

How-To Guide Configuring User, User Roles and User Templates

Document Type: External

Document Version: 1.0

Date: 17/08/2021

Author: Hadhi Jawahir

Table of Contents

Introduction.....	3
Overview	3
User Role Configuration	3
Create a new User Role	3
User Role – General Tab	5
User Role – Authorised Functions Tab	5
User Role – Special Functions Tab	8
User Role – Report Functions Tab	9
User Template Configuration	9
Create a new User Template	9
User Template – General Tab	10
User Template – Roles Tab	11
User Template – Security Tab.....	12
User Configuration	13
Create a new User	14
User – General Tab	15
User – Address Tab.....	15
User – Access Times Tab.....	16
User – Associated Locations Tab	17
User – Biometrics Tab.....	17
User Group Configuration	18
Create a new User Group	18
User Team Configuration	19
Create a new User Team	20
User Team – General Tab	20
User Team – Team Customers Tab.....	21
User Team – Team Users Tab	21
Functional Authorisation Codes	22
Setting Functional Codes in User Roles	22
Configuring Tender Limits using Functional Codes.....	23
Configuring Reasons for specific Functional Codes	24
Broadcasting.....	24
POS Screens.....	25
About This Document.....	27
Current Document Version information.....	27
Document Context	27
Document Inquiries	27
Document History	28

Introduction

The purpose of this guide is to show how to configure Users, User Templates and User Roles to allow you to set up different access to meet your organization's needs.

Access covers a certain set of functions a user will be allowed to perform.

Eg: A Sales Assistant might be able to sell but not do returns, there may be tendering limits for certain groups. In order to do this, this guide walks you through on how you can define and configure your own User Roles with the set of enabled permissions (privileges), configure new Users Templates and Users, and be able to assign the User Roles to the specific Users as required.

Overview

This guide will cover the configuration for the following:

- **User Role Configuration** – to set up and assign privileges so as to assign what functions a User can have access to perform.
- **User Template Configuration** – to template a set of users with common behaviour using User Templates.
- **User Configuration** – to set the user information, passwords and individual user settings.
- **User Group Configuration** – to set up a hierarchical structure to group users for group selection such as task allocation.
- **User Team Configuration** – to set up a team of users that associates with a location and cost centre. A team manager, the users who belong to the team and the customers that the team supports are specified here as well.
- **Functional Authorisation Codes** – limiting users' tender limits and reason code limits.

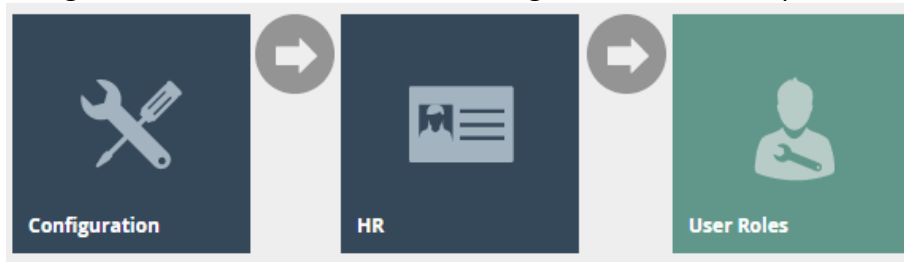
User Role Configuration

The **User Role** configuration element provides a convenient method of grouping together privileges, which may then be associated with one or more Users who require them. This way it allows certain users to access only certain functions. Eg: Returns, Loyalty, Ordering. The most basic elements of application functionality in Enactor Retail are **Functions** and these are typically associated with **Privileges** which are a requirement for access to the Function. Each function requires that a privilege is available in at least one of the User Role that is associated with the User's Account, which would grant access for the User to run that function since the Privilege has been assigned to that User. All functions and their privileges are grouped into **Processes** and these Processes are grouped into **Packages**. This is further explained in the "Authorised Tab" section.

Create a new User Role

To create a new User Role follow the steps below:

Navigate to User Role Maintenance using the Search or the path



To create a new User Role, select **Create a New User Role** on the User Role Maintenance page.

User Role Maintenance

Region: [Dropdown]
 User Role ID: Starts With [Text]
 Authorisation Level: [Text]
 Apply Filters | Reset Filters

	User Role ID	Description	Authorisation Level
	ADMINISTRATOR	Administrator	100
	ASSIST_MANAGER	Assistant Manager	50
	CENTRAL_INVENTORY	Central Inventory	60
	CRM_POS	CRM POS	10
	CUSTOMER_ORDER_MGR	Customer Order Manager (HO)	70
	GIFTCARD	Gift Cards	20
	LOYALTY	Loyalty	15
	MANAGER	Manager	60
	MANAGER_MENU	Manager Menu	60
	OPERATIONAL_ADMIN	Operational Administrator	90
	POS_ADMIN	Pos Admin	70
	POS_CASH_MAN	Pos Cash Management	40
	PRE_SIGN_IN_POS	Pre Sign In POS	20
	RESTAURANT_UK	Restaurant - UK	100

Page 1 of 1 | Page Size: 100

Create a new User Role

Select the Region from the **Region** drop-down.

Enter a unique **User Role ID** for the new User Role. The ID can be alphanumeric and contain a maximum of 20 characters and will be used to uniquely identify this new User Role. Use of a systematic and business-specific naming convention is recommended here.

We will create a User Role for Manager - Returns which would contain the privileges required to carry out return functions for all Managers as follows:

User Role Maintenance

You are adding a new User Role, please select a region and enter an ID:

Region: All Regions
 User Role ID: MANAGER_RETURNS

Back | Create

The User Role Maintenance, for the newly created User Role, is presented as follows with the 4 key tabs namely; **General, Authorised Functions, Special Functions and Report Functions**.

User Role – General Tab

The **General** Tab has the basic information that captures the identity of the new User Role and the Authorisation Level for it.

