory is a network share click this check box to optionally enter the credentials. NOTE: Not applicable for a local folder.
UserName	If the CSV import directory is a network share optionally enter the username to access the network share. Enter the username in the following format `Domain Name\Username`.
Password	If the CSV import directory is a network share optionally enter the password to access the network share.
IsNativeEpicAuthentication	Click this checkbox if the Epic environment is configured to use native Epic authentication. This value determines whether the Epic EMP user account password changes are propagated to the target system or not. Password updates to Epic EMP user accounts take place only if native Epic authentication is configured.
Use Custom PowerShell Script for User Import	If the Epic EMP user report generated out of Epic needs to be customized even further before it is used by the Epic connector check this check box. Copy the *EpicUserReportFilterScript.ps1* from the One Identity Manager installer's dvd/Addon folder to the CSV import directory. Customize the PowerShell script according to the requirements. Now, the Epic connector would use the data returned by the PowerShell script rather than the EMP user report CSV file. IMPORTANT: If local folder is used, make sure to copy the PowerShell script to the job server's local folder and One Identity Manager workstation's local folder. If the

	PowerShell script execution policy on job server or One Identity Manager workstation is set to AllSigned, then the PowerShell script has to be signed after modification or change the script execution policy on the server to be less restrictive for the script to run.
Synchronization server for Epic health care system	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 Epic connector must be installed on the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server. **Property Value** Server function Epic connector Machine role Server | Job server | Additional properties for the Job server. For more information, see Setting up the synchronization server.
One Identity Manager database connection data	Database server • Database • SQL Server Login and password Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	To configure synchronization with a target system, **One Identity Manager** must load the data from the target system. **One Identity Manager** communicates directly with target system to do this. Sometimes direct access from the workstation on which the **Synchronization Editor** is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection. The remote connection server and the workstation must be in the same **Active Directory** domain.

Remote connection server configuration

- One Identity Manager Service is started
- RemoteConnectPlugin is installed
- Epic connector is installed

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

> NOTE: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the RemoteConnectPlugin as well. For more information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide.*

> NOTE: The following sequence describes how you configure a synchronization project if **Synchronization Editor** is both
>
> - Run in default mode, and
> - Started from the launchpad
>
> If you run the project wizard in expert mode or directly from **Synchronization Editor**, additional configuration settings can be made. Follow the project wizard instructions through these steps.

To set up an initial synchronization project for Epic health care system

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

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

2. Select **Target system type Epic** and click **Start**.

   This starts the Synchronization Editor's project wizard.

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

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

4. Enter the system connection details for your client.
5. Enter the advance settings details if the option has been chosen.

6. 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.

7. 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.
8. On the Restrict target system access page, you specify how system access should work. You have the following options

   Table 5: Specify target system access

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

9. Select the synchronization server to run synchronization on the **Synchronization** server page.

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

a. Click to add a new Job server.

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

c. Click **OK**.

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

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

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

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

The synchronization project is created, saved and enabled immediately.

> NOTE:
>
> - If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the **Synchronization Editor**.
> - The connection data for the target system is saved in a variable set and can be modified under **Configuration | Variables** in **Synchronization Editor**.

Configure the created initial synchronization project for Epic health care system

Configure the following variables of the synchronization project

1. **Locale**: The locale that is used in Epic. Date time values are formatted based on the locale. Contact your Epic administrator to get the locale. Default locale is **en-US**.
2. **EpicVersion**: Epic deployment version should be entered in "Month Year" format. For example, to indicate Epic version May 2020, enter as May 2020. This variable would be used for futuristic version specific implementation for any API upgrades.
3. **LinkedProviderIDType**: Epic EMP-SER Link Provider ID Type that the customer would like to use. Once synchronization has been run after configuring the ID Type it should not be changed to avoid data inconsistency or potential data loss.

Configure the following fields under the Mappings section of the synchronization project

1. **User Mappings**
   a. **vrtDateFormat**: Configure the date format that you want to use based on the locale. If the locale is en-US, the configuration is already done and you need not to do anything more.
2. **UserHasEMPTemplate Mappings**
   a. **vrtDateFormat**: Configure the date format that you want to use based on the locale. If the locale is en-US, the configuration is already done and you need not to do anything more.

To configure the content of the synchronization log

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

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

To synchronize on a regular basis

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

To start initial synchronization manually

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

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

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

To select user accounts through account definitions

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

3. Assign the account definition and manage level to user accounts in linked status.
    a. In **One Identity Manager**, select **Epic Healthcare | User accounts | Linked but not configured | <Client>**.
    b. Select **Assign account definition to linked accounts**.

Related Topics

- Setting up the synchronization server
- Displaying synchronization results
- Customizing synchronization configuration
- Configuration parameters for managing Epic health care system
- Default project template for Epic

Displaying synchronization results

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

To display a synchronization log

1. Open the synchronization project in the **Synchronization Editor**.
2. Select **Logs**.
3. Click in the navigation view toolbar.

   Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking on it.

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

To display a provisioning log

1. Open the synchronization project in the **Synchronization Editor**.
2. Select **Logs**.
3. Click in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking on it. An analysis of the provisioning is show as a report. You can save the report.
5. The log is marked in color in the navigation view.

   This mark shows you the execution status of the synchronization/provisioning.
6. Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In **Designer**, enable the **DPR | Journal | LifeTime** configuration parameter and

enter the maximum retention period.

Customizing synchronization configuration

You have used the **Synchronization Editor** to set up a synchronization project for synchronization of an Epic health care system. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Epic health care system. You can customize the synchronization as required by updating the synchronization project's workflow, mappings, variables and start up configurations

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

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

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

Updating Schemas

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

To include schema data that have been deleted through compressing and schema modifications in the synchronization project, update each schema in the synchronization project.

This may be necessary if

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

To update a system connection schema

1. Open the synchronization project in the **Synchronization Editor**.
2. Select the category **Configuration | Target systems**.

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

   The **Mapping Editor** is displayed.

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

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

Post-processing outstanding objects

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

Outstanding objects

- Cannot be edited in **One Identity Manager**
- Are ignored by subsequent synchronization

- Are ignored by inheritance calculations

This means, all memberships and assignments remain intact until the outstanding objects have been processed. Start target system synchronization to do this.

To post-process outstanding objects

1. In **One Identity Manager**, select the **Epic health care | Target system synchronization: Epic** category.

   All tables assigned to the target system type Epic as synchronization tables are displayed in the navigation view.

   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 in the target system.

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

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

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

   NOTE:

   To display object properties of an outstanding object

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

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

3. Click one of the following icons in the form toolbar to run the respective method.

Table 6: Methods for handling outstanding objects

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

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

NOTE:

- By default, the selected objects are processed in parallel, which speeds up execution of the selected method. If an error occurs during processing, the action is stopped and all changes are discarded.
- Bulk processing of objects must be disabled if errors are to be localized, which means the objects are processed sequentially. Failed objects are named in the error message. All changes that were made up until the error occurred are saved.

To disable bulk processing

- Deactivate in the form toolbar.

  You must customize synchronization to synchronize custom tables.

To add custom tables to the target system synchronization

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

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

Help for the analysis of synchronization issues

You can generate a report for analyzing problems which occur during synchronization, for example, insufficient performance.

The report contains information such as

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

To generate a synchronization analysis report

1. Open the synchronization project in the **Synchronization Editor**.
2. Select the menu **Help | Generate** synchronization analysis report and answer the security prompt with **Yes**.

   The report may take a few minutes to generate. It is displayed in a separate window.
3. Print the report or save it in one of the available output formats.

Deactivating synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited 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. Open the synchronization project in the **Synchronization Editor**.
2. Select **General** on the start page.
3. Click **Deactivate project**.

Related Topics

- Creating a synchronization project for initial synchronization of an Epic health care system

3

Basic Data for managing an Epic health care system

To manage an Epic health care system environment in One Identity Manager, the following basic data is relevant.

Configuration parameters

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements. Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. You can find an overview of all configuration parameters in Base data | General | Configuration parameters in Designer.

For more information, see Configuration parameters for managing Epic health care system.

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 Account definition for Epic User Account.

Password policies

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

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

For more information, see Password policies for Epic User Account.

Initial password for new user accounts

You have the different options for issuing an initial password for user accounts. The central password of the assigned employee can be aligned with the user account password, a predefined, fixed password can be used, or a randomly generated initial password can be issued.

For more information, see Initial password for new Epic user accounts.

Email notifications about login data

When a new user account is created, the login data are sent to a specified recipient. In this case, two messages are sent with the username and the initial password. Mail templates are used to generate the messages. For more information, see Email notifications about login data.

Target system types

Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types. For more information, see Post-processing outstanding objects.

Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign the employees who are authorized to edit all tenants in One Identity Manager to this application role. Define additional application roles if you want to limit the edit permissions for target system managers to individual tenants. The application roles must be added under the default application role. For more information, see Target system managers.

Server

Servers must know your server functionality in order to handle Epic specific processes in One Identity Manager. For example, the synchronization server.

For more information, see Editing a server.

Account definition for Epic User Account

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

The data for the user accounts in the respective target system comes from the basic employee data. The employees must have a central user account. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role

(template processing). Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required. For detailed information about account definitions, see the One Identity Manager Target System Base Module Administration Guide.

The following steps are required to implement an account definition

- Creating account definitions
- Creating manage levels
- Creating mapping rules for IT operating data
- Entering IT operating data
- Assigning account definitions to employees
- Assigning account definitions to a target system

Creating Account Definitions - Master data for an Account Definition

To create a new account definition

1. In **One Identity Manager**, select **Epic healthcare | Basic configuration data | Account definitions | Account definition**s.

2. Select an account definition in the result list. Select Change master data.

- OR -

Click in the result list toolbar.

3. Enter the account definition's master data.

4. Save the changes

For more information, see Master data for an account definition.

Table 7: Master data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Required account definitions. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it.

