Preface

This Guide is intended to be read by bank security officers responsible for registering Trade Innovation users and for controlling their access to Trade Innovation functionality.

# Introduction

This chapter provides an overview of the Trade Innovation system's security features.

## Overview

Access to the system is controlled by a comprehensive security infrastructure in line with industry standards. This security infrastructure can be configured to work with your bank's existing infrastructure (for example, a single sign-on system) in which case you will need to refer to that system's documentation for further details in addition to this Guide.

This Guide describes the facilities offered by the standard security system supplied Trade Innovation.

Users access the system via a log-on program. They log on using a password and a user ID, which identify a user profile. This user profile determines the level of access the user will have, to Trade Innovation zones and to the Trade Innovation system itself. When a user logs on, the system checks that the password is correct and that the user is not barred. After successful log-on, the user is presented with a list of the Trade Innovation zones to which you have granted them access. The user can then select and run an application from within that zone.

The applications they can access, and the functionality they can use within each application, is set up by you as security officer, using a combination of design features that include:

* Teams
* User roles
* Capabilities

As security officer you set up each of the Trade Innovation users and their profiles, assign them user roles, organise them into teams, and set their capabilities.

In addition, as security officer, you have access to system functionality used to set up and maintain system security parameters and zones.

## Applications

The system consists of a number of applications. The table below lists each of the applications and explains what they do. When setting up Trade Innovation users, you define which applications a user will be able to run:

|  |  |
| --- | --- |
| Application | What the Application Does |
| Batch processing | Background application used to run overnight processing. |
| Batch setup | Used to define batch processes for Trade Innovation. |
| Clean payments | Allows users to process clean payments. |
| Configuration | Used during system installation to load standard system parameters. |
| Rate fixing | Used to enter foreign exchange rates notified during business hours and to apply them to transactions awaiting rate fixing. |
| Message manager | Used to send and receive electronic messages and to control the integration of incoming electronic messages into the Trade Innovation workflow and to check electronic messages generated by the system. |
| Security | Used to control user access to the functionality within Trade Innovation. |
| Static data maintenance | Used to set up and maintain static data used by Trade Innovation. |
| System tailoring | Used to set up and maintain (among other things) product- and branch-related parameter sets that determine how transactions are processed. |
| Trade finance processing | Allows users to process trade finance transactions. |
| Supply chain finance | Allows users to process Invoices, Buyer and Seller Centric Finance, Pool based factoring and Credit Notes. |
| Departmental limits | Allows users to define limits for customer, groups and countries and enquire and report on outstanding exposures. |
| User-defined applications | These are applications defined by your bank to appear on the standard Trade Innovation application list. This is maintained in the Security application. See page 19. |

## Branches, Zones, User Roles and Teams

The Trade Innovation approach to security involves dividing your bank up into its individual legal and/or organisational components, and then arranging them into a branch hierarchy that reflects that bank's structure. If your bank has several discrete operations, each handled separately, then it can designate certain branches within its hierarchy as main banking/business entities; that branch and the branches below it in your bank's branch hierarchy are then treated as a separate business entity in the system and user access can be restricted by main banking/business entity.

Branches are organised into zones. Each zone has its own Trade Innovation database of transactions, static data and Trade Innovation users; and the branches within a zone share that database.

The parameters used to govern how the system behaves, how transactions are processed and what items are generated upon release of events can be set up at individual branch level using parameter sets. This allows different branches to process products and events in different ways, if required. (For information on setting up parameter sets see the System Tailoring User Guide – Trade Innovation.)

Whilst most of Trade Innovation's functionality runs at the level of the zone, the system also provides an overarching global layer of administration and control functionality and functionality to allow users to monitor work levels and workflow across the entire organisation. A Dashboard feature allows Trade Innovation users - input clerks, their supervisors and managers - to monitor and manage the work allocated to them and the teams to which they belong or for which they are responsible.

For each branch your bank decides what actual Trade Innovation processing functions are to be carried out there and then puts together one or more teams to handle the work. Each team is set up in the system as a collection of user roles, with each user role corresponding to an actual real-work role that a member of your bank's staff carries out in that team. Users are assigned user roles as they are assigned to teams. Teams are then linked to the branches whose transactions they will process.

Each transaction entered belongs to a particular branch - the Behalf Of branch - and can be completed only by users in teams that are linked to the Behalf Of branch. This allows your bank to limit what transactions a particular user can work on by branch. (You can go further and set up a user so that they can only work on transactions belonging to the branch that they belong to.)

Each user can be assigned to one or more teams, and can have different roles in different teams. This allows your bank flexibility in how it deploys its staff.

If a user is assigned to more than one team, one of those teams is designated their default team. When they log on to Trade Innovation, they are logged on using their default team. They can subsequently change their team in which they are working during transaction processing.

Your bank can set up users to be team supervisors, with access to information about the workload of the teams for which they are responsible. This allows them to monitor workflow using the Dashboard and (if their security settings permit) re-allocate work from one team to another.

## Controlling User Access to Trade Innovation

Two methods of controlling access to Trade Innovation functionality are employed:

* One for use with the trade finance processing application
* The other for use with all other Trade Innovation applications

### Controlling Access to the Trade Finance Application

Whether or not a user can access Trade Innovation's trade finance application is controlled by the TradeFinanceProcessing application-level capability. What they can do within that application is controlled by the user roles you assign them when you add them to teams. A user role gives a user access to each of the events they process in the course of their job, and to the relevant steps in each event's life-cycle. For example, a particular user might be responsible for processing the Input steps used to issue and to amend letters of credit, so your bank could set up a user role that permits access to just those steps for those particular events and products.