User Role Maintenance

Save

Cancel

You are editing user role ID: 'MANAGER_RETURNS' for region 'All Regions'

General

Authorised Functions

Special Functions

Report Functions

Description*

Manager - Returns

Authorisation Level*

15

* Denotes Mandatory

Set the appropriate values on the **General** Tab as follows:

Configuration	Description
Description	Enter a User-Friendly, meaningful name by which Users will be able to identify and select the Roles in other locations of the Estate Manager. The use of some systematic and business-specific naming convention is recommended. Maximum 30 alphanumeric characters.
Authorisation Level	This field allows this role to be ranked against other roles with the same privileges. A numeric value which ranges from 0-100 is to be entered here. In this scenario, the newly created Manager Role should rank higher than the Sales Assistant Role. So, the value entered here should be higher than the value assigned for the Sales Assistant Role. This way, when both the Manager and Sales Assistant use the same function, it is the Manager who is given a higher priority than the Sales Assistant.

User Role – Authorised Functions Tab

The **Authorised Functions** Tab is used to assign Privileges for User Roles in relation to the **Functions**. Each Function is associated with a **Process** and a Process is associated with an Application **Package**. This is all available for configuration in this Authorised Functions Tab as dropdown lists, so that the privileges for this User Role can be easily filtered and enabled as required.

The details of the most commonly used Application Packages are as follows:

Application Package	Description
Enactor Cash Management	Contains all cash management related functions and privileges for Estate Manager and Back Office.

Enactor POS	Contains all POS related functionalities and privileges that are accessed when using the Enactor POS.
Enactor Web Maintenance	Contains all UI related functionalities and privileges that are accessed when using the Enactor Web Maintenance.

The details of the occasionally used Application Packages are as follows:

Application Package	Description
Enactor Address Lookup Service	Contains functionalities and privileges that are required when accessing AFD, PA, Postcode, QAS and Internal Services.
Enactor Application Download Service	Contains functionalities and privileges that are required when accessing Application Download Services.
Enactor CRM	Contains all CRM functionalities and privileges such as Customer Activity Flow Service Access.
Enactor Card Payment	Contains ICC Reader related functionalities and privileges for Enactor Card Payment.
Enactor Card Payment Services	Contains all Card Payment functionalities and privileges required when accessing Card Payment Services such as authorising and refunding card payments.
Enactor Core Reporting	Contains all Reporting functionalities and privileges required when accessing Report functions such as viewing saved report and charts.
Enactor Customer Orders Maintenance	Contains all Customer Order functionalities and privileges for Estate Manager and Order Manager.
Enactor Customer Orders Retail	Contains functionalities and privileges that are required for Retail Customer Orders.
Enactor Customer Orders Processing	Contains all Customer Order Processing functionalities and privileges for running Customer Orders.
Enactor Diary	Contains all Customer Order Processing functionalities and privileges required for viewing, editing, running, removing in the Diary Entry Maintenance of the Estate Manager.
Payment Gateway - Card Services	Contains Payment Gateway Card Service functionalities and privileges for generating card tokens and bulk tokenisation.
Receipt Maintenance	Contains all Receipt functionalities and privileges required when accessing Receipt based functions in the Receipt Maintenance.

Enactor Repairs Manager	Contains all Repairs Management related functionalities and privileges for Repairs Manager.
Restaurant Maintenance	Contains all Restaurant Management related functionalities and privileges when accessing Restaurant processes.
Enactor Web Maintenance - CRM	Contains all UI related functionalities and privileges that are accessed when using the CRM related Maintenance of Enactor Web Maintenance.
Enactor Web Maintenance - Inventory	Contains all Inventory Management related functionalities and privileges that are accessed when using the Inventory related Maintenance of Enactor Web Maintenance.

Each package has a dropdown to select from a list of all available Processes, relevant to a functional area of Enactor. Eg: Discount Item, Receipt Return, Return Item.

Note: It is common for a function to have both an allowed privilege and an authorised privilege. The allowed privilege would let this User to start the function but in order to complete it, the user should also require the authorised privilege. This is further illustrated in the example scenario of the Item Returns function below.

The checkboxes corresponding to each Function can be used to enable or disable a particular function for this User Role.

The screenshot shows the 'User Role Maintenance' interface for the user role 'MANAGER RETURNS'. The 'Authorised Functions' tab is active. The 'Application Package' is set to 'Enactor POS' and the 'Process' is set to '-'. The table below lists functions with checkboxes for enabling or disabling them.

3	Package 1	Process 2	Function ID	Function Name
<input type="checkbox"/>	Enactor POS	Account Payment Item Void	enactor.pos.AuthorisesVoidAccountPaymentItem	Authorises Account Payment Item Voids
<input type="checkbox"/>	Enactor POS	Account Payment Item Void	enactor.pos.VoidAccountPaymentItemAllowed	Void Account Payment Items Allowed
<input type="checkbox"/>	Enactor POS	Account Withdrawal Item Void	enactor.pos.AuthorisesVoidAccountWithdrawalItem	Authorises Account Withdrawal Item Voids
<input type="checkbox"/>	Enactor POS	Account Withdrawal Item Void	enactor.pos.VoidAccountWithdrawalItemAllowed	Void Account Withdrawal Items Allowed
<input type="checkbox"/>	Enactor POS	Add Loyalty Points	enactor.pos.AddLoyaltyPointsAllowed	Add Loyalty Points Allowed
<input type="checkbox"/>	Enactor POS	Add Loyalty Points	enactor.pos.AuthorisesAddLoyaltyPoints	Authorises Add Loyalty Points
<input type="checkbox"/>	Enactor POS	Add Text to Item	enactor.pos.AddItemTextAllowed	Add Text Allowed
<input type="checkbox"/>	Enactor POS	Add Text to Item	enactor.pos.AuthorisesAddItemText	Authorises Add Text
<input type="checkbox"/>	Enactor POS	Admin	enactor.admin.EstateManagerButton	Estate Manager Button
<input type="checkbox"/>	Enactor POS	Admin	enactor.admin.Run	Run

Configuration	Description
Packages	Select from a drop list of available packages. Eg: Enactor POS. The various Processes and the Functions of the Enactor retail System are organised into Packages.
Processes	Dropdown selection from a list of all available Processes defined for the selected Application Package.

Enable/Disable Privileges	A fixed set of Functions and their checkboxes is presented for the selected Process. Checkboxes, which if checked, indicate the Function is enabled for this Role. Convenience options are available below the table to Enable or Disable the Function checkboxes of the selected Process all at once.
---------------------------	--

Following is an example scenario of how to enable the Allowed and Authored privileges of Item Return transactions, in the Enactor POS, for this Manager - Returns Role.