Description	Spare text box for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the configuration parameter QER | CalculateRiskIndex is activated. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide.*
Service item	Service item Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can also be assigned directly to employees and roles outside of IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: The account definition assignment remains in effect. The user account stays the same. Option not set: The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment on deferred deletion of employees. Option set: The account definition assignment remains in effect. The user account stays the same. Option not set: The account definition assignment is not in effect. The associated user account is deleted.

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 stays the same. Option not set: The account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company specific information. Use Designer to customize display names, formats and templates for the input fields

Creating manage level - Master data for manage level

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 later, the changes are passed onto the user account.

> NOTE: The Full managed and Unmanaged are analyzed in templates. 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 later, the user accounts are also reactivated.

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

To assign manage levels to an account definition

1. In **One Identity Manager**, select **Epic healthcare | Basic configuration data | Account definitions | Account definitions**.

2. Select an account definition in the result list.

3. Select **Assign manage level**.

4. Assign the manage levels in **Add assignments**.

- OR -

Delete the manage levels in **Remove assignments.**

5. Save the changes.

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

To edit a manage level

1. Select **Epic healthcare | Basic configuration data | Account definitions | Manage levels**.

2. Select the manage level in the result list. Select Change master data.

- OR -

Click in the result list toolbar.

3. Edit the manage level's master data.

4. Save the changes.

Related Topics

- Master data for a manage level

Master data for a manage level

Enter the following data for a manage level.

Table 8: Master data for a manage level

Manage level	Name of the manage level.
Description	Spare text box for additional explanation.

IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • Never: Data is not updated. • Always: Data is always updated. • Only initially: The data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion are locked.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether locked user accounts retain their group memberships.

Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the employee's primary roles. The following IT operating data is used in the One Identity Manager default configuration for automatic creating and modifying of user accounts for an employee in the target system.

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

the target system.

- EMPTemplate can be inherited
- SubTemplate can be inherited
- Privileged user account

To create a mapping rule for IT operating data

1. In **One Identity Manager**, select **Epic healthcare | Basic configuration data | Account definitions | Account definitions**.

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

Table 9: Create a mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see 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: Only use the primary business role if the Business Roles Module is installed • Empty If you select a role, you must specify a default value and set the option **Always use default value**.
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The Employee - new user account with default properties created mail template is used. To change the mail template, adjust the TargetSystem | EPC | Accounts | MailTemplateDefaultValues configuration parameter.

3. Save the changes.

Related Topics

- Entering IT operating data

Entering IT operating data

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

Example

Normally, each employee in department A obtains a default user account in the connection A. In addition, certain employees in department A obtain administrative user accounts in the connection A. Create an account definition A for the default user account of the connection A and an account definition B for the administrative user account of connection A. Specify the "Department" property in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data. Specify the effective IT operating data of department A for the connection A. This IT operating data is used for standard user accounts. In addition, specify the effective account definition B IT operating data for department A. This IT operating data is used for administrative user accounts.

To define IT operating data

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

Table 10: IT operating data

Property	Description
Effects on	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 for an account definition. c. Select the specific target system or account definition under Effects on.

	d. Click OK.
Column	User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information, see the *One Identity Manager Target System Base Module Administration Guide*.
Value	Concrete value which is assigned to the user account property

4. Save the changes.

Related topics

- Creating mapping rules for IT operating data
- Modifying IT operating data

Modifying 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 business role or to a primary location changes, the templates are automatically run.

To run the template

1. In **One Identity Manager**, select the **Epic healthcare | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Execute templates** task.

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

Old value: Current value of the object property.

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

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

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

5. Click **Apply**.

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

Assigning account definition to employees

Account definitions are assigned to company employees. Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations, or roles. The employees are categorized into these departments, cost centers, locations, or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees. You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop. In the One Identity Manager default installation, the processes are checked at the start to see if the employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

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

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).

NOTE: As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the assignment of an account definition is removed, the user account that was created from this account definition is deleted. For detailed information about preparing role classes to be assigned, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations
- Assigning an account definition to business roles
- Assigning account definitions to all employees
- Assigning account definitions directly to employees
- Assigning account definitions to system roles
- Assigning account definitions to a target system

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

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

NOTE: In **Remove assignments**, you can remove the assignment of organizations. To remove an assignment, select the organization and double-click .

5. Save the changes.

Assigning an account definition to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In **One Identity Manager**, select the **Epic healthcare | 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. Assign business roles in **Add assignments**.

NOTE: In **Remove assignments**, you can remove the assignment of business roles. To remove an assignment, select the business role and double-click .

5. Save the changes.

Assigning account definitions to all employees

To assign an account definition to all employees

1. In **One Identity Manager**, select the **Epic healthcare| Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, enable the Automatic assignment to employees option.

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

5. Save the changes.

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

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

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In **One Identity Manager**, select the **Epic healthcare| 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. Assign employees in **Add assignments**.

> NOTE: In **Remove assignments**, you can remove the assignment of employees. To remove an assignment, select the employee and double-click .

5. Save the changes.

Assigning account definitions to system roles

Installed modules: System Roles Module

NOTE: Account definitions with 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 **One Identity Manager**, select the **Epic healthcare| 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. Assign system roles in **Add assignments**.

NOTE: In Remove assignments, you can remove the assignment of system roles. To remove an assignment, select the system role and double-click .

5. Save the changes

Adding account definitions in the IT Shop

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

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

NOTE: 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

1. In **One Identity Manager**, select the **Epic healthcare| Basic configuration data | Account definitions | Account definitions (non role-based login)** category.

- OR -

In **One Identity Manager**, select the **Entitlements | Account definitions (role-based login)** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. Assign the account definitions to the IT Shop shelves in **Add assignments**.

5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. In **One Identity Manager**,, select the **Epic healthcare| Basic configuration data | Account definitions | Account definitions (non role-based login)** category.

- OR -

In **One Identity Manager**, select the **Entitlements | Account definitions (role-based login)** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. Remove the account definitions from the IT Shop shelves in **Remove assignments**.

5. Save the changes.

To remove an account definition from all IT Shop shelves

1. In **One Identity Manager**, select the **Epic healthcare | Basic configuration data | Account definitions | Account definitions (non role-based login)** category.

- OR -

In **One Identity Manager**, select the **Entitlements | Account definitions (role-based login)** 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 One Identity Manager Service. All requests and assignment requests with this account definition are canceled in the process.

Related topics

- Master data for an account definition
- Assigning account definitions directly to employees
- Assigning account definitions to a target system
- Assigning account definitions to all employees
- Assigning account definitions to departments, cost centers, and locations
- Assigning account definitions to system roles
- Assigning an account definition to business roles

Assigning account definitions to a target system

The following prerequisites must be fulfilled if you implement automatic assignment of user accounts and employees resulting in administered user accounts.

• 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. This is the case on initial synchronization, for example.

To assign the account definition to a target system

1. In **One Identity Manager**, select the connection in the **Epic healthcare | Connections**.

2. Select the **Change master data** task.

3. Select the account definition for user accounts from the Account definition (initial) menu.

4. Save the changes.

Related topics

- Automatic assignments of persons to Emp user accounts
- Master data for a manage level

Deleting an account definition

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.

a. In **One Identity Manager**, select the **Epic healthcare| Basic configuration data | Account definitions | Account definitions** category.

b. Select an account definition in the result list.

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

d. Disable the **Automatic assignment to employees** option on the **General** tab.

e. Save the changes.

2. Remove direct assignments of the account definition to employees.

a. In **One Identity Manager**, select the **Epic healthcare | 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. Remove employees from **Remove assignments**.

e. Save the changes.

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

a. In **One Identity Manager**, select the **Epic healthcare | 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 **Remove assignments**, remove the relevant departments, cost centers, and locations.

e. Save the changes.

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

a. In **One Identity Manager**, select the **Epic healthcare | Basic configuration data | Account definitions | Account definitions** category.

b. Select an account definition in the result list.

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

Remove the business roles in Remove assignments.

d. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

To remove an account definition from all IT Shop shelves

a. In **One Identity Manager**, select the **Epic healthcare | Basic configuration data | Account definitions | Account definitions (non role-based login)** category.

- OR -

In **One Identity Manager**, select the **Entitlements | Account definitions (role-based login)** 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 **One Identity Manager Service** . All requests and assignment requests with this account definition are canceled in the process.

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

a. In **One Identity Manager**, select the **Epic healthcare | Basic configuration data | Account definitions | Account definitions** category.

b. Select an account definition in the result list.

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

d. Remove the account definition in the **Required account definition** menu.

e. Save the changes.

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

a. In **One Identity Manager**, select the client in the **Epic healthcare | Connection**.

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

c. Remove the assigned account definitions on the **General** tab.

d. Save the changes.

8. Delete the account definition.

a. In **One Identity Manager**, select the **Epic healthcare | Basic configuration data | Account definitions | Account definitions** category.

b. Select an account definition in the result list.

c. Click to delete an account definition.

Password policies for Epic User Account

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

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

> NOTE: To set password for Epic EMP user accounts, the target Epic system should be using Epic Native authentication

Detailed information about this topic

- Predefined password policies
- Predefined password policies
- Editing password policies
- Initial password for Epic User Account

Predefined password policies

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

Password for logging in to One Identity Manager

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

> NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts or system users. For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming employees' central passwords

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

> IMPORTANT: Ensure that the Employee central password policy password policy does not violate the system-specific requirements for passwords. For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policies for user accounts

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

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

The Epic password policy is predefined for Epic. You can apply this password policy to Epic user accounts (EPCUser.Password) of an Epic connection.

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

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

Applying password policies

The Epic password policy is predefined for Epic.