User roles are constructed using event groups. Each user role is linked to a single event group, which brings together all the events (within or across products) that a user assigned that user role will be able to work on. As you set up a user role you select the relevant event group, and then specify the step or steps at which users assigned that role can work on the events in that group. So, for each user role:

* The event group provides the events users a can work on
* The user role settings provide the steps at which they can work on them

When setting up user roles you can also specify which master-level tasks they can perform. Master-level tasks involve functionality (such as working with notes against a transaction and diary actions) that is not event-specific.

When a user logs on to the system and opens the transaction processing application, they typically start work either by using the Dashboard to view their workload, or by opening the Masters window. If they belong to only one team then they are logged on using that team. If they belong to more than one team, then they are logged on using their default team and can subsequently select the team in which to work. The team in which they are currently working controls:

* Which transactions they can work with. They can only access transactions belonging to branches linked to their current team and transactions belonging to branches below them in the branch hierarchy. In addition to this team-related restriction, individual users may be prevented from working with transactions for branches other than their own (see page 5).

Their user roles within their current team control:

* Which products and events they can work with. A user can only work with the products and events that are specified in the event groups associated with the user role(s) to which they are assigned in their current team
* The step(s) at which they can work with events
* What master-level tasks they can perform

Access to some aspects of Trade Innovation transaction processing functionality is controlled at user level. You can:

* Restrict users' access to individual events at the Input, Review or Authorise step based on the event value, using staff bands and associated limit amounts
* Define the maximum overline amount a user is to be permitted to approve, if your bank has Trade Innovation's credit risk management module implemented

### Controlling Access to Other Trade Innovation Functionality

User roles control access to transaction processing functionality. Access to other applications and functionality is controlled by:

* A user's class - these are listed in the next section
* Capabilities, which relate to functionality used for purposes other than transaction processing

Access to the transaction processing application is controlled by user roles; access to other applications is controlled by user class and capabilities.

#### User Classes

Each Trade Innovation user is set up with an indicator showing what class of user they are. Users can be defined as belonging to one of the following classes:

|  |  |
| --- | --- |
| User Class | What They Can Do |
| Help Desk | This level of user exists to allow your bank to re-enable user profiles that have been disabled because the allowed period of inactivity has been exceeded or because the permitted number of failed login attempts has been exceeded. (Profiles that have been disabled because they have reached their expiry date cannot be re-enabled by help desk users.) |
| Normal users | Normal users run Trade Innovation applications to set up and maintain system tailoring data and static data and to process transactions. |
| Operators | This level of user exists as a security feature to allow system administrators to log on with restricted access to Trade Innovation functionality in order to run overnight processing and to suspend and back up a zone. |
| Security officers | Security officers have access to the full functionality of the Trade Innovation and to all Trade Innovation applications. This includes functions used to register new users and to set up and maintain security parameters. |
| System administrators | System administrators can define zones and set the global parameters governing Trade Innovation security. |
| User administrators | User administrators can create and maintain the following classes of users in the Trade Innovation Application: Helpdesk, Normal users, Operators and other User administrators. They can also upload the restricted password list and use the application monitor. This class of users exists so that a specific user or group of users can be set up to oversee user on-boarding. |

A Trade Innovation user's class determines the extent to which a user can access functionality used to set up and administer Trade Innovation, including defining zones and users, starting and stopping the system, and monitoring user activities. Normal users and supervisors have no access to such functionality and are limited to working with the functionality provided by Trade Innovation applications.

It is possible to vary the scope of some of the user classes based on configuration options.

### Strict User Administrator Class

The User Administrator class allows specific users to be set up who are responsible for setting other users or groups of users. User administrators can create and maintain the following classes of users in the Trade Innovation Application: Helpdesk, Normal users, Operators and other User administrators.

In some cases, a bank may want to further restrict the User administrator class.

As a result, further restrictions are available for that user role through additional configuration options.

If the configuration option *override.enable.strict.user.administrator* is set then these extra restrictions ensure that:

* A user administrator cannot create other user administrators or amend their own details. This essentially means that user administrator role becomes a more specific user administrator function only so restricting what this user can do
* When a user in this class accesses Trade Innovation, the only application they will be authorised to is the Security application allowing them to only create or amend the non-security users of the system
* A user administrator may not create or change user details in Trade Innovation with security capabilities, again ensuring that security capabilities are not assigned to normal users

An additional configuration option is available to enable whether a user administrator can set or change another user’s password.

* If the configuration option *override.enable.changepassword* is set the user administrator cannot change passwords for users. This ensures that one or more security officers are responsible for maintaining passwords if the bank controls passwords through the Global application (rather than through an external authentication system). This ensures that a user administrator cannot create a user within the application, give them security capabilities, and sign on under that profile user and enter transactions.

#### Capabilities

Access to Trade Innovation applications other than the transaction processing application is controlled by capabilities. Each capability controls:

* What application the user can open. Each application has an application-level capability that must be assigned to a user for them to be able to access it when they log in
* What they can then use that application to do - certain tasks have an associated capability, and access to some menu options and buttons are also capability controlled

Instructions for downloading the capabilities are listed in Chapter 11, (see page 68).

### SOX User Administration

For bank SOX regulations for user administrators to be able to provision, modify and remove all users within an application, and have no other capability, a modified user administrator class is available.