Filter the fields as follows:

Application Package > Enactor POS

Function ID > Contains, returnitem

User Role Maintenance

You are editing user role ID: 'MANAGER_RETURNS' for region 'All Regions'

General Authorised Functions Special Functions Report Functions

Application Package: Enactor POS

Function ID: Contains, returnitem

Process: -

Function Name: Starts With

	Package	Process	Function ID	Function Name
<input type="checkbox"/>	Enactor POS	Quantity Return Product Item	enactor.pos.AuthorisesReturnItem	Authorises Return Item
<input type="checkbox"/>	Enactor POS	Quantity Return Product Item	enactor.pos.ReturnItemAllowed	Return Item Allowed

☒ Enable All Displayed Functions
 ☐ Disable All Displayed Functions

Page 1 of 1 Page Size 10

You will notice there is the **enactor.pos.ReturnItemAllowed** privilege which allows to start the Item Return function and **enactor.pos.AuthorisesReturnItem** privilege which allows to complete the Item Return function.

Make sure to tick both these boxes and click Save in order to enable the Item Return function for this Manager - Returns Role.

User Role Maintenance

You are editing user role ID: 'MANAGER_RETURNS' for region 'All Regions'

General Authorised Functions Special Functions Report Functions

Application Package: Enactor POS

Function ID: Contains, returnitem

Process: -

Function Name: Starts With

	Package	Process	Function ID	Function Name
<input checked="" type="checkbox"/>	Enactor POS	Quantity Return Product Item	enactor.pos.AuthorisesReturnItem	Authorises Return Item
<input checked="" type="checkbox"/>	Enactor POS	Quantity Return Product Item	enactor.pos.ReturnItemAllowed	Return Item Allowed

☒ Enable All Displayed Functions
 ☐ Disable All Displayed Functions

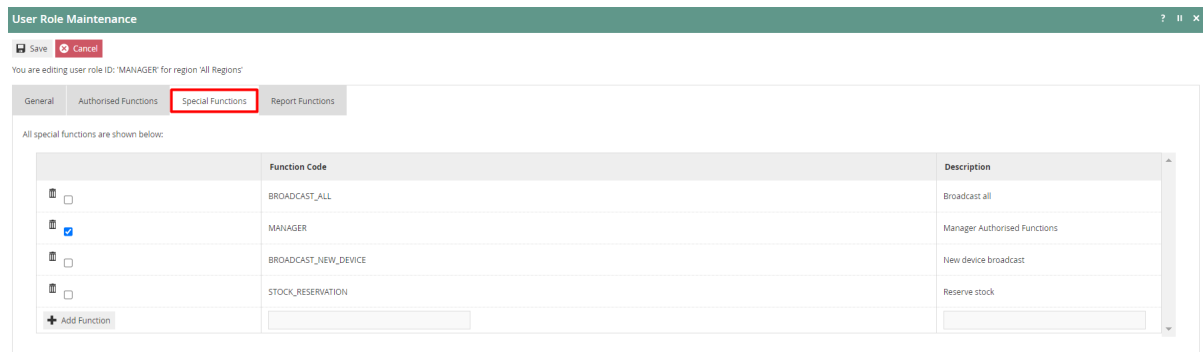
Page 1 of 1 Page Size 10

Screenshots of the usage of these privileges in the POS can be found later in the POS Screens section of this guide.

Note: Shown above is assigning only the item return privileges to the Manager – Returns Role. In a more realistic scenario, other return privileges such as tender rules and receipt returns should also be assigned to this user role.

User Role – Special Functions Tab

The **Special Functions** Tab is used to create and remove User-defined Function Codes, which are further explained in the Functional Authorisation Codes section of this guide.



User Role – Report Functions Tab

The **Report Functions** Tab is used to select one of the User-Defined Report Categories and configure permissions of the Role to enable or disable individual elements of a general set of Reporting-specific functions, which would then allow the User to manage the Reports. The Report Categories are configured using the Report Categories Maintenance and is not covered in this guide.

The User selects a Report Category in the list at the left-hand side of the page and may then enable or disable permission for the specific functions. The Enable All Process Functions and Disable All Process Functions options are available for convenience.

After configuring all the above 4 tabs, select **Save** to complete creating the new User Role.

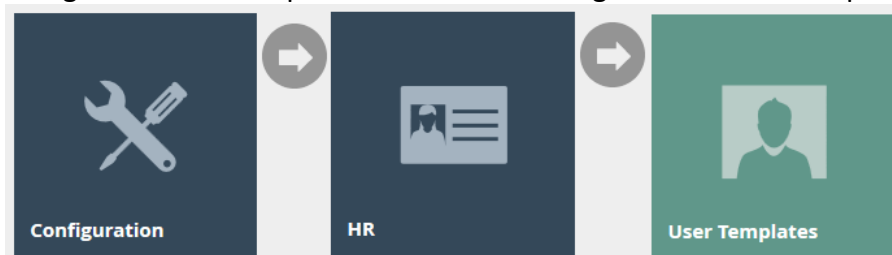
User Template Configuration

User Templates can be set up and assigned to a user, so that common behaviour can be applied to many Users. It eases and makes it convenient to create new Users since all the functional roles that were configured in the User Template applies to the new User created. A User Template can be set up for a specific type of user. Eg: Store Operator, Store Manager. This also allows users with the same roles to take advantage when a new privilege is added to a role i.e., if a new privilege to access a new area of the system is needed for a certain set of users, they will all get the change when the User Template is changed and will not have to edit each user.