You can apply this password policy to Epic user accounts (EPCUser.Password) of an Epic Connection. If the clients' password requirements differ, it is recommended that you set up your own password policies for each client. Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

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

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

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

To reassign a password policy

1. Select **Epic healthcare | Basic configuration data | Password policies** in **One Identity Manager**.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data

Table 11: Cap

Property	Description
Apply to	Application scope of the password policy. To specify an application scope a. Click next to the text box. b. Select one of the following references under Table: The table that contains the base objects of synchronization. Select the TSBAccountDef table to apply the password policy based on the account definition. Select the TSBBehavior table to apply the password policy based on the manage level. c. Select the table that contains the base objects under Apply to.

	• 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. d. Click OK.
Password column	The password column's identifier.
Password policy	The identifier of the password policy to be used.

5. Save the changes.

To change a password policy's assignment

1. Select **Epic healthcare | Basic configuration data | Password policies** in **One Identity Manager.**
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Select the assignment you want to change in Assignments.
5. Select the new password policy to apply from the **Password Policies** menu.
6. Save the changes.

The EMPTemplate is deleted from the One Identity Manager database and all the associated EMPTemplate to the Epic User.

Editing password policies

To edit a password policy

1. Select **Epic healthcare | Basic configuration data | Password policies** in **One Identity Manager**.
2. Select the password policy in the result list and select Change master data.

- OR -

Click in the result list toolbar.

3. Edit the password policy's master data.
4. Save the changes.

Detailed information about this topic

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

General master data for a password policy

Enter the following master data for a password policy.

Table 12: Table Master data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Spare text box for additional explanation.Translate the given text using the button.
Error Message	Custom error message outputted if the policy is not fulfilled. Translate the given text.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. NOTE: The One Identity Manager password policy is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts or system users.

Policy settings

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

Table 13: Table Policy Settings

Property	Meaning
Initial password	Initial password for newly created user accounts. If a password is not entered or if a random password is not generated when a user account is created, the initial password is used.
Password confirm-ation	Reconfirm password.

Min. length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager. You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the *One Identity Manager Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If, for example, a value of 5 is entered, the user's last five passwords are stored.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1, 2, 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name properties are not permitted in passwords. The values of the columns for which the Contains name properties for password check option is set are taken into account. Adjust this option in the column definition in Designer

Character classes for passwords on page

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

Table Character classes for passwords

Table 14: Table Character classes for passwords

Character classes	Description
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.

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

Custom scripts for password requirements

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

For more information see

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

Script for checking a password on page

You can implement a check script if additional policies need to be used for checking a password, which cannot be mapped with the available settings. Syntax for Check Scripts Public Sub CCC_CustomP Script for checking a password.

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

Syntax for Check Scripts

Public Sub CCC_CustomPwdValidate(policy As VI.DB.Passwords.PasswordPolicy, spwd As

System.Security.SecureString)

With parameters:

policy = password policy object

spwd = password to test

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

Example for a script for testing a password

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

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

To use a custom script for checking a password

1. Create your script in the category **Script Library** in the **Designer**.

2. Edit the password policy.

a. Select **Epic healthcare| Basic configuration data | Password policies** in **One Identity Manager.**

b. Select the password policy in the result list.

c. Select **Change master data**.

d. Enter the name of the script to be used to check a password in the **Check script input field** on the **Scripts** tab.

e. Save the changes.

Related Topics

Script for generating a password

Script for generating a password

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

Syntax for generating script

Public Sub CCC_PwdGenerate(policy As VI.DB.Passwords.PasswordPolicy, spwd As

System.Security.SecureString)

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

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

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

Excluded list for passwords

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

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

To add a term to the restricted list

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

Checking Passwords

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

To test whether a password conforms to the password policy

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

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

Testing generation of a password

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

To generate a password that conforms to the password policy

1. Select **Epic healthcare | Basic configuration data | Password policies** in **One Identity Manager**.

2. Select the password policy in the result list.
3. Select **Change master data**.
4. Select the **Test** tab.
5. Click **Generate**.

This generates and displays a password.

Initial password for Epic User Account

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

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

Related Topics

- Email notification about login data
- Password policies for Epic User Account

Email notification about login data

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

Prerequisites

The following prerequisites must be fulfilled in order to use notifications

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

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

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

4. Ensure that a language can be determined for all employees. Only then can they receive email notifications in their own language. For more 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**, activate the configuration parameter **TargetSystem | Epic healthcare | Accounts | InitialRandomPassword**.

2. In the **Designer**, activate the configuration parameter **TargetSystem | Epic healthcare | Accounts | InitialRandomPassword | SendTo** and enter the recipient of the notification as a value.

3. In the **Designer**, activate the configuration parameter **TargetSystem | Epic healthcare | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName**.

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

4. In the **Designer**, activate the configuration parameter **TargetSystem | Epic healthcare | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

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

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

Target system managers

A default application role exists for the target system manager in One Identity Manager.

Assign the employees who are authorized to edit all tenants in One Identity Manager to this application role.

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

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

Implementing application roles for target system managers

1. The **One Identity Manager** administrator assigns employees to be target system managers.

2. These target system managers add employees to the default application role for target system managers.

Target system managers with the default application role are authorized to edit all tenants in **One Identity Manager**.

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

Default Application Roles for Target System Managers

Table 15: Default Application Roles for Target System Managers

Users	Tasks
Target system managers	Target system managers must be assigned to Target systems | Epic or a sub-application role. Users with this application role: Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts and update the EMPTemplates or SubTemplates. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop. • Can create employees with an identity that differs from the Primary identity. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to **One Identity Manager** as **Manager administrator (Base role | Administrators)**.

2. Select **One Identity Manager Administration | Target systems | Administrators**.

3. Select **Assign employees**.

4. Assign the employee you want and save the changes.

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

1. Log into **One Identity Manager** as **Target System Administrator (Target systems | Administrators)**.

2. Select **One Identity Manager Administration | Target systems | Epic healthcare**.

3. Select **Assign employees** in the **Task** view.

4. Assign the employees you want and save the changes.

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

1. Log into **One Identity Manager** as target system manager.

2. Select the application role in **Epic healthcare | Basic configuration data | Target system managers**.

3. Select **Assign employees**.

4. Assign the employees you want and save the changes.

To specify target system managers for individual clients

1. Log into **One Identity Manager** as target system manager.

2. Select **Epic healthcare | Connections**.

3. Select the client from the result list.

4. Select **Change master data**.

5. On the General tab, select the application role in the Target system manager menu.

- OR -

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

a. Enter the application role name and assign the **Target systems | Epic healthcare** parent application role.

b. Click **OK** to add the new application role.

6. Save the changes.

7. Assign employees to this application role who are permitted to edit the client in **One Identity Manager**.

Related Topics

One Identity Manager users for managing an Epic health care system

Editing a server

Servers must know your server functionality in order to handle Epic specific processes in One Identity Manager. For example, the synchronization server.

You have several options for defining a server's functionality:

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

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 run its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

To edit a Job server and its functions

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

For more information, see

- Master data for jobserver
- Specifying server functions

Master data for jobserver

NOTE:

- All editing options are also available in **Designer** under **Base Data | Installation | Job server**.
- More properties may be available depending on which modules are installed.

Table 16: Job Server Properties table

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: .

Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The properties Server is cluster and Server belongs to cluster are mutually exclusive
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed 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 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. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32, Windows, Linux and Unix are permitted. If no

	value is specified, Win32 is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server) the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the procedure QBM_PJobQueueLoad the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the program "Job Queue Info". For more detailed information, see the One Identity Manager Process Monitoring and Troubleshooting Guide.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently being run.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

Specifying server functions

Specifying server functions

NOTE:

- All editing options are also available in **Designer under Base Data | Installation | Job server**. The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled

depending on the server function.

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

Table 17: Table

Server Function	Remark
Update Server	This server runs automatic software updating of all other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. The server can run SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	The server can run SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	The server can process CSV files using the ScriptComponent process component.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
One Identity Epic Connector	Server on which the One Identity Epic connector is installed. This server runs synchronization with the One Identity Epic target system.

Related topics

Master data for jobserver

Epic EMP template

EMPTemplate determines the access rights that a user has on an Epic System. The list of EMPTemplates are exported from the target system to the file **EMPTemplate.csv**.

EMPTemplate is loaded into the One Identity Manager by synchronization. You can assign and remove EMPTemplate from an user in One Identity Manager. However, you cannot edit the EMPTemplate in One Identity Manager.

To add EMPTemplate to an user, you can assign the EMPTemplate directly to the users. Or it can be added indirectly to departments, cost centers, location, business roles, or to the IT Shop.

After an EMPTemplate is assigned to an user, the following additional optional properties can be assigned to the EMPTemplate.

Table 18: Additional optional properties that can be assigned to the EMPTemplate

Property	Description
LoginType	The applications for which this template should be applied automatically.
StartDate	The date from which the user should begin to have access to this template.
EndDate	The date after which the user should no longer have access to this template.

Format of the CSV file EMPTemplate.csv

The CSV file **EMPTemplate.csv** has a specific format with the columns **TemplateID** and **TemplateName**.

The columns in the **EMPTemplate.csv** file are

Table 19: Columns in the EMPTemplate.csv file

Column name	Description
TemplateID	EMPTemplate's External ID

	IMPORTANT: Only ExternalID should be used.
TemplateName	Describes the EMP Template name

NOTE:

- If the **TemplateName** or **TemplateID** field has comma (,), it must be properly escaped with double quotes.
- Sample EMPTemplate report can be found in the EPC module's Miscellaneous folder.

Editing EMP template

EMPTemplate is loaded into the One Identity Manager by synchronization.

The CSV file allows you to

- Add new EMPTemplates
- Update the EMPTemplates

  NOTE: You can update only Template Name.

To edit the EMPTemplate

1. In **EMPTemplate.csv**, modify the rows.
2. In the **Synchronization Editor**, run the Synchronization project.
3. **EMPTemplate** data will be synchronized based on the operation performed on the **EMPTemplate.csv**.

Assigning the EMP template to Epic User

EMPTemplate can be assigned directly or indirectly to Epic user. For indirect assignment, employees are assigned to hierarchical roles, such as, departments, cost centers, locations, or business roles.