To compliment the user administrator class, the helpdesk class is also adjusted to allow for resetting a user’s password and re-enabling user access without access to other functionality.

The approach for defining these classes is based on principle of least privilege and separation of duty.

1. If this is enabled, it takes priority over the Strict User Administrator functionality in the global application.

If the configuration option *override.enable.sox.user.administration* is set:

* A user administrator may add, modify, remove and assign zones to any class of user.
* A help desk user may enable a disabled user profile, no matter the reason, and may reset a user’s password – this means that they may select from all users that have been defined, not just those whose profile is disabled.

### Controlling What Transactions a User Can Work With

The team in which a user is currently working controls which transactions they can work with. They can only access transactions belonging to branches linked to their current team and transactions belonging to branches below them in the branch hierarchy. In addition to this team-related restriction, individual users may be prevented from working with transactions for branches other than their own.

Two optional branch settings further control what the user can do with the transactions they can access.

Users can be assigned to:

* A transaction branch. This is used as the user's default Input branch and determines the branches for which that user can enter and complete work (their transaction scope)
* An enquiry branch. This is used to allow the user to view transactions for branches other than their transaction branch for enquiry purposes; and to initiate, but not complete, events for transactions belonging to those branches (their enquiry scope)

Your bank can set up different transaction and enquiry branches for each user in each of the teams to which they are assigned.

The user's transaction branch and the enquiry branch are matched to a transaction's Input branch and Behalf Of branch in the following way:

* If a user has a transaction branch set but not locked then this branch is used as the default Input branch for a transaction and the Behalf Of branch can be set to any branch mapped to the user's current team. The user can also change the Input branch to be any branch mapped to the team, as required
* If a user has a transaction branch set and locked, then this branch is used as the default Input branch for a transaction; the Behalf Of branch can be selected only from those branches below the user's transaction branch in the branch hierarchy. The user can change the Input branch to be any other branch below their transaction branch within the branch hierarchy, if required. Events can only be completed by this user where the Input branch and the Behalf Of branch are both within the user's transaction scope. Depending on the user's enquiry scope they may be able to create events for branches outside their own transaction scope but will not be able to complete them
* If a user has a transaction branch set and locked and that branch is at the lowest level of the branch hierarchy (that is, there are no branches below it) then the Input branch and the Behalf Of branch are both set to the user's transaction branch. Depending on the user's enquiry scope they may be able to create events for branches outside their own transaction scope but will not be able to complete them
* If a user has an enquiry branch set, then they will be able to view transactions belonging to the enquiry branch and to all branches below it in the branch hierarchy. They will also be able to work on transactions for those branches, but will need to pend events rather than save them. If a user has no enquiry branch set they will be able to see transactions for all branches within the branch hierarchy (or within the main bank/business entity, where one is set)

The enquiry branch is provided to allow staff in one location to provide assistance to a customer of another branch by, for example, enquiring on the status of a transaction or initiating a new one (which would then be pended and subsequently assigned by a supervisor to the correct team for completion).

#### Supervisors

Users who are flagged as supervisors have their access to Trade Innovation transaction processing controlled in the same way as for normal users, via teams, user roles and their transaction branch and enquiry branch. In addition they can view the workload of all users in the teams to which they belong and their child teams.

If they have the capability ReassignTxns assigned to them, then they can also reassign transactions from one user or team to another.

When assigning supervisors to a team you do not need to assign them a user role. This allows you to set up users whose sole role is that of supervisor; they will be able to see the workloads of their teams, but not work on transactions.

## Registering Additional Security Officers and System Administrators

You may wish to create further users in the security officer class to whom you can delegate the day-to-day management of the system after you have completed system set-up. Any users you create in the security officer class will have identical system privileges to yours (and will be able to delete you).

You can set up a number of system administrators for different shifts or to provide stand-by cover for holiday or sickness leave. You can then use the Access Barred flag at the start and end of shifts, holidays and periods of sickness to control who can act as system administrator.

You will probably need to set up at least one user profile that can be used by system administrators to log on as an operator. This enables the system administrator to initiate overnight processing and to leave the terminal being used unattended, without the risk that another unauthorised user will be able to use the terminal in their absence.

## Registering Normal Users by a Restricted User Administrator

A typical scenario with the restricted user administrator feature set on and change password set off is as follows:

* A security officer creates one or more user administrators
* Those user administrators:
* Create users in Global application
* Create users in Security application
* Can only assign non-security capabilities to those users
* The security officer then:
* reviews the user set up to ensure correct capabilities have been assigned and
* assigns the user a password with force password change set
* The user signs on and is immediately forced to change their password before they can access the system

1. If a user administrator has both transaction and security capabilities assigned to them through capabilities or security groups then an error message is issued and the user cannot continue until this is resolved by the Security officer.

## External Security - Your Bank's Responsibility

Trade Innovation controls access to its various internal components.

It is the responsibility of your bank to:

* Define and set up the overall security environments across the platforms the system uses to meet your own security needs
* Ensure that incoming messages from the SWIFT network are adequately secure

# Getting Started

This chapter explains how to log on to the system and to the Trade Innovation security application. It also lists the security application menu options.