Create a new User Template

To create a new User Template follow the steps below:

Navigate to User Template Maintenance using the Search or the path



User Template Maintenance

Template ID



















Starts With



Description


Starts With


Apply Filters

Reset Filters

	Template ID	Description
  	ENACTOR_ADMIN	Enactor Administrator
  	OPERATIONAL_ADMIN	Operational Administrator
  	SALES_ASSIST_UK	UK Sales Assistant
  	STORE_MANAGER_UK	UK Store Manager
  	SALES_ASSIST_US	US Sales Assistant
  	STORE_MANAGER_US	US Store Manager

 Page 1 of 1 

Page Size 10 

 Create New User Template

User Template Maintenance

User Template – General Tab

enactor®

User Template Maintenance

Save

Cancel

You are editing user template ID: 'STORE_MANAGER'

General

Roles

Security

Access Times

Associated Locations

Template Description*

Store Manager

1

Employee ID

2

Location

-

3

Locale

English (UK)

4

User Group

-

5

User Team

-

6

7

Optional

Fixed

Fixed

Fixed

* Denotes Mandatory

Set the appropriate values on the **General** tab as follows:

Configuration	Description
Template Description	Enter a User-Friendly, meaningful name by which Users will be able to identify and select the Roles in other locations of the Estate Manager. The use of some systematic and business-specific naming convention is recommended. Maximum 30 alphanumeric characters.
Locale	Select from a dropdown list of all configured Locales.
Rules for specific fields	<p>When creating a user from a template, the rules on the fields are inherited from the user template and this is where you can set such rules for each field.</p> <ul style="list-style-type: none"> Optional – The field will be optional when creating a new user. Fixed – The field will be pre-filled and cannot be changed when creating a new user. Mandatory – The field must be entered when creating a new user.

User Template – Roles Tab

The **Roles** tab allows to specify the roles, which have been configured in User Roles, for this User Template.

In the User Roles section, we have already created a User Role called “Manager - Returns” to provide privileges for all manager-based functions. So here we can assign the Manager - Returns Role to our new Store Manager User Template by ticking on the corresponding checkbox as follows:

User Template Maintenance

You are editing user template ID: 'STORE_MANAGER'

General **Roles** Security Access Times Associated Locations

The following roles are enabled for this user:

<input type="checkbox"/>	Administrator
<input type="checkbox"/>	Category Management
<input type="checkbox"/>	Central Operations
<input type="checkbox"/>	Financial Control Team
<input checked="" type="checkbox"/>	Manager - Returns
<input type="checkbox"/>	Marketing
<input type="checkbox"/>	Operational Administrator
<input type="checkbox"/>	Pre_Sign_On_Pos
<input type="checkbox"/>	Sales Advisor
<input type="checkbox"/>	Supervisor

Mandatory

User Template – Security Tab

The **Security** tab consists of security related configurations and setting up values in this User Template will save time when setting up new users. The security tab settings can also be set as optional, fixed or mandatory.

User Template Maintenance

You are editing user template ID: 'STORE_MANAGER'

General Roles **Security** Access Times Associated Locations

Preferred Authentication Method: Default 1

Single Sign-On User ID: 2

Single Sign-On Common Name: 3

Minimum Password Length: 4 4

Maximum Password Length: 20 5

Password Expiry Time (days): 0 (Zero means unlimited) 6

Force Alpha-Numeric Password: 7

Force Mixed Case Password: 8

Prevent Password Re-Use: 9

Prevent Password similar to User Id: 10

Inactivity Delay (seconds): 500 (Zero means unlimited) 11

Maintenance Inactivity Delay (seconds): 1000 (Zero means default to Inactivity Delay) 12

Training Mode: 13

Disallow Multi-Device Sign On: 14

Allow Sign-On with Card Only: 15

Skip Password Validation if Sign-On with Card: 16

Disallow Locking Multiple Pos: 17

Mandatory

Set the appropriate values on the **Security** tab as follows:

Configuration	Description
Preferred Authentication Method	Selected from a fixed drop list i.e., Default Enactor Internal or Active Directory. The integration setup for this is not included as part of this document
Single Sign-On User ID	A user ID (Alphanumeric; maximum 20 characters) which is used for linking to single sign on directory services such as active directory. The integration setup for this is not included as part of this document.
Single Sign-On Common Name	Common name for single sign on use. The integration setup for this is not included as part of this document.
Minimum Password Length	The minimum length of the password. Integer value minimum 1.
Maximum Password Length	The maximum length of the password. Integer value maximum 20.
Password Expiry Time (days) (Zero means unlimited)	Number of days until password expires. Integer value maximum 999 and 0 means unlimited.

Force Alpha-Numeric Password	Checkbox, if checked indicates that the User will be forced to use alpha and numeric characters when they change their password.
Force Mixed Case Password	Checkbox, if checked indicates that the User will be forced to use mixed case characters when they change their password.
Prevent Password Re-Use	Checkbox, if checked indicates that the User will be prevented from using a previously used password when they change their password.
Prevent Password similar to User Id	Checkbox, if checked indicates that the User will be prevented from using a password that bears similarity to the User ID.
Inactivity Delay (seconds) (Zero means unlimited)	The delay in seconds after which this User is automatically logged off the POS system. Integer value where 86400 is the maximum value and 0 means unlimited.
Maintenance Inactivity Delay (seconds) (Zero means same as Inactivity Delay value)	The delay in seconds after which this User is automatically logged off the Web Maintenance. Integer value where 86400 is the maximum value and 0 would take the value of the previous Inactivity Delay field.
Training Mode	Checkbox, if checked indicates that this User is operating in training mode and will have reduced privileges.
Disallow Multi-Device Sign On	Checkbox, if checked indicates that this User is prevented from signing onto the system at more than one location at any one time.
Allow Sign-On with Card Only	Checkbox, if checked indicates that this User can only sign onto the system with a card.
Skip Password Validation if Sign-On with Card	Checkbox, if checked indicates that password validation will be skipped if this User logs onto the system using a card.
Rules for specific fields	When creating a user from a template, the rules on the fields are inherited from the user template and this is where you can set such rules for each field. <ul style="list-style-type: none"> • Optional – The field will be optional when creating a new user. • Fixed – The field will be pre-filled and cannot be changed when creating a new user. • Mandatory – The field must be entered when creating a new user.

After configuring all the above 3 tabs, select **Save** to complete creating the new User Template.