Prerequisite for the indirect assignment of EMPTemplate to the employees

1. Assignment of EMPTemplate is permitted for role classes (departments, cost centers, locations, or business roles).
2. Epic User accounts are marked with the EMPTemplate can be inherited option.

EMPTemplate can also be assigned to Epic user using IT shop.

Assigning EMP template directly to the Epic User

EMPTemplate can be assigned to the Epic User directly.

To assign a EMPTemplate directly to the Epic User

1. In **One Identity Manager**, navigate to **Epic Health care**.
2. Select the **User** account to which the EMPTemplate must be assigned.
3. Select **Assign Epic EMPTemplates** from **Tasks** .
4. To add the EMPTemplate, click **Add** in the form.
5. Select the EMPTemplate from the dropdown list.
6. Select **LoginType**, **StartDate** and **EndDate** according to the requirement.
7. Save the changes.

Assigning EMP template to the department, cost center, and locations

Assign EMPTemplate to departments, cost centers, or locations so that the EMPTemplate can be assigned to Epic User through these organisations.

To assign an EMPTemplate to departments, cost centers, or locations (non rolebased login)

1. In **One Identity Manager**, select the **Epic Healthcare | Epic EMPTemplates** category.
2. Select the EMPTemplates in the result list.
3. Select the **Assign organizations** task.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost centers** tab.

   NOTE:
   - You can remove the assignment of organizations in **Remove** assignments.
   - To remove an assignment, select the organization and double-click .
5. Save the changes.

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

1. In **One Identity Manager**, select the **Organizations | Departments** category.

   -OR-

   In **One Identity Manager**, select the **Organizations | Cost centers** category.

   -OR-

   In **One Identity Manager**, select the **Organizations | Locations** category.
2. Select the **department**, **cost center**, or **location** in the **result** list.
3. Select the **Assign Epic EMPTemplates** task.
4. Assign **EMPTemplate** in **Add assignments**.

   NOTE:

   - You can remove the assignment of **EMPTemplate** in **Remove** assignments.
   - To remove an assignment, select the **EMPTemplate** and double-click .
5. Save the changes.

Assigning EMP template to the business roles

Assign EMPTemplate to Business roles so that the EMPTemplate can be assigned to Epic User through these business roles.

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

1. In the **One Identity Manager**, select the **Epic Healthcare | EMPTemplates** category.
2. Select the EMPTemplates in the result list.
3. Select the **Assign business roles** task.
4. Assign business roles in **Add assignments**.

   NOTE:

   - You can remove the assignment of business roles in **Remove** assignments.
   - To remove an assignment, select the business role and double-click .
5. Save the changes.

To assign EMPTemplate to a business role (role-based login)

1. In **One Identity Manager**, , select the **Business roles** category.
2. Select the business role in the result list.
3. Select the **Assign Epic EMP Templates** task.

4. Assign EMPTemplates in **Add assignments**.

   NOTE:
   - You can remove the assignment of EMPTemplate in **Remove** assignments.
   - To remove an assignment, select the EMPTemplate and double-click .

5. Save the changes.

Assigning EMP template to the IT shop

When you assign an EMPTemplate to a IT Shop shelf, it can be requested by the shop customers.

Prerequisites

To ensure that an EMPTemplate can be requested, the following prerequisites are required

- The EMPTemplate must be marked with the IT Shop option.
- The EMPTemplate must be assigned a service item.

  NOTE: In the web portal, all products that can be requested are grouped together by service category. To make the EMPTemplate easier to find in the web portal, assign a service category to the service item.

- If you only want it to be possible for the EMPTemplate to be assigned to employees through IT Shop requests, the EMPTemplate must also be labelled 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 EMPTemplates to IT Shop shelves.

To add an EMPTemplate to IT Shop

1. In **One Identity Manager**, select the **Epic HealthCare | EMPTemplate** category.
2. In the result list, select the **EMPTemplate**.
3. Select the **Add to IT Shop** task.
4. In **Add assignments**, assign the EMPTemplate to the IT Shop shelves.
5. Save the changes.

Deleting EMP template

To delete the EMPTemplate

1. Remove the EMPTemplate from the **EMPTemplate.csv** file.
2. In **Synchronization Editor**, run the Synchronization project.

The EMPTemplate is marked as outstanding in **One Identity Manager**.

3. Remove the the EMPTemplate assignment from the EPCUser in One Identity Manager.
4. Delete the EMPTemplate from the outstanding object

   The EMPTemplate is deleted from the One Identity Manager database and all the associated EMPTemplate to the Epic User.

5

Epic SubTemplate

SubTemplate determines the access rights that a user has on an Epic System. The list of SubTemplates are exported from the target system to the file **SubTemplate.csv**.

SubTemplate is loaded into **One Identity Manager** by synchronization. You can assign and remove SubTemplate from an user in **One Identity Manager**. However, you cannot edit the SubTemplate in **One Identity Manager**.

To add SubTemplate to users, you can assign the SubTemplate directly to the users. This can be assignments of SubTemplate to departments, cost centers, location, business roles, or to the IT Shop.

SubTemplate assigned to an Epic EMP user must have a priority (also called index). SubTemplates with lower priority take precedence over higher priority. Epic EMP users can be assigned a maximum of seven SubTemplates with priority ranging from 1-7.

In case of conflicting priority in the new assignment, **One Identity Manager** resolves the conflict by maintaining the priority of the newly created SubTemplate while incrementing the priority of all existing SubTemplate by 1 starting from the conflicting priority.

The default value of **IndexPriority** can be set in **One Identity Designer |Edit Configuration parameters**.

Table 20: Default values of IndexPriority

Default value	Description
SubTemplateDefaultPriority	This default value is used for indirect assignment
SubTemplateMatrixPriority	This default value is used for SecurityMatrix SubTemplate assignment

Edit default values of IndexPriority

To edit the default values of IndexPriority

1. In **Designer**, navigate to **Edit Navigation Parameter**.
2. Expand **Target Systems** and navigate to **EPC**.
3. Update the **Default Values**.

Format of the CSV file SubTemplate.csv

The CSV file **SubTemplate.csv** has a specific format with the following columns **TemplateID** and **TemplateName**.

The columns in the **SubTemplate.csv** file are

Table 21: Columns in the SubTemplate.csv file

Column name	Description
TemplateID	SubTemplate's External ID IMPORTANT: Only External ID should be used.
TemplateName	Describes the SubTemplate name

NOTE:

- If the **TemplateName** or **TemplateID** field has comma (,), it must be properly escaped with double quotes.
- Sample **SubTemplate** report can be found in the EPC module's Miscellaneous folder.

Editing the Sub template

SubTemplate is loaded into **One Identity Manager** by synchronization.

Only **TemplateName** can updated in the csv file. If **TemplateID** is updated it will be considered as new Template in the One Identity Manager.

To edit the SubTemplate

1. In **SubTemplate.csv**, modify the rows.
2. In the **Synchronization Editor**, run the Synchronization project.
3. SubTemplate data will be synchronized based on the operation performed on the **SubTemplate.csv**.

Assigning the Sub template to Epic User

SubTemplate can be assigned directly or indirectly to Epic user. For indirect assignment, employees are assigned to hierarchical roles, such as, departments, cost cent res, locations, or business roles.

Prerequisite for the indirect assignment of SubTemplate to the employees

1. Assignment of SubTemplate is permitted for role classes (departments, cost centers, locations, or business roles).
2. Epic User accounts are marked with the SubTemplate can be inherited option.

NOTE: SubTemplate can also be assigned to Epic user through IT shop.

Assigning the Sub template directly to the Epic User

SubTemplate can be assigned to the Epic User directly.

To assign a SubTemplate directly to the Epic User

1. In **One Identity Manager**, navigate to **Epic Health care.**
2. Select the **User** account to which the SubTemplate must be assigned.
3. Select **Assign Epic SubTemplates** from **Tasks** .
4. To add the SubTemplate, click **Add** in the form.
5. Select the priority Index options from the dropdown.
6. Save the changes.

Assigning SubTemplate to the department, cost center, and locations

Assign SubTemplate to departments, cost centers, or locations so that the SubTemplate can be assigned to Epic User through these organizations.

To assign a SubTemplate to departments, cost centers, or locations (non rolebased login)

1. In One Identity Manager, select the **Epic Healthcare | Epic SubTemplates** category.
2. Select the SubTemplate in the result list.
3. Select the **Assign organizations** task.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost centers** tab.

   NOTE:

- You can remove the assignment of organizations in **Remove** assignments.
- To remove an assignment, select the organization and double-click .

5. Save the changes.

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

1. In One Identity Manager, select the **Organizations | Departments** category.
   - OR –
   In One Identity Manager, select the **Organizations | Cost centers** category.
   - OR –
   In One Identity Manager, select the **Organizations | Locations** category.
2. Select the **department**, **cost center**, or **location** in the result list.
3. Select the **Assign Epic SubTemplates** task.
4. Assign SubTemplate in **Add assignments**.

   NOTE:
   - You can remove the assignment of SubTemplate in **Remove** assignments.
   - To remove an assignment, select the SubTemplate and double-click .

5. Save the changes.

Assigning Sub template to the business roles

Assign SubTemplate to **Business roles** so that the SubTemplate can be assigned to Epic User through these business roles.

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

1. In **One Identity Manager**, select the **Epic Healthcare | SubTemplates** category.
2. Select the SubTemplates in the result list.
3. Select the **Assign business roles** task.
4. Assign business roles in **Add assignments**.

   NOTE:
   - You can remove the assignment of business roles in **Remove** assignments.
   - To remove an assignment, select the business role and double-click .

5. Save the changes.

To assign a SubTemplate to a business role (role-based login)

1. In **One Identity Manager**, select the **Business roles** category.
2. Select the business role in the result list.

3. Select the **Assign Epic Sub Templates** task.
4. Assign SubTemplates in **Add assignments**.

   NOTE:
   - You can remove the assignment of SubTemplate in **Remove** assignments.
   - To remove an assignment, select the SubTemplate and double-click .
5. Save the changes.