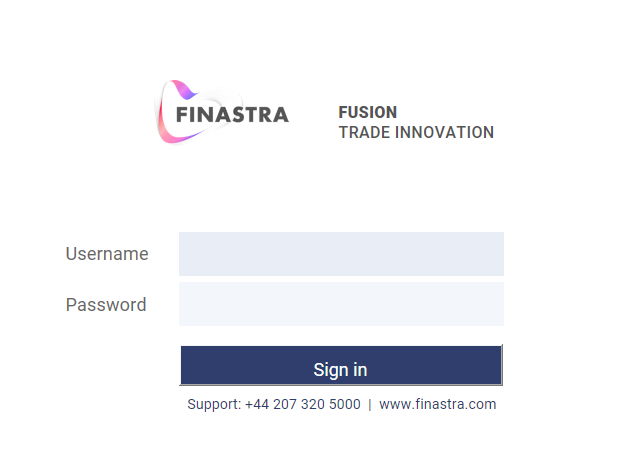
## Logging On to Trade Innovation for the First Time

Trade Innovation is delivered with a single user with security officer status. The user ID is SUPERVISOR and the password is SUPERVISOR1.

To log on as security officer for the first time, log on to a PC using the standard procedure at your bank.

Open an internet browser and type in the URL configured for the system when the software was delivered. (Your system administrator will provide this.)

The system displays a log-on window.



Enter:

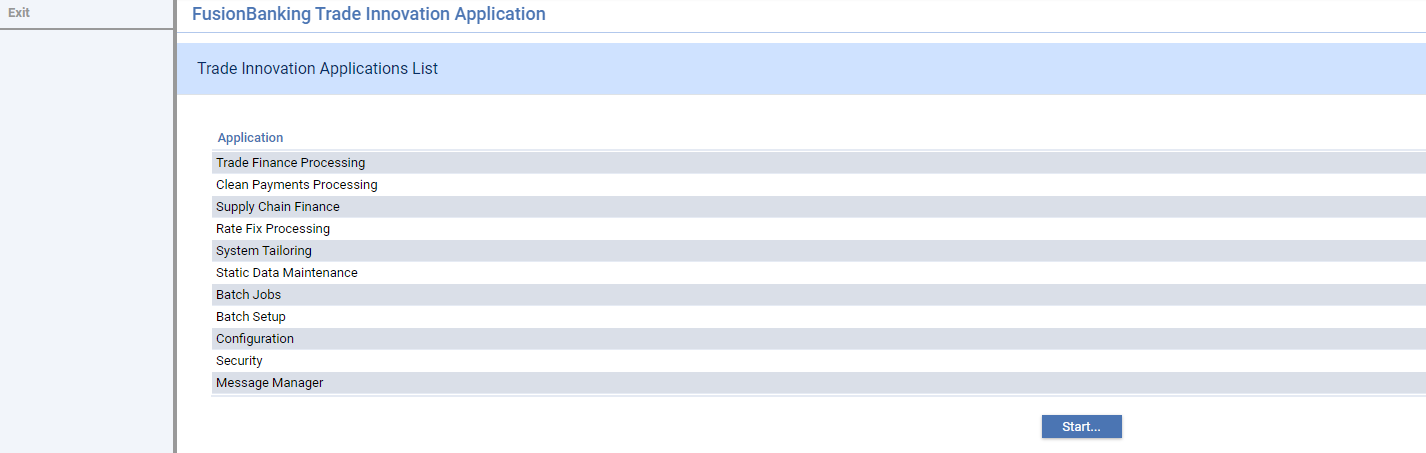
* The user name SUPERVISOR
* The password SUPERVISOR1

Then click **Sign in**.

Provided that you enter these values correctly the Trade Innovation system is accessed, and lists all the Trade Innovation zones you are authorised to use.



Select the zone in which you wish to work, then click **Start**. The system displays a list of applications available in that zone.



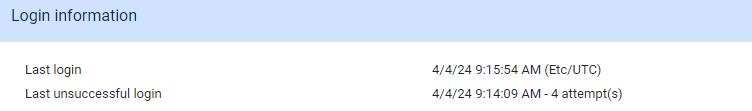
The application names displayed in this window may be modified by your bank, and thus may differ from the ones delivered.

This includes the security application. To open the application, either double-click on it or highlight it and click **Start**.

1. Finastra recommend that you change your password (see page 12) immediately, after logging on for the first time. As security officer you should be especially careful not to forget your user ID or password. If you are the only user registered with security officer privileges and you forget either your user ID or your password you will not be able to log on. You will need to apply to Finastra for assistance in regaining access to the system.

## Logging On Subsequently

When you log on subsequently, the Login information pane shows the time and date you last logged on to the system. The format used is that of the locale of the server running the software.



This allows you to check whether anyone else has tried to log on using your user profile.

The Zone list page has the following links:

|  |  |
| --- | --- |
| Link | How It Is Used |
| User administration | Used by security officers and use administrators to set up and manage Trade Innovation users. |
| Deployment administration | Used by security officers and system administrators to maintain and tune zone deployment details. |
| Zone administration | Used by security officers and system administrators to set up and maintain zones. See the Business Operations Guide – Trade Innovation. |
| Application monitor | Used by security officers and system administrators to control access to the deployments, servers and zones running on them. Also, to list the users currently accessing them, to send them messages and to forcibly log them out, when necessary. |
| Restricted passwords | Allows you to set up a list of words and character strings that users are not allowed to use (see page 17 ). |
| Change password | Used to change your password (see page 12). |
| Who am I? | Displays a window that shows login information, your authorisation level and the date when your password will expire. |
| Global application parameters | Used to control general settings such as password requirements (see page 14). |
| Logout | Logs you off the system (see page 10). |
| The Trade Innovation Zone list section has the following buttons: | |
| Start | Used to start work in a zone - see the previous section. As security officer, you can use this button at any time, regardless of the status of the zone (provided it is online). Normal users cannot use this button if the zone is suspended or closed – required for running certain configurations of overnight processing. |
| Refresh | Refreshes the information being displayed. Use this button to refresh the data shown each time you return to the Zones List window. |

## Logging Off

To log off from Trade Innovation, close the security application using the Exit link. Then click on the Logout link in the Zones List window to close the system.