User Configuration

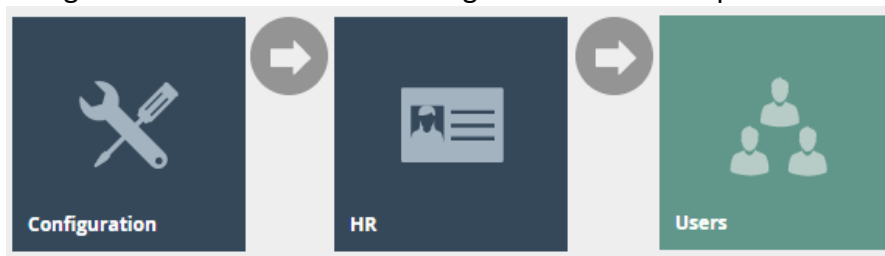
User configuration defines the User Accounts via which staff who have access to the Software Applications may Sign-On and are assigned Permissions to the Application functions they need to use. User configuration also captures information about the staff member that is required by the system.

The Maintenance of User configuration is typically a responsibility of the System Administrator. Each person requiring access to Applications of the Enactor Retail System must be identified to the system based on a User Account, which provides for authentication of the User at Sign On time and, through enabled Roles configuration, defines their access to functionality of the Applications. User configuration is maintained using the User function described following

Create a new User

To create a new User follow the steps below:

Navigate to User Maintenance using the Search or the path



To create a new User, select **Create New User** on the User Maintenance page.

User Maintenance ? || x

Location: User ID: Hide

Surname: Short ID:

Employee ID: User Team:

	Location	User ID	Surname	Forename	Short ID	Employee ID
	Enactor Store	CUST_USER				
	Enactor Store	INVENTORY				
	Enactor Store	MANAGER	Manager			
	Estate Manager	OPERATIONAL_ADMIN	Operational Admin			
	Estate Manager	ADMIN	Admin			

Page 1 of 33 Page Size: 5

Enter a unique **User ID** for the new User. The ID can be alphanumeric and contain a maximum of 20 characters and will be used to uniquely identify this new User. Use of a systematic and business-specific naming convention is recommended here.

If you wish to apply a User Template, then select it from the **Template ID** drop-down.

User Maintenance

Please enter the ID of the new user or select auto generate ID:

User ID

STORE_MANAGER_UK

Autogenerate ID

Template ID

Store Manager

← Back

+ Create

The User Maintenance, for the newly created User, is presented as follows with the 8 key tabs namely; **General**, **Address**, **Roles**, **Security**, **Access Times**, **E-mail**, **Biometrics** and **Associated Locations**.

Note: Only a few fields in General and Address tabs have to be configured since most of the remaining fields are all managed by the already selected User Template.

User – General Tab

The **General** tab captures the basic information of the new User. Here, only the Display Name and Surname are mandatory fields.

The screenshot shows the 'User Maintenance' window with the 'General' tab selected. The form contains the following fields and values:

- Display Name*: Store Manager - UK (marked with a red 1)
- Title: Mr
- Surname*: Store Manager - UK (marked with a red 2)
- Forename: Tom
- Initials: (empty)
- Date Of Birth: (empty)
- Sex: (empty)
- Left Handed: ☐
- Short ID: (empty)
- Employee ID: (empty)
- Location: Estate Manager
- Locale: English (UK)
- User Group: (empty)
- User Team: (empty)
- Template ID: STORE_MANAGER (with a 'Change Template' link)

A red box highlights the 'General' tab in the top navigation bar.

Set the appropriate values on the **General** tab as follows:

Configuration	Description
Display Name	Alphanumeric; maximum 30 characters. Enter a value that meaningfully associates with the User and by which they and other Users will recognise their User Account. This name will be displayed in screens and on receipts.
Surname	Alphanumeric; maximum 100 characters. Enter the User's Surname.


User – Address Tab

The **Address** tab captures the standard address information related to the User.

User Maintenance

 Save  Cancel

You are editing user ID: 'STORE_MANAGER_UK' based on template ID: 'STORE_MANAGER'

General	Address	Roles	Security	Access Times	E-mail	Biometrics	Associated Locations
Organisation	<input type="text"/>						
Street 1	<input type="text"/>						
Street 2	<input type="text"/>						
Street 3	<input type="text"/>						
Town	<input type="text"/>						
County	<input type="text"/>						
Country	<input type="text" value="-"/>						
Postcode	<input type="text"/> 						
Home Phone Number	<input type="text"/>						
Work Phone Number	<input type="text"/>						
Mobile Phone	<input type="text"/>						
Email Address	<input type="text"/>						

User – Access Times Tab

The **Access Times** tab allows to set times that a user can access the Enactor system.

User Maintenance

Save

Cancel

You are editing user ID: 'STORE_MANAGER_UK' based on template ID: 'STORE_MANAGER'

General

Address

Roles

Security

Access Times

E-mail

Biometrics

Associated Locations

Sunday

00 : 00 to 00 : 00

Monday

00 : 00 to 00 : 00

Tuesday

00 : 00 to 00 : 00

Wednesday

00 : 00 to 00 : 00

Thursday

00 : 00 to 00 : 00

Friday

00 : 00 to 00 : 00

Saturday

00 : 00 to 00 : 00

User – Associated Locations Tab

The **Associated Locations** tab allows to specifically add any other location that a user is to be given access to.

User Maintenance

Save

Cancel

You are editing user ID: 'STORE_MANAGER_UK' based on template ID: 'STORE_MANAGER'

General

Address

Roles

Security

Access Times

E-mail

Biometrics

Associated Locations

Associated Locations

	Location ID	Location Description
	0001	Enactor Store
<div>+ Add</div>	UK Warehouse	

User – Biometrics Tab

The **Biometrics** tab allows to enable fingerprint scanning to the User. This is not covered in this guide.

User Maintenance

Save Cancel

You are editing user ID: 'STORE_MANAGER_UK' based on template ID: 'STORE_MANAGER'

General Address Roles Security Access Times E-mail **Biometrics** Associated Locations

Biometric Data Type	

Note: The User Configurations for Roles and Security are discussed in the User Templates Configuration section of this guide.

After configuring all the above 8 tabs, select **Save** to complete creating the new User.