Assigning SubTemplate to IT shop

When you assign an SubTemplate to a IT Shop shelf, it can be requested by the shop customers.

Perquisites

To ensure it can be requested, the following prerequisites are required

- The SubTemplate must be marked with the IT Shop option.
- The SubTemplate must be assigned a service item.

  NOTE: In the web portal, all products that can be requested are grouped together by service category. To make the SubTemplate easier to find in the web portal, assign a service category to the service item.
- If you only want it to be possible for the SubTemplate to be assigned to employees through IT Shop requests, the SubTemplate must also be labelled 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 SubTemplates to IT Shop shelves.

To add an SubTemplate to IT Shop

1. In **One Identity Manager**, select the **Epic HealthCare | SubTemplate** category.
2. In the result list, select the SubTemplate.
3. Select the **Add to IT Shop** task.
4. In **Add assignments**, assign the SubTemplate to the IT Shop shelves.
5. Save the changes.

Deleting the Sub template

To delete the SubTemplate

1. Remove the SubTemplate from the **SubTemplate.csv** file
2. In **Synchronization Editor**, run the synchronization project

   The SubTemplate is marked as outstanding in **One Identity Manger**.
3. Remove the SubTemplate assignment from the EPCUser in One Identity Manager.
4. Delete the SubTemplate from the outstanding object

   The SubTemplate is deleted from the **One Identity Manager** database and all the associated SubTemplate to the Epic User.

6

Epic Connection

Epic connection contains the details about the target Epic system. The Creating a synchronization project for initial synchronization of an Epic health care system section provides the necessary per-requisites to connect to the target Epic system. Refer to the section for details.

General Master Data for Epic Connection

Enter the following data on **General**

Table 22: General Master Data for Epic Connection

Display Name	The Epic connection's display name
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 Epic connection and user accounts should be created which are already managed (**Linked configured** state). 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 client. Target system managers only edit objects of the client to which they are assigned. Each Epic connection can have a different target system manager assigned to it. Select the **One Identity Manager** application role whose members are responsible for administration of this Epic connection. Use the button to add a new application role.
Synchronized By	Type of synchronization through which the data is synchronized between the Epic and One Identity Manager.

You can no longer change the synchronization type once objects for this tenant are present in One Identity Manager. Use One Identity Manager when you create a Epic connection with the Synchronization Editor.

Table 23: Table Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	Epic Connector	Epic Connector
No Synchron-ization	None	None

Related Topics

- Automatic assignments of persons to Emp user accounts
- Target system managers

Assign Epic EMPTemplate Matrix Property Mapping

A mapping must be established between the Person Identity attributes and the EMPTemplate security matrix attributes to group the EMPTemplate with one or more attributes of the Identity. Refer to the section Configuring SecurityMatrix for EMPTemplate for configuration details.

Related Topics

- Epic EMP template
- Security Matrix for EMP template

Define Search criteria for Employee assignment

The criteria for matching Epic user accounts to Employee is defined for an Epic connection. Refer to the section Editing search criteria for automatic employee assignment.

Related Topics

- Automatic assignments of persons to Emp user accounts

View Epic Security Matrix for EMPTemplate

The **Security Matrix** for **EMPTemplate** once imported could be viewed using **One Identity Manager**. Refer to the section Viewing the EMPTemplate Security Matrix for details.

Related Topics

- Epic EMP template
- Security Matrix for EMP template

Assign Epic SubTemplate Matrix Property Mapping

A mapping must be established between the Person Identity attributes and the SubTemplate security matrix attributes, in order to group the SubTemplate with one or more attributes of the Identity. Refer to the section Configuring SecurityMatrix for SubTemplate for configuration details.

Related Topics

- Epic SubTemplate
- Security Matrix for SubTemplate

View Epic Security Matrix for SubTemplate

The **Security Matrix** for **SubTemplate** once imported could be viewed using **One Identity Manager**. Refer to the section Viewing the SubTemplate Security Matrix for details.

Related Topics

- Epic SubTemplate
- Security Matrix for SubTemplate

Configure settings for SubTemplate Index

SubTemplate assigned to an Epic EMP user must have a priority (also called index). The default SubTemplate priority for different OneIM organizations and business roles can be configured. When an user receives a SubTemplate through base tree based inheritance, the configured SubTemplate priority for the organization is automatically applied.

To configure the SubTemplateIndex settings follow the below mentioned steps:

1. In **One Identity Manager**, select the appropriate Epic connection that has been created.
2. In the **Tasks** section, select the link **Configure settings for SubTemplateIndex**.
3. Update the **SubTemplate Index** for the organization or business role
4. Save the settings.

Related Topics

- Epic SubTemplate
- Configuration parameters for managing Epic health care system

Epic EMP User Accounts

Epic EMP user accounts can be managed from One Identity.

User Report

The master list of Epic EMP user accounts that should be managed from One Identity Manager should be exported from Epic and provided in a CSV file. The name of the CSV file should be **Users.csv**. This is called the user report and the generated report should be copied to the configured CSV import directory (The CSV import directory was configured when you created the synchronization project).

NOTE:

- Contact Epic regarding on how to automate the user report generation and dropping the report generated to the CSV import directory.

If the CSV import directory is a local folder on the job server and One Identity Manager workstation, make sure to copy the user report to both the job server's and One Identity Manager workstation's local folder

If the CSV import directory is a network share, make sure it is accessible from both the job server and One Identity Manager workstation.

The **Users.csv** report has a specific format. It should contain the following fields and the order should be maintained.

- **User Number (Local ID or External ID)**: The Epic Emp user's External ID.
- **System Login**: The Epic Emp user's System Login ID.
- **UserName**: The Epic Emp user's name.
- **User Record Status**: The Epic Emp user's status (Active / InActive).

IMPORTANT:

- The first line in the **Users.csv** report should be the header row with the fields specified above.
- Field ordering in the **Users.csv** report should be maintained.
- The user number provided should be the Epic EMP user's External ID.
- If any of the field has a comma it should be escaped properly with double quotes.

- The user report should contain only the list of EMP user accounts that need to be managed from One Identity Manager. EMP user accounts such as service user accounts or In-Active accounts or any other user accounts that does not need to be managed from One Identity Manager should not be there in the user's report and these users can be filtered out when the report is generated in Epic.

User Report customization

Epic connector uses the user report to get the master list of Epic EMP user accounts. Sometimes additional customization might need to be done to the user report generated. For example, we might want to remove certain Epic EMP user accounts such as contractors from the user report, which could have not been possible when the report is generated in Epic. To address these use cases, Epic connector provides the ability to perform additional customization to the user report generated from Epic. The Epic report customization is done in a PowerShell script named **EPCUserReportFilterScript.ps1**.

The Epic connector now uses the Epic EMP user data returned by the **EPCUserReportFilterScript.ps1** PowerShell script as the master list of Epic EMP users and does not use the user data from the **Users.csv** file.

To perform additional user report customization

1. In the synchronization project choose advance settings
2. Select the option **Use Custom PowerShell Script for User Import**. Save the synchronization project changes.
3. Copy the **EPCUserReportFilterScript.ps1** PowerShell script from installer's EPC Module dvd/Addon folder to the configured CSV import directory in synchronization project .

   NOTE: If the CSV import directory is configured as a local folder then the PowerShell script must be copied to the local folder in job server and OneIM workstation.
4. The Epic connector calls the PowerShell script's **Get-OneIMEpicUsers function** to get the list of Epic EMP users. Customize the function according to the requirements.

   IMPORTANT: The data must be returned in the format as documented in the function.

Testing the changes

Once the PowerShell script has been customized it must be tested.

1. Update the **Test-Get-OneIMEpicUsers** function in the PowerShell script and run the script. This is a test function that validates the data returned by the **Get-OneIMEpicUsers** function. Make sure the data is returned is correct

   NOTE: The PowerShell script can be run from the OneIM workstation.
2. Open the synchronization project and navigate to the start up configuration. Run a simulation. Make sure the data returned is correct. This test makes sure that the Epic connector can invoke the PowerShell script and load the data returned by the PowerShell script.

   NOTE:

- If the PowerShell script execution policy on job server or One Identity Manger workstation dictates that it needs to be signed, then the PowerShell script has to be signed after modification or change the script execution policy on the server to be less restrictive for the script to run.
- For more information on PowerShell script execution policy refer to https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-5.1.

Epic EMP user account attribute un-locking

Epic EMP user account attributes need to be un-locked in Epic in order to manage them from One Identity. The following table provides the list of Epic EMP attributes along with the EMP item number. Contact the Epic data courier team and un-lock attributes that you want to manage from One Identity.

Table 24: Epic EMP attributes

EMP item number	EMP attribute name	Comments
.1	User Number	
.2	UserName	
23	Contact Comment	
35	User Name	
36	User Name Over Time	
45	System Login	
50	Status	
55	User Login Blocked	
180	User Alias	
720	Effective From Date	
730	Effective To Date	
14100	Notes	
14700	Sex	
20414	Primary Manager	
198	Applied Linkable Template	
.198	Applied Linkable Template Record Name	
1101	Default Linkable Template	

.1101	Default Linkable Template Record Name	
40	Password	Applicable only if Native authentication has been enabled in Epic
20415	Additional Managers	
1110	Linkable Templates	
1111	Linkable Templates Effective from Date	
1112	Linkable Templates Effective to Date	
1115	Linkable Templates Login Types	
9205	Linked Subtemplates	
20701	User MPI ID	
20700	User MPI ID Type	
2401	Type of External ID	
2402	External User ID	
2405	External ID Active	
14150	Employee Demographic 1	
14151	Employee Demographic 2	
14152	Employee Demographic 3	
100	Address	
110	City/Locality	
112	County	
135	Country	
120	State/Province	
130	Zip Code	
140	Phone Number	
150	Email Address	
114	District	
102	House Number	
17500	LinkedProviderID	

Linking user account to employees

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

One Identity Manager supports the following method for linking employees and their user accounts.