The system prompts you to confirm log-off.

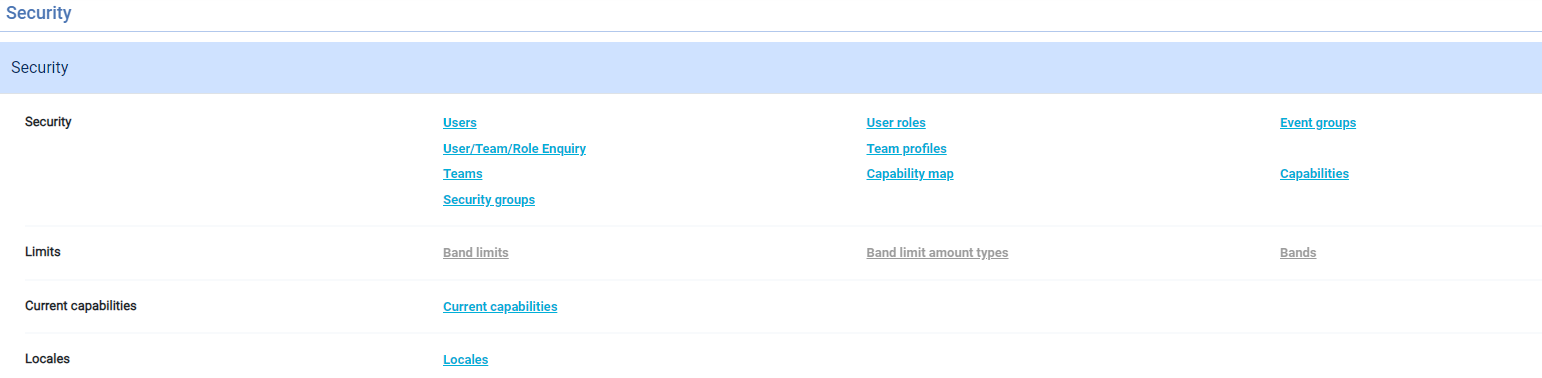
Logging off closes all your sessions in all zones.

1. It is also possible to log off using the link available on the Finastra dropdown menu. However if you are in the middle of a transaction, all unsaved changes will be lost.

## The Trade Innovation Security Application

The list of applications displayed when you log on to the system includes the security application.

Click on this application to open it. The system displays the menu window, which is the starting point for security management within Trade Innovation.



The following table shows the menu options in the Trade Innovation security application:

|  |  |  |
| --- | --- | --- |
| Menu Option | Sub-Option | What They Do |
| Security | Users | Allows you to set up and amend Trade Innovation users and assign them to security groups. |
|  | User Roles | Allows you to set up user roles (see page33). |
|  | Event Groups | Allows you to set up event groups (see page 31) |
|  | User/Team/Role Enquiry | Allows you to view what access you and other Trade Innovation users have to the system (see page 62). |
|  | Teams | Allows you to set up teams (see page 36). |
|  | Team Profiles | Allows you to set up team profiles. |
|  | Security Groups | Allows you to set up and amend security groups and assign users to them. |
|  | Capability Map | Allows you to define which capabilities users and groups are to be authorised to use (see page 52). |
|  | Capabilities | Allows you to set the default availability mode for capabilities (see page 50). |
|  | Limit Identifiers | Allows you to set up the supervisor password necessary if your system has implemented Trade Innovation's credit risk management module |
| Limits | Band Limits | Allows you to set the amount limits used to control access to events against staff bands (see page 58). |
|  | Band limit amount types | Allows you to identify events to be subject to limit checking and the fields to be used in comparison with staff band limits (see page 58). |
|  | Bands | Allows you to set up staff bands (see page 56). |
| Current Capabilities | Current Capabilities | Lists the capabilities you are authorised to use (see page 49). |
| Locales | Locales | Allows you to set up locales (see page18). |

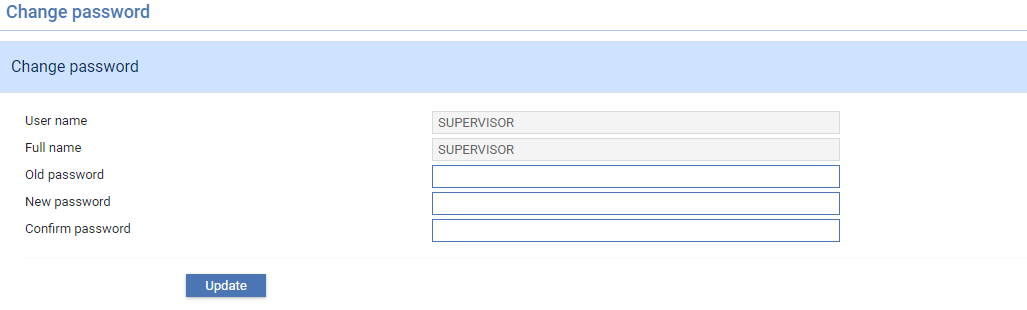
## Password Management

If the system has been configured so that Trade Innovation provides password management, then a user may change their password using the Change password link once they have successfully logged in.