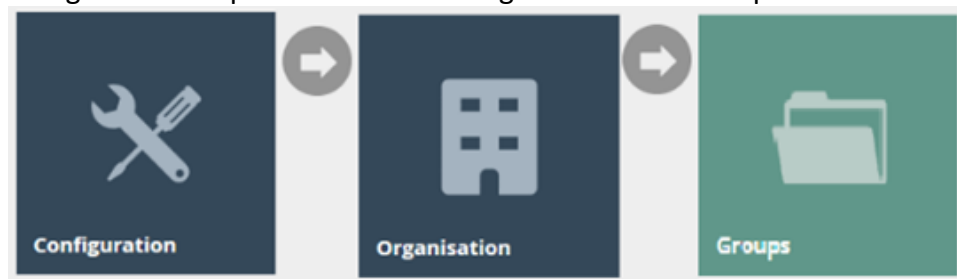
User Group Configuration

The User Group Type is a hierarchical structure that can defined with up to 10 levels, which is used to group Users for group selection like for example, in task allocation.

Create a new User Group

To create a new User Group follow the steps below:

Navigate to Groups Maintenance using the Search or the path



To create a new User Group, filter Group Type as **User Group** from the dropdown and select **Create New User Group Hierarchy** on the Groups Maintenance page.

Group Hierarchy Maintenance ? || ×

Group Type 1 Hide
 User Group

Hierarchy ID
 Starts With

▼ Apply Filters ↺ Reset Filters ⚙

Hierarchy ID	Name	Region
-	-	-

2 Page Size 10 ↺

+ Create New User Group Hierarchy ⇒ Export User Group Hierarchy

Enter a unique **Hierarchy ID** for the new User Group. The ID can be alphanumeric and contain a maximum of 20 characters and will be used to uniquely identify this new User Role. Use of a systematic and business-specific naming convention is recommended here.

Select the Region from the **Region** drop-down.

Group Hierarchy Maintenance ? || ×

Please enter an ID for the new User Group hierarchy.

Hierarchy ID SALES_DEPARTMENT

Region All Regions

← Back + Create

Once the Group Hierarchy has been created the User Group Hierarchy Edit page is available to Add, Edit or Remove Group nodes in the hierarchy as illustrated below:

Group Hierarchy Maintenance

💾 Save ✖ Cancel

You are editing User Group hierarchy ID: SALES_DEPT, for region: All Regions

📁 SALES_DEPT - SALES_DEPT

- MARKETING - Marketing
- SALES_EXEC - Sales Executives

+ Add User Group ✎ Edit User Group

After creating the User Group Hierarchy, click **Save**.

Finally, these User Groups can be assigned when creating a new User or User Template.

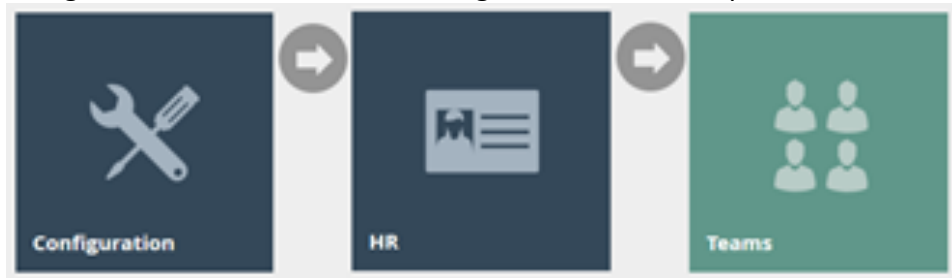
User Team Configuration

User Teams are created to be able to give the team a Name, associate it with a Location and Cost Centre, specify a Team Manager, identify the Users who belong to the Team and the Customers that the Team supports. A User Team may also be created and given just the required Identifier with no further input.

Create a new User Team

To create a new User Team follow the steps below:

Navigate to Team Maintenance using the Search or the path



To create a new User Team, select **Create a New Team** on the Team Maintenance page.

Team Maintenance

Location:

Team ID: Starts With:

Name: Starts With:

Manager User ID: Starts With:

	Team ID	Name	Location	Manager	Cost Centre ID
<input type="button" value="Eye"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	DREAM_TEAM				

Page 1 of 1 Page Size: 10

Enter a unique **Team ID** for the new User Team. The ID can be alphanumeric and contain a maximum of 20 characters and will be used to uniquely identify this new User Role. Use of a systematic and business-specific naming convention is recommended here.

Team Maintenance

Please enter following details for the new Team

Team ID:

The Team Maintenance, for the newly created User Team, is presented as follows with the 3 key tabs namely; **General, Team Customers, Team Users**

User Team – General Tab

The **General** tab captures the basic information of the new User Team.

Team Maintenance

Save Cancel

You are editing Team ID: 'TIER_1_TEAM'

General Team Customers Team Users

Name Tier 1 Team 1

Location UK Hertford Store 2

Manager Hertford Manager, 000101 - 000101 3

Cost Centre - 4

Set the appropriate values on the **General** tab as follows:

Configuration	Description
Name	Enter a User-defined, meaningful name for the Team by which Users may recognise and select it in other UIs. Alphanumeric; maximum 40 characters.
Location	Select from a dropdown list of all configured Locations.
Manager	Select from a dropdown list of all configured Users
Cost Centre	Select from a dropdown list of all configured Cost Centres.

User Team – Team Customers Tab

The **Team Customers** tab captures a List of Customers, which is list of Customers affiliated with this Team. The list is created and accumulated by selecting the Add option. Customers appear in the list with a Delete Icon, which may be used to Remove the Customer from the List.

Team Maintenance

Save Cancel

You are editing Team ID: 'TIER_1_TEAM'

General Team Customers Team Users

	Customer
	101
	102
	103
	Add

User Team – Team Users Tab

The **Team Users** tab captures a List of Users belonging to the Team. The list is created and accumulated by selecting the Add option. Users appear in the list with a Delete Icon, which may be used to Remove the User from the List.

Team Maintenance ? || x

Save Cancel

You are editing Team ID: 'TIER_1_TEAM'

General Team Customers **Team Users**

	User	Relationship ID	Relationship Name
	000101	2	Manager
	4	1	Owner

+ Add

The columns of the table depict the following:

Configuration	Description
User	Enter a User-defined, meaningful name for the Team by which Users may recognise and select it in other UIs. Alphanumeric; maximum 40 characters.
Relationship Name	This is the Relationship of the User to the Team. Enter a User-defined, meaningful name for the Team-User Relationship by which Users may recognise and select it in other UIs. Alphanumeric; maximum 40 characters.
Relationship ID	This uniquely identifies the Relationship of the User to the Team. Enter a User-defined, unique ID for this Relationship. Alphanumeric; maximum 20 characters.