- Employees can automatically obtain their user accounts using account definitions. If an employee does not yet have a user account in Epic, 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 user accounts through account definitions, you can specify the way user accounts behave when employees are enabled or deleted.
- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee master data is created on the basis of existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. Define criteria for finding employees for automatic employee assignment
- Employees and user accounts can be entered manually and assigned to each other.

For more information, see

- Editing master data for user account
- Account definition for Epic User Account
- Automatic assignments of persons to Emp user accounts
- For detailed information about handling and administration of employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

Editing master data for user account

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

NOTE:

- It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.
- If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location or a primary cost center.

To create a user account

1. In **One Identity Manager**, select **Epic health care | User accounts**.
2. Click in the result list toolbar.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

To edit master data for a user account

1. In **One Identity Manager**, select **Epic health care | User accounts**.
2. Select the user account in the result list and run Change master data.
3. Edit the user account's resource data.
4. Save the changes.

For more information, see

- General master data for Epic User Account
- Demographic data for Epic User Account
- Password data for Epic User Account
- Template data for Epic User Account

Related Topics

Account definition for Epic User Account

General master data for Epic User Account

General master data for an Epic EMP user account

Enter the following data on **General** tab

Table 25: Additional Master Data for 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. For a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity or Service identity, you can create a new employee. To do this, click **Next** to the input field and enter the required employee master data. The login data required depends on the selected identity type.
Account Definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved.
Manage Level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Account Name	Template calculated value that is set to user's Name.
User Account is Blocked	Check this check box if user account is blocked.
Block status reason	Optionally select the reason why the user is account is blocked. NOTE: Block status reason is a defined list of values and can be customized in the Designer
Block status comment	Optional comment on why the user account is blocked.
First Name	The first name of the user. If you have assigned an account definition, the input field is automatically filled with the manage level.
Last Name	The last name of the user. If you have assigned an account definition, the input field is automatically filled with the manage level.
Middle Name	The middle name of the user. If you have assigned an account definition, the input field is automatically filled with the manage level.

Gender	Select the gender of the user. If you have assigned an account definition, the input field is automatically filled with the manage level.
UserExternalID	Read only field. The user's external id is created in Epic and synchronized back in to OneIM database.
Community ID	Read only field. The user's community id is created in Epic and synchronized back in to OneIM database.
Internal ID	Read only field. The user's internal id is created in Epic and synchronized back in to OneIM database.
System Login ID	The user's system login id.
Display Name	Template calculated value that is set to user's Name.
Name	Template calculated value that is set to user's Name. Once synchronization runs for the user, the user's External ID is appended to the name.
User Alias	The user's alias.
User Notes	Any notes about the user.
Start Date	The date on which the user becomes active. On object creation, if you have assigned an account definition, the input field is automatically filled with the manage level.
End Date	The date at which the user becomes inactive. If you have assigned an account definition, the input field is automatically filled with the manage level.
Contact Comment	Contact comment for the user. This is a Template calculated value. NOTE: • The template can be customized in the Designer according to customer requirements. • The contact comment for Epic EPC User would be set only on user input and no default value would be applied.
Primary Manager	The user's primary manager. NOTE: Primary manager can be chosen only from the list of managers assigned to the user
Category	Categories for the inheritance
EMPTemplate can be inherited	Specifies whether the user can inherit EMPTemplate through Base tree inheritance via Organizations, Business Roles and ITShop.

SubTemplate can be inherited	Specifies whether the user can inherit SubTemplate through Base tree inheritance via Organizations, Business Roles and ITShop.
IsTemplateUpdateDisabled	Specifies whether the EMPTemplate and SubTemplate can be inherited through SecurityMatrix approach. Select this option if EMPTemplate and SubTemplate inheritance should NOT happen for the user. NOTE: Only applicable for SecurityMatrix inheritance.
DoNotSync	Specifies whether the user information should NOT be synchronized from the target Epic system in to One Identity Manager. Select this option if user information should NOT be synchronized.
Privileged User Account	Specifies whether this account is a Privileged User Account. NOTE: This option is only for governance. Setting this option does not have any impact of the target Epic system.
User account is disabled	This is a Template calculated value. Specifies whether the user account is disabled. NOTE: The template can be customized in the Designer according to customer requirements
EMP SER Link	This field specifies the link between the Epic EMP User record and SER record. NOTE: The prerequisite for provisioning this field is to have the LinkedProviderIDType to be configured in the respective targets synchronization project.

Related topics

- Account definition for Epic User Account
- Linking user account to employees
- Disabling Epic User Account

Demographic data for Epic User Account

Enter the following Demographic data on the **Demographics** tab. The demographic information listed here can be provisioned on to the target Epic system. This information is not synchronized from the target Epic system on to One Identity Manager.

Table 26: Demographics data

Property	Description
Phone	The user's phone number. If you have assigned an account definition, the input field is automatically filled with the manage level.
Phone extension	The user's phone extension. If you have assigned an account definition, the input field is automatically filled with the manage level.
Contact Email	The user's contact Email. If you have assigned an account definition, the input field is automatically filled with the manage level.
House Number	The user's house number. If you have assigned an account definition, the input field is automatically filled with the manage level.
Street	The user's street. If you have assigned an account definition, the input field is automatically filled with the manage level.
City	The user's city. If you have assigned an account definition, the input field is automatically filled with the manage level.
County	The user's county. If you have assigned an account definition, the input field is automatically filled with the manage level.
District	The user's district. If you have assigned an account definition, the input field is automatically filled with the manage level.
State	The user's state. If you have assigned an account definition, the input field is automatically filled with the manage level.
Country	The user's country. If you have assigned an account definition, the input field is automatically filled with the manage level.
Zip code	The user's zip code. If you have assigned an account definition, the input field is automatically filled with the manage level.

Password data for Epic User Account

Enter the following Password data on the **Password** tab.

Table 27: Password data

Property	Description
Password	Enter the password
Confirmation	Renter the password for confirmation

NOTE: The password data is applicable only if Epic Native Authentication has been enabled in the Target Epic system. Password updates in the target Epic system take place only if Epic Native authentication has been enabled in Epic and Epic Native authentication

option is selected in the synchronization project.

Template data for Epic User Account

The templates data tab is used to configure the Default and Applied EMPTemplates for the user.

Table 28: Template data for Epic User Account

Property	Description
Default EMP Template inherited	This is a read only calculated field. If the Designer configuration parameter AutoSetAppliedEMPTemplate option has been selected, then whenever a user inherits an EMPTemplate either through Base tree or Security matrix it is automatically set as the Default EMPTemplate for the user in the target Epic system. NOTE: The Designer configuration parameter AutoSetAppliedEMPTemplate is NOT selected by default.
Default EMP Template	This option allows you to manually set the default EMPTemplate for a user. NOTE: The Default EMPTemplate set in the target Epic system is always synchronized back to this field
Applied EMPTemplate inherited	This is read only calculated field. If the Designer configuration parameter AutoSetAppliedEMPTemplate option has been selected, then whenever a user inherits an EMPTemplate either through Base tree or Security matrix it is automatically set as the Applied EMPTemplate for the user in the target Epic system. NOTE: The Designer configuration parameter AutoSetAppliedEMPTemplate is NOT selected by default.
Applied EMP Template	This option allows you to manually set the Applied EMPTemplate for a user. NOTE: The Applied EMPTemplate set in the target Epic system is always synchronized back to this field

NOTE: If a user has only one EMPTemplate assigned either through direct or indirect assignment, it is automatically set as the Default and Applied EMPTemplate for the user.

Additional tasks for managing Epic User Account

Overview of Epic User Account

Use this task to obtain an overview of the most important information about a user account.

To obtain an overview of a user account

1. Select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. Select **Epic user account**.

Changing the manage level of Epic EMP 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 **One Identity Manager**, select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. On the **General** tab, select the manage level in the **Manage level** menu.
5. Save the changes.

Related Topics

Editing master data for user account

Managing IdentityIDs for Epic User Account

Identity ID's are additional identities a user can have on the target Epic system.

To assign an Identity ID for an Epic EMP user

1. In **One Identity Manager**, select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. In **Tasks**, select **Manage IdentityIDs**.
4. Click **Add**.

5. Enter the System User ID and System type.
6. Click **Save**.

NOTE:

- The system type needs to be valid and depends on customer configuration
- The system type could be set to a pre-defined list of values in the Designer depending on customer requirements
- Once an Identity has been created only the System User ID can be changed
- Identity ID cannot be removed from One Identity Manager

Managing External Identifiers for Epic User Account

These are the external identifiers that a user can have on the target Epic system.

To assign an external identifier for an Epic EMP user

1. In **One Identity Manager**, select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. In **Tasks**, select **Manage External IDs**.
4. Click **Add**.
5. Enter the System User ID, System type and select the **IsActive** option.
6. Click **Save**.

NOTE:

- The system type needs to be valid and depends on customer configuration
- The system type could be set to a pre-defined list of values in the Designer depending on customer requirements
- Once an external identifier has been created, the IsActive option can be toggled as required

Managing Epic User Account Managers

An Epic user can contain multiple managers and these managers can be assigned here.

To assign a manager for an Epic EMP user

1. In **One Identity Manager**, select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. In **Tasks**, select **Assign Epic User managers**.
4. Select the user managers in **Add assignments**.

5. Click **Save**.

Managing Demographics for Epic User Account

Epic EMP user demographic information can be managed from One Identity Manager.

To assign Demographic information for an Epic EMP user

1. In **One Identity Manager**, select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. In **Tasks**, select **Manage Demographics**.
4. Click **Add**.
5. Enter the UserDemographic1, UserDemographic2, UserDemographic3.
6. Click **Save**.