The password must conform to the configuration settings defined by the security officer.

### Changing Password

You are required to change your password after your password has been reset, and at regular intervals (for example, when the maximum number of days a password can remain valid is reached). Security officers can also force a change of password on an ad hoc basis. You can also choose to change your password using the system Change password link from the Zones list page, in which case the system displays the Change password page.



The length and format of the password is defined by your bank, as are the rules on how often you are allowed or required to change password. The system keeps a history of the last five passwords you have used, and will not allow you to reuse an old password until it has been replaced in this history. Your bank can also set up a list of words and character strings that cannot be used as passwords.

As security officer you should be especially careful not to forget your user ID and password. If you are the only user registered as a security officer and you forget either your user ID or your password you will not be able to log on and will need to apply to Finastra for assistance in regaining access to the system.

### Passwords and Access to the System

As security officer, you are responsible for setting and maintaining various parameters used to control user access to Trade Innovation.

For passwords you are able to define, among other things:

* How often a user must, or is able to, change password
* The minimum and maximum length of a password
* Whether passwords are case sensitive and, if so, whether they must include upper case characters
* Whether passwords must include at least one numeric character
* Whether special characters are allowed and, if so, which ones
* The number of failed log-in attempts a user can have before being blocked from logging on
* The number of passwords to hold in the password history for a user

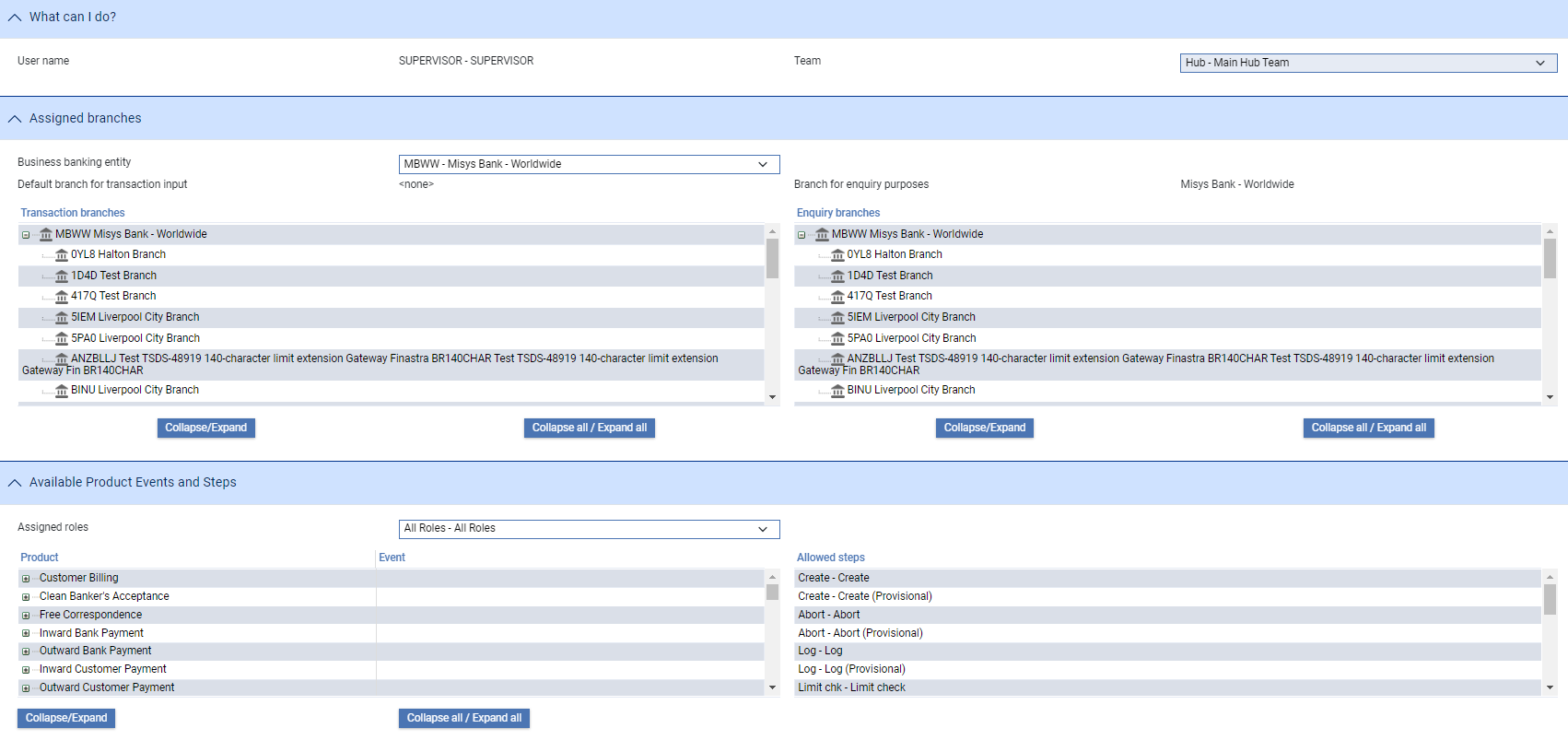
You can define whether users are to be allowed to have more than one concurrent Trade Innovation session open at a time and, if so, how many.