After creating the User Team, click **Save**.

Finally, these User Teams can be assigned when creating a new User or User Template.

Functional Authorisation Codes

They can be created new (initially un-associated with any Application Function) in the Role Maintenance page of Web Maintenance while editing any Role. However, once created they are available for association with any other Role. Various Web Maintenance configurations provide for qualifying access to an option based on a Functional Authorisation Code. Thus, once created in Role Maintenance, they can now be associated with Functions of this type. The same Functional Authorisation Code may be used in more than one of these configurations, typically being associated with a Role that will be granted to Users who require to access the Functions they identify.

The main places this is used is to set Tender debit limits and to limit specific Reason codes to these users.

Setting Functional Codes in User Roles

In User Role Maintenance, edit a role and go to the Special Functions Tab.

To create a new Function Code, enter a Function Code and Description and click on Add Function.

User Role Maintenance

Save Cancel

You are editing user role ID: 'MANAGER' for region 'All Regions'

General Authorised Functions **Special Functions** Report Functions

All special functions are shown below:

	Function Code	Description
<input type="checkbox"/>	BROADCAST_ALL	Broadcast all
<input checked="" type="checkbox"/>	MANAGER	Manager Authorised Functions
<input type="checkbox"/>	BROADCAST_NEW_DEVICE	New device broadcast
<input type="checkbox"/>	STOCK_RESERVATION	Reserve stock

+ Add Function

Configuration	Description
Function Code	Maximum 20 alphanumeric characters. Enter a User-defined, unique value.
Description	Maximum 30 alphanumeric characters. Enter a User-Friendly, meaningful value by which Users will identify and select the Function Code in other UIs.

To set the special function for the role ensure the tick box is selected and click **Save**.

Configuring Tender Limits using Functional Codes

Tender Limits can be set on each tender for a functional code.

A sales assistant may be able to tender with a different amount to a manager.

Configuring the tender limit using the Functional Code, will limit the user if they try to tender over this limit and ask for authorisation for a manager.

To get to Tender Maintenance

Sign on to Estate Manager

Configuration → Financial → Tender

Edit the tender and go to the User Limits Tab

Add the Authorisation Code and set the user limit

Tender Maintenance

Save Cancel

You are editing Tender ID 'CASH' for Region 'United Kingdom'

General Restrictions 1 Restrictions 2 Discount Restrictions Overlap Tenders **User Limits** Cash Management Change Surcharge Cash Tender Attributes

Debit Limits Credit Limits

Enter the user debit limits for the tender below

	Authorisation Code	Amount	
	Sales Assistant	£1,000.00	
	Manager	£10,000.00	
	-		+ Add

For changes to take effect the Tender entity will need to be broadcast to the POS.

Configuring Reasons for specific Functional Codes

It is possible to limit the user of specific reason codes to users with the correct Functional Code. Eg: A transaction discount reason.

When a user tries to use this reason, they will be required to get authorisation from a user who has the correct Functional Code.

To get to Reason Maintenance

1. Sign on to Estate Manager
2. Configuration → Organisation → Reasons
3. Edit the reason to change set the Functional Authorisation Code

The screenshot shows the 'Reason Maintenance' window. At the top, there's a title bar with a green header 'Reason Maintenance' and icons for help, full screen, and close. Below the header, there are 'Save' and 'Cancel' buttons. A status message reads: 'You are editing Transaction Discount Reason ID: 'Enter Amount' for region 'All Regions''. The main area has a tabbed interface with tabs: General, Discount, Employee Discount, Modifier, Item Discounts, Transaction Discounts, Transaction Types, Price Types, Price Change Types, and Witness. The 'Discount' tab is active. The form fields include: 'Description*' with a text input 'Enter Amount Transaction Discount' and a language dropdown 'English (UK)'; 'Function Authorisation Code' with a dropdown menu showing 'Manager'; 'Capture Reference Number?' with a checkbox; 'Capture Customer Name and Address?' with a checkbox; 'Parent Reason ID' with a dropdown menu showing '-'; 'Reason Start Date' with a date picker; and 'Reason End Date' with a date picker. A footnote at the bottom left states '* Denotes Mandatory'.

For changes to take effect the Reasons entity will need to be broadcast to the POS.

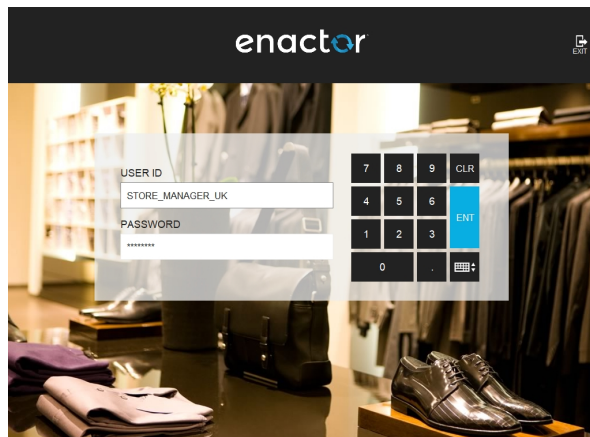
Broadcasting

To deliver all the configuration changes to the POS, broadcast the following entities.