NOTE:

- DemographicsIndex represents a row number and is automatically incremented when a record is created
- In case of deletion, higher order DemographicsIndex record must first be deleted prior to removing lower order DemographicsIndex record.
- The captions UserDemographic1, UserDempgraphic2 and UserDemographic3 can be updated in the Designer depending on what the attribute has been mapped to in the customer's Epic environment

Automatic assignments of persons to Emp user accounts

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

If automatic employee assignment to user accounts is enabled, automatic assignment of employees to user accounts takes place from that moment onwards. If you disable the automatic employee assignment to user accounts later, the changes only affect user

accounts added or updated after this point in time. Existing employee assignment to user accounts remain intact.

Perform the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, enable the configuration parameter TargetSystem | Epic | PersonAutoFullsync and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer activate the TargetSystem | Epic | PersonAutoDefault configuration parameter and select the required mode.
- Use the TargetSystem | Epic | 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 client. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for assigning employees to the client.

NOTE:

The following applies for synchronization

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

The following applies outside synchronization

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

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

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

To select user accounts through account definitions

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

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

Related Topics

- Creating account definitions on page
- Creating Account Definitions - Master data for an Account Definition
- Assigning account definition to employees
- Editing search criteria for automatic employee assignment

Editing search criteria for automatic employee assignment

The criteria for employee assignment are defined for the client. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criterion is written in XML notation to the Search criteria for automatic employee assignment column (AccountToPersonMatchingRule) in the EPCRoot table. Search criteria are evaluated when employees are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly.

NOTE: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined. It is not recommended to make assignment to administrative user accounts based on search criteria. Use Change master data to assign employees to administrative user account for the respective user account.

NOTE: One Identity Manager supplies a default mapping for employee assignment.

Only carry out the following steps when you want to customize the default mapping.

To specify criteria for employee assignment

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

Table 29: : Standard search criteria for user accounts and contacts

Apply to	Column for employee	Column for user account
Epic EMP User accounts	FirstName	FirstName

	LastName	LastName
	MiddleName	MiddleName

5. Save the changes.

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

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

Table 30: : Manual Assignment View

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

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

To apply search criteria to user accounts

- Click **Reload**.

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

To assign employees directly over a suggestion list

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

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

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

– OR –

2. Click **No employee assignment**.
   a. Click **Select** employee for the user account to which you want to assign an employee. Select an employee from the menu.
   b. Click **Select** for all user accounts to which you want to assign the selected employees. Multi-select is possible
   c. . Click **Assign selected**.
   d. Confirm the security prompt with **Yes**.

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

To remove assignments

1. Click **Assigned user accounts**.
   a. Click **Select** for all user accounts for which you want to delete the employee assignment. Multi-select is possible.
   b. Click **Remove selected**.
   c. Confirm the security prompt with **Yes**.

      The assigned employees are removed from the selected user accounts.

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

Related Topics

Automatic assignments of persons to Emp user accounts

Disabling Epic User Account

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

Scenario

The user account is linked to employees and is managed through account definitions. User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the manage level Full managed manage level are disabled depending

on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the EPCUser.AccountDisabled column

Scenario

User accounts are linked to employees. No account definition is applied. Specify the desired behavior using the QER | Person | TemporaryDeactivation configuration parameter. If the configuration parameter is set, the employee's user accounts are locked if the employee is permanently or temporarily disabled. 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 **One Identity Manager**, select **Epic Healthcare | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Enable **Account is disabled** on the **General** tab.
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 **One Identity Manager**, select **Epic Healthcare | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Enable **Account is disabled** on the **General** tab.
5. Save the changes.

Related Topics

- Account definition for Epic User Account
- Creating manage level - Master data for manage level
- Deleting and restoring Epic EMP user accounts

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

Deleting and restoring Epic EMP user accounts

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

To delete a user account

1. Select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. Delete the user account.
4. Confirm the security prompt with **Yes**.

To restore a user account

1. Select **Epic health care | User accounts**.
2. Select the user account in the result list.
3. Click **Undo delete** in the result list toolbar.

Configuring deferred deletion

By default, user accounts are finally deleted from the database after 30 days. The user accounts are initially disabled. You can re-enable the user accounts until deferred deletion is run. After deferred deletion is run, the user account are deleted from the database and cannot be restored anymore. The deferred deletion days can be configured to a value other than the default value, which is 30 days.

Setting External User ID on Epic EMP user creation

The External User ID can be set either by letting Epic auto-generate the ID or the customer can manually set the ID.

If the ID needs to be auto-generated by Epic, then a temporary unique id of the format *OneIM_Autogenerated_GUID* is automatically created on user account creation. The connector reads the ID and checks if it is an auto generated string of the format *OneIM_Autogenerated_GUID*. If that is the case, it lets Epic generate the ID for the user. The Epic generated ID is re-synced back in to OneIM.

If the Epic Admin needs to enter the ID manually on user creation, admin can disable the UserExternalID column's value template that generates the unique id in the designer. The admin can then manually set the ID on user creation.

8

Security Matrix

Entitlements in Epic, including the EMPTemplate and SubTemplates, are assigned to the Epic users based on one or more attributes associated with the Identity. Security matrix is a table that consists of entitlements grouped with one or more attributes of the Identity, which mostly consist of organizational attributes.

One Identity Manager out of the box provides capabilities to assign these entitlements, including the EMPTemplates and SubTemplates, to organizations or business roles. This allows all user accounts linked to person Identities that belong to these organizations to automatically inherit the respective entitlements. Maintenance of such assignments becomes difficult while dealing with a combination of business roles as dynamic groups. Several dynamic group calculations also degrade the overall performance of assignments. In this scenario, configuring entitlements for the combination of One Identity Manager organizations and business roles in the security matrix makes the process easier to maintain and performance effective.

Security Matrix for EMP template

Security matrix for EMPTemplate is a table that consists of EMPTemplates grouped with one or more attributes of the Identity, which mostly consist of organizational attributes.

Configuring SecurityMatrix for EMPTemplate

A mapping must be established between the Person Identity attributes and the EMPTemplate security matrix attributes to group the EMPTemplate with one or more attributes of the Identity.

This section describes the steps to define such mappings in One Identity Manager.

To define the column mappings between the Person Identity and the Security Matrix for EMPTemplate

1. Open **One Identity Manager** and select the appropriate Epic connection that has been created.
2. In the **Tasks** section, select the link **Assign Epic EMPTemplate Matrix property mapping**.
3. Select the **Person** column and corresponding **Security Matrix** column from the respective drop downs for the mapping.
4. Save the mappings.

NOTE: The Epic EMPTemplate security matrix has a maximum of ten Properties that can be mapped with the Person Identity. The security matrix will always apply an AND operation on the combination of properties when assigning the respective EMPTemplate.

Importing SecurityMatrix for EMPTemplate

EMPTemplates can be assigned automatically to an Epic user account through **SecurityMatrix**. To achieve this, **SeurityMatrix** must be imported into **One Identity Manager**. On subsequent changes to the security matrix, the updates to the matrix must be imported so that the Epic user account to **EMPTemplate** assignments are updated.

You can import the SeurityMatrix using these methods

- Importing the matrix using CSV import Synchronization Project
- Importing the matrix directly into One Identity Manager Table

Importing the matrix using CSV import Synchronization Project

The **SecurityMatrix** for **EMPTemplate** can be imported into **One Identity Manager** using a **SecurityMatrix csv file**.

The csv file is imported into **One Identity Manager** using a CSV synchronization project.

Setup Security Matrix Synchronization Project

This project provides a CSV synchronization workflow which imports the **SecurityMatrixEMPTemplate** into **One Identity Manager**.

EMPTemplate assignments are setup in the file named **SecurityMatrixEMPTemplate.csv**

SecurityMatrixEMPTemplate CSV file configuration

The names of the columns in this file are

- Property01
- Property02
- Property03
- Property04
- Property05
- Property06
- Property07
- Property08
- Property09
- Property10
- EMPTemplateID

Details about the values in the columns in the EMPTemplate csv file

Enter the values mentioned in the following table in the corresponding columns of the csv file.

Table 31: Columns in the csv file

Columns in the csv file	Values
Property01 to Property10	Full name of the **One Identity Manager Organization** or **Business role**. NOTE: Property01 to Property10 represent the different possible One Identity Manager Built-in Organization or Business role or Identity Attributes like Title. Out of box only one business role assignment is supported that is mapped to the value entered in UID_Org in the person table.
EMP Template	EMP Template External ID NOTE: Property01 to Property10 represent the different possible One Identity Manager Built-in Organization or Business role or Identity Attributes like Title.

After the Security Matrix CSV files has been setup, the synchronization project can be created using the procedure below.

To create the synchronization project

1. In the **Synchronization Editor**, create a new Synchronization Project using the **CSV connector**.
2. Select the **SecurityMatrixEMPTemplate csv** file.

   NOTE: A sample CSV file can be found in the **Miscellaneous** folder under the EPC module.

3. Set the value of the number of lines in header to 1.
4. Select the **EPCSecurityMatrix** as the template and create the csv project.
5. Update the project variable **UID_EPCROOT** with the **UID** of the **EPCRoot** object that has been created for Epic Synchronization project.
6. The value can be obtained from the **One Identity Manager Object Browser** by navigating to the **EPCRoot** table.
7. Save changes to database

Importing the matrix directly into One Identity Manager Table

The **SecurityMatrix** for **EMPTemplate** can be populated into the **EPCMatrixEMPTemplate** table using a custom solution implemented in the customer environment.

There could be scenarios where the customer would prefer alternate sources for security matrix import other than a csv file, for example a direct interface from the Epic Database or a custom application based on their implementation.

Viewing the EMPTemplate Security Matrix

The **Security Matrix** for **EMPTemplate** once imported could be viewed using **One Identity Manager**.

To view the imported matrix

1. In **One Identity Manager** and navigate to the **Epic connection** that was created.
2. In the **Task** menu, click **View Security Matrix** for **EMPTemplate**.

   A grid is displayed with the **EMPTemplate** and the corresponding **Property values** for Identity.