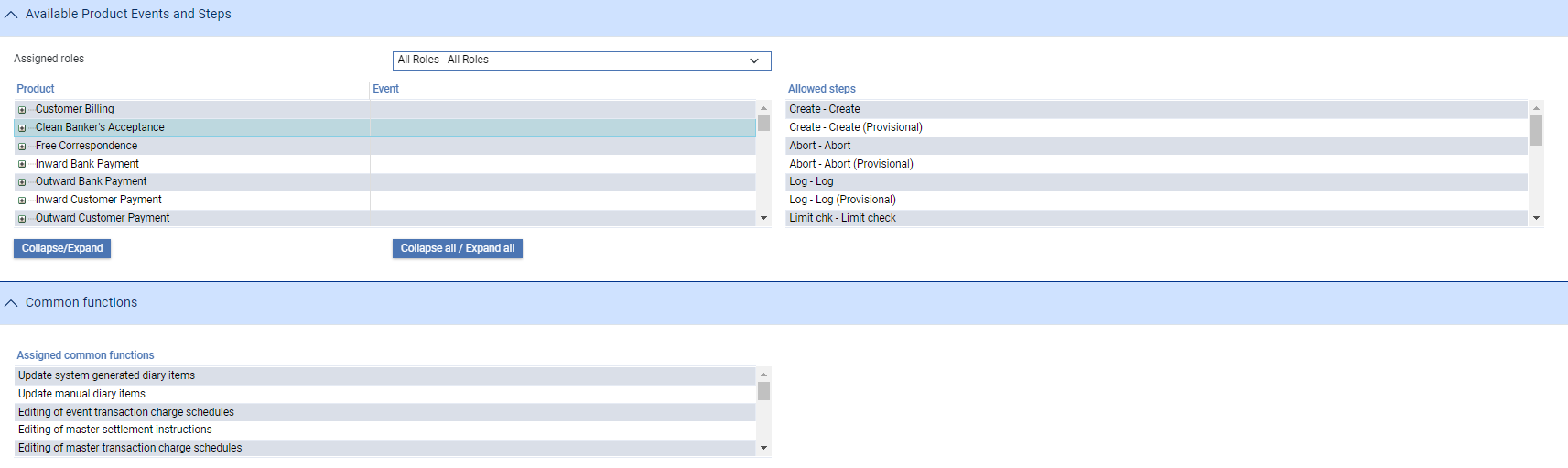
For each individual user you can set an expiry date, after which they are flagged as inactive and therefore should be removed from the system. In addition you can define how much time needs to elapse since a user last logged off before they are considered inactive.

## What Can I Do?

Trade Innovation's What Can I Do link in the security application's menu window displays a window that shows you to see which teams you belong to, the user roles you have within the team and the branches for which you can enter transactions.

The window that opens shows the user name you used to log in.





The Teams drop-down field lists all the teams you are assigned to. Once you select a team the Business Banking Entity drop-down list is populated with the business/banking entities that the team is associated with. Once you select a team and business banking entity the columns in the Assigned Branches pane show information for the selected combination:

* The Transaction Branches column lists all the branches whose transactions you can work on
* The Enquiry Branches column lists all the branches whose transactions you can view but not work on

The Available Products Events and Steps pane includes a drop-down list of the user roles available to you for the selected combination. When you select a user role, the Available Product Events and Steps pane shows information on the products and events that user role allows you to work with, and at what steps. The Common Functions pane lists the master-level tasks the user role allows you to perform.

This same functionality is available to you as security officer via the Security|User/Team/Role Enquiry menu option, but is extended to allow you to view information for all users (see page 62).

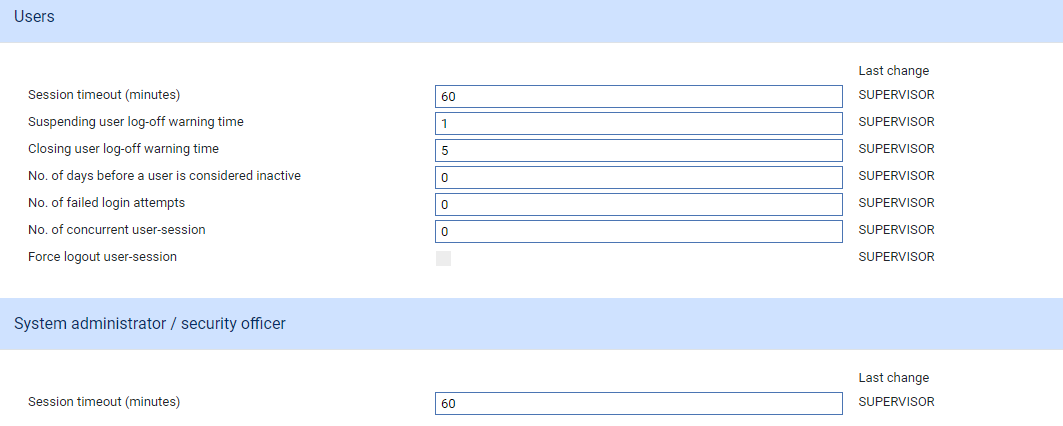
# Global Parameters

This chapter explains how to set security parameters that affect Trade Innovation processing across all zones.