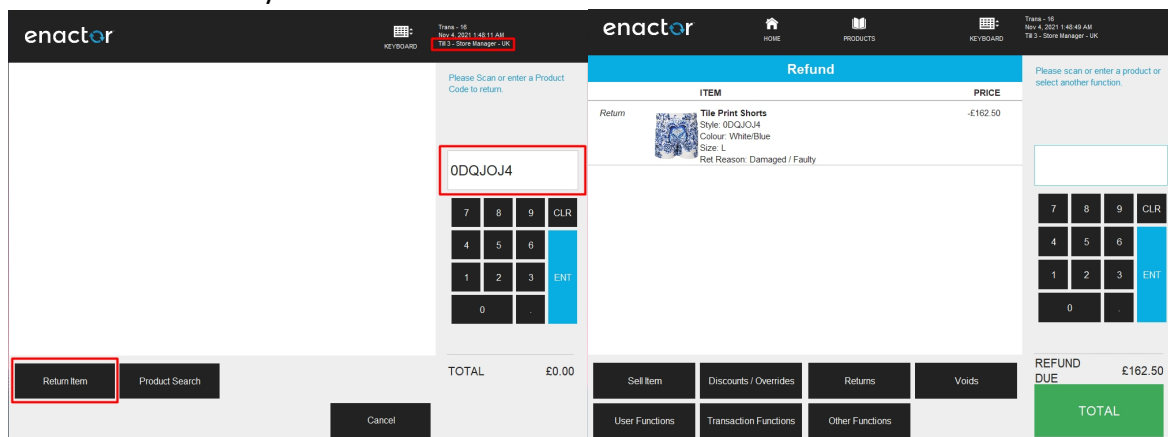
- Role
- User
- User Template
- Group
- Team
- Tender
- Reasons

POS Screens

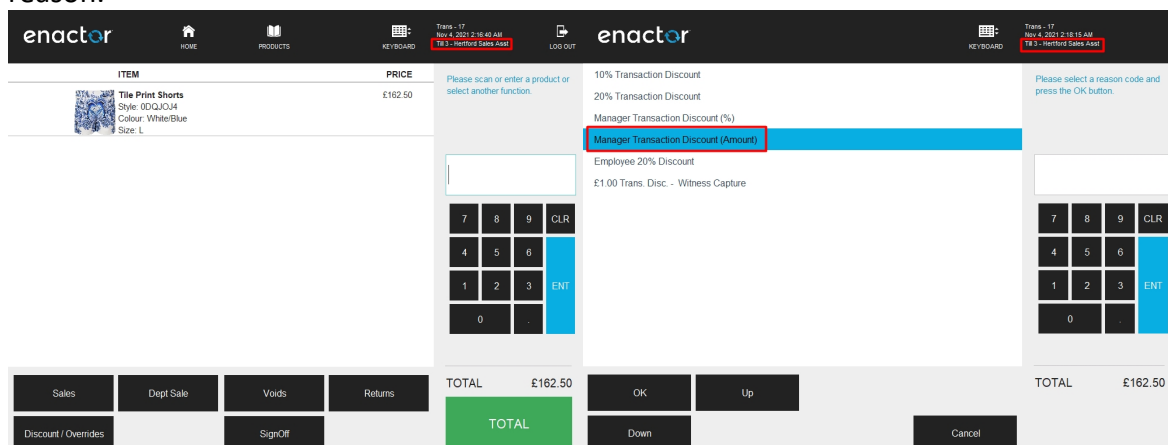
Following screen shows how we **sign on** using the **STORE_MANAGER_UK** user that we have created.



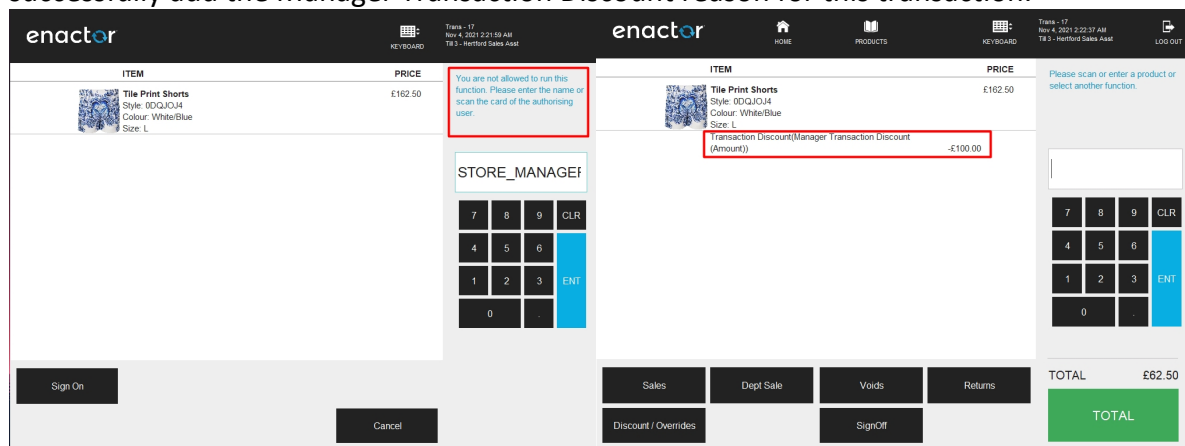
The following screens show how an **Item Return** is done using this User, which also shows that the **privileges** we have added in the **Manager – UK** role is allowing the Item Return to function successfully for this User.



The following screens show how a **Sales Assistant User** is trying to give a **Manager Transaction Discount** which has a functional authorisation code configured against this reason.



When this reason has been selected, the POS prompts for the Manager to authorise the use of this reason. We will use our **STORE_MANAGER_UK** user to **authorise** this reason, since this user's role has the functional authorisation code that matches with the one configured with this reason. After authorising with this User, the Sales Assistant will be able to successfully add the Manager Transaction Discount reason for this transaction.



About This Document

©2021 Enactor Ltd

All documents produced by Enactor Ltd are supplied to customers subject to Copyright, commercial confidentiality and contractual agreements and must not be copied or transferred without permission.

The amendment history of this document can be found in the table below.

Current Document Version information

Document Context

This document is part of the Enactor Product Documentation Series. All Enactor products include a comprehensive documentation set designed to improve understanding of the product and facilitate ease of use.

Document Inquiries

At Enactor we aspire to producing the highest quality documentation to reflect and enhance the quality of our product. If you find that the document is inaccurate or deficient in any way, please assist us in improving our standard by letting us know.

For matters of document quality or any other inquiries regarding this document please contact:

By Email: documentation@enactor.co.uk

Document History

The following versions of the document have been produced:

VERSION	STATUS	ISSUE DATE	AUTHOR	REASON FOR ISSUE
1.0	Review	19/10/20	Kevin Charlesworth	Initial version