Assignment of the EMPTemplate to Epic user accounts

The Epic user account can inherit EMP Templates from security matrix based on the properties mapped between the Identity and the matrix, provided that the **Is Template Update Disabled** flag for the user account is set to false.

The assignments inherited by the user from the Security Matrix has an **XOrigin** set to **Matrix**.

The User account **EMPTemplate** assignments are updated in the following cases

1. An initial import of the data into the **EPCMatrixEMPTemplate** table.
2. Subsequent updated to the Security Matrix for **EMPTemplate**.
3. Changes to the property values of the Identity linked to the user account.
4. Change of the Identity liked to the user account.

NOTE: Assignment of applied and default **EMPTemplate** by Security Matrix is disabled by default. To enable it the configuration parameter **AutoSetAppliedEMPTemplate** must be enabled.

Security Matrix for SubTemplate

Security matrix for SubTemplate is a table that consists of SubTemplates grouped with one or more attributes of the Identity, which mostly consist of organizational attributes.

Configuring SecurityMatrix for SubTemplate

A mapping must be established between the Person Identity attributes and the SubTemplate security matrix attributes, in order to group the SubTemplate with one or more attributes of the Identity.

This section describes the steps to define such mappings in One Identity Manager.

To define the column mappings between the Person Identity and the Security Matrix for SubTemplate follow the below mentioned steps:

1. In **One Identity Manager**, select the appropriate Epic connection that has been created.
2. In the **Tasks** section, select the link **Assign Epic SubTemplate Matrix property mapping**.
3. Select the **Person** column and corresponding **Security Matrix** column from the respective drop downs for the mapping.
4. Save the mappings.

NOTE: The Epic SubTemplate security matrix has a maximum of ten Properties that can be mapped with the Person Identity. The security matrix will always apply.

Importing SecurityMatrix for SubTemplate

SubTemplates can be assigned automatically to an Epic user account via SecurityMatrix.

In order to achieve this, SeurityMatrix must be imported into One Identity Manager.

On subsequent changes to the security matrix the updates to the matrix must be imported in order to have the Epic user account to SubTemplate assignments updated.

The SeurityMatrix can be imported using these methods

- Importing the matrix using CSV import Synchronization Project
- Importing the matrix directly into One Identity Manager Table

Importing the matrix using CSV import Synchronization Project

The **SecurityMatrix** for **SubTemplate** can be imported into **OneIdentity Manager** using a **SecurityMatrix csv** file.

The csv file is imported into **One Identity Manager** using a CSV synchronization project.

Setup Security Matrix Synchronization Project

This project provides a CSV synchronization workflow which imports the **SecurityMatrixSubTemplate** into **One Identity Manager**.

SubTemplate assignments are setup in the file named **SecurityMatrixSubTemplate.csv**.

SecurityMatrixSubTemplate CSV file configuration

The names of the columns in this file are

- Property01
- Property02
- Property03
- Property04
- Property05
- Property06
- Property07
- Property08
- Property09
- Property10
- SubTemplateID
- SubTemplateNumber

Details about the values in the columns in the SubTemplate csv file.

Enter the values mentioned in the following table in the corresponding columns of the csv file

Table 32: Columns in the csv file

Columns in the csv file	Values
Property01 to Property10	Full name of the One Identity Manager Organization or Business role NOTE: Property01 to Property10 represent the different possible One Identity Manager Built-in Organization or Business role or Identity Attributes like Title. Out of box only one business role assignment is supported that is mapped to the value entered in UID_Org in the person table.
SubTemplateID	SubTemplate External ID
SubTemplateNumber	The SubTemplateNumber and the SubTemplateID form a unique identifier for the Property Columns specified.

After the Security Matrix CSV files has been setup, the synchronization project can be created using the below steps.

To create a synchronization project

1. In the **Synchronization Editor**, create a new Synchronization Project using the CSV connector.
2. Select the **SecurityMatrixSubTemplate csv** file.

   NOTE: A sample CSV file can be found in the Miscellaneous folder under the EPC module
3. Set the value of the number of lines in header to 1.
4. Select the **EPCSecurityMatrix** as the template and create the csv project.
5. Update the project variable **UID_EPCROOT** with the **UID** of the **EPCRoot** object that has been created for Epic Synchronization project.
6. The value can be obtained from the **One Identity Manager Object Browser** by navigating to the **EPCRoot** table.
7. Save changes to database.

Importing the matrix directly into One Identity Manager Table

The **SecurityMatrix** for SubTemplate can be populated into the **EPCMatrixSubTemplate** table using a custom solution implemented in the customer environment.

There could be scenarios where the customer would prefer alternate sources for security matrix import other than a csv file, for example a direct interface from the Epic Database or a custom application based on their implementation.

Viewing the SubTemplate Security Matrix

The Security Matrix for **SubTemplate** once imported could be viewed using **One Identity Manager.**

To view the imported matrix

1. In **One Identity Manager** and navigate to Epic connection which was created.
2. In the **Task** menu click on **View Epic Security Matrix for SubTemplate**.

   A grid would be displayed with the **SubTemplate** and the corresponding Property values for Identity.

Assignment of the SubTemplate to Epic user accounts

The Epic user account can inherit **SubTemplates** from security matrix based on the properties mapped between the Identity and the matrix, provided that the **Is Template Update Disabled** flag for the user account is set to false.

The assignments inherited by the user from the Security Matrix has an **XOrigin** set to **Matrix**.

The User account **SubTemplate** assignments are updated in the following cases:

1. An initial import of the data into the **EPCMatrixSubTemplate** table.
2. Subsequent updated to the Security Matrix for **SubTemplate**.
3. Changes to the property values of the Identity linked to the user account.
4. Change of the Identity liked to the user account.

Customizing Security Matrix

The security matrix CSV project has two mappings. The EPCMatrixEMPTemplate mapping synchronizes the EMP Template assignment for users and EPCMatrixSubtemplate synchronizes the Subtemplate assignment for the users.

The virtual property vrtKey defined on the OneIM side and target system side, does the object matching. The vrtKey is defined as the combination of 10 properties (script vrtProperties on the OneIM end) along with the EpcRoot.

On the left side of the mapping (OneIM side), virtual script property corresponding to each property has been defined. Example we have virtual property vrtProperty01 defined corresponding to Property01 and so on. The Properties (Property01 to Property10) can be mapped to match the Identity's OneIM Org or Identity's simple field (example job title). Property column mapping is defined in the EPCMatrixColumnEMPTemplate and

EPCMatrixColumnSubtemplate tables. The virtual script properties (vrtProperty01 to vrtProperty10) by default resolves Orgs based on the Org's "**Full Path**", if the corresponding Property has been mapped to an Org and resolves to the field value in case of simple properties.

If resolution of Orgs based on Org's "**Full Path**" does not suffice the requirement, customers can resolve it differently. The read and write script of all vrtProperties can be updated according to requirements.

Appendix A

Configuration parameters for managing Epic health care system

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

Table 33: Additional configuration parameters available in One Identity Manager after the module has been installed

Configuration parameter	Description
TargetSystem|Epic Healthcare	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system Epic Healthcare. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
TargetSystem|EPC|Accounts	This configuration parameter permits configuration of user account data.
TargetSystem | EPC | Accounts | InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | EPC | Accounts | InitialRandomPassword | SendTo	This configuration parameter specifies to which employee the email with the randomly generated password should be sent (manager cost center/department/location/role, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the TargetSystem |

	EPC | DefaultAddress configuration parameter.
TargetSystem | EPC | Accounts | InitialRandomPassword | SendTo |MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The Employee - new user account created mail template is used.
TargetSystem | EPC | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The Employee - initial password for new user account mail template is used.
TargetSystem | EPC | Accounts | MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. The Employee - new user account with default properties created mail template is used.
TargetSystem | EPC | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem | EPC | PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem | EPC | PersonAutoDisabledAccounts	This configuration parameter specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem | EPC | PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem | EPC | PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: ADMINISTRATOR
TargetSytem |EPC|SubTemplateDefaultPriority	This configuration parameter specifies the SubTemplate default priority to be assigned for direct and base tree assignments. the default

	value is set to 4 and can be updated.
TargetSystem|EPC| SubTemplateMatrixPriority	This parameter specifies the SubTemplate default priority for SecurityMatrix assignments. The default value is 1 and can be updated.
TargetSystem|EPC| AutoSetAppliedEMPTemplate	If a user receives an EMPTemplate through base tree or SecurityMatrix inheritance and AutoSetAppliedEMPTemplate parameter value is 1, then the EMPTemplate is automatically set as the Applied and Default EMPTemplate for the user. The default value is set to 0 and can be updated.
TargetSystem | EPC | Accounts | NotRequirePasswor	This configuration parameter determines whether a password is generated for the user. If this configuration parameter is set to 1 then no password is generated for the user. If this configuration parameter is not set to 1 and the Initial Random Password configuration parameter is enabled, then a password is generated for the user. The default value of this configuration parameter is set to 1.

Appendix B

Default project template for Epic

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**.

Use a default project template for setting up the synchronization project initially. For custom implementations, you can extend the synchronization project with the **Synchronization Editor**.

One Identity Manager accesses the Epic healthcare target system through a web service exposed by Epic.

The various **One Identity Manager** tables that is used for mapping

Table 34: One Identity Manager schema tables for Epic Health care

Table in the One Identity Manager schema Description	Description
EPCEMPTemplate	EMPTemplate details
EPCSubTemplate	SubTemplate details
EPCUser	An EPC User details
EPCUserHasEMPTemplate	EMPTemplate assigned to an EPCUser
ECPUserHasSubTemplate	SubTemplate assigned to an EPCUser
EPCUserIdentityID	User IdentityID assigned to an EPCUser
EPCUserExternalID	External Identifiers assigned to an EPCUser
EPCUserManager	EPCUserManager
EPCUser Demographics	Demographics data assigned to an EPCUser

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

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

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

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