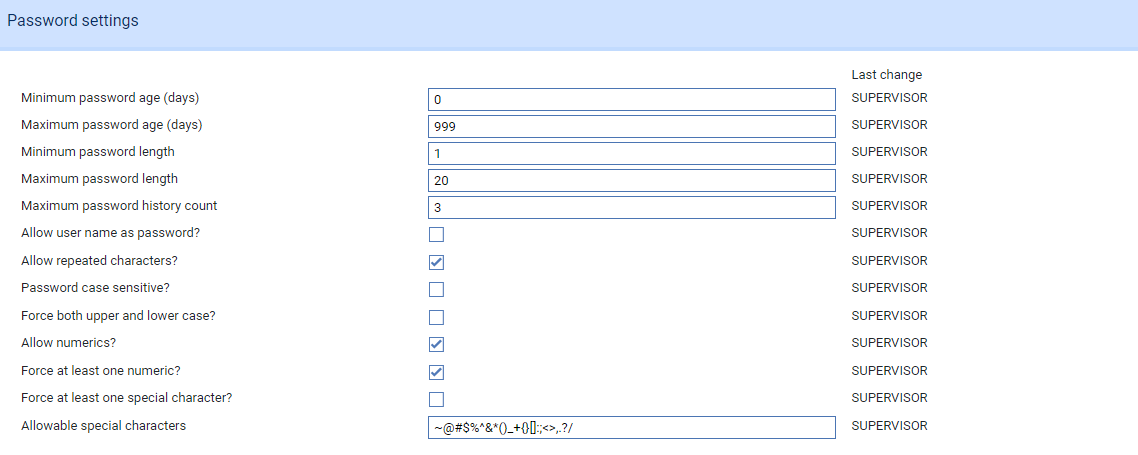
## Setting Global Parameters

Global parameters are set using the Global application parameters link.

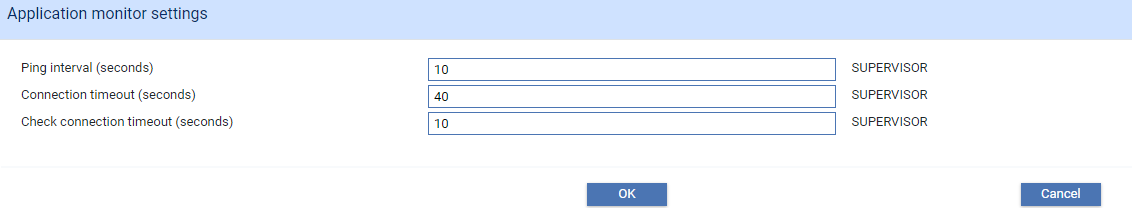
The first set of parameters is to do with user settings:



If Trade Innovation has been configured to manage user passwords, then the following parameters are shown:



Finally parameters associated with the application monitor:



The following table explains what each of the fields in this page controls. For each parameter, the system ID of the user who made the last change and when it was changed are in brackets:

|  |  |
| --- | --- |
| Field | What it Controls |
| Session timeout (minutes) | Defines the number of minutes users can leave their use of Trade Innovation before being forced to re-access the system.  Enter either the number of minutes here or 0 (zero) if you don’t want the session to timeout. Note that any sessions created and not destroyed via logging off will not be reclaimed by the application server.  You are able to set two different session timeout values - one for security officers and system administrators, the other for normal users and operators. |
| Suspending user log-off warning time | When a zone, deployment or server is suspended for any reason (using the Suspend button), the system produces a warning message that goes out to all users logged on to that zone, deployment or server, advising them that the system is suspending and that they should save their work. The warning message includes the number of minutes users have to save their work. This field defines the number of minutes users will have between this message being issued and actual suspension of the system. The default value is 1 minute.  If the value is greater than a minute, a second warning is produced one minute before suspension takes effect. |
| Closing user log-off warning time | If the overnight processing or rate fixing configuration has been configured to close the system before commencing, then when the system administrator starts either of these processes, the system produces a warning message that goes out to all users logged on to that zone, advising them that the system is closing and that they should save their work. The warning message includes the number of minutes users have to save their work. This field defines the number of minutes users will have between this message being issued and actual suspension of the system. The default value is 5 minutes.  A second warning is produced one minute before the zone is closed. |
| No. of days before a user is considered inactive | Defines the maximum number of calendar days a user can remain logged off the system before being flagged as inactive. You can define this period using a value in the range 0 - 999.  If you enter 0, users will never be flagged as inactive.  This field does not apply to system administrators and security officers. |
| No. of failed login attempts | Defines how many log-on attempts users will be allowed before being barred automatically. |
| No. of concurrent user-session | Defines the number of concurrent sessions a user is allowed to open before the system prevents new sessions from being opened. You can enter a value in the range 0 - 9. The value entered here indicates the number of sessions a user can have running at the same time; when that number is reached the system will prevent any new sessions from being opened by that user.  If you enter 0, there will be no restriction on the number of concurrent sessions a user can have open. |
| Force logout user-session | This field may be checked if the No. of concurrent user session is set to 1. If you check this field, users will be prevented from having more than one session open. If this field is checked, when a user attempts to open a second session, they will be given the option of logging off from the session they already have open. |
| Minimum password age (days) | Defines the minimum number of days a user must wait after changing their password before being able to change it again. You can enter a value in the range 0 - 999. If you enter 0, users will be able to change their password as often as they wish.  The value in this field should not be greater than the value in the Maximum password age (days), unless Maximum password age (days) is set to zero. This is to allow users to change their password on, or before a forced password change comes into effect.  The setting of this field does not affect system administrators and security officers, who will be able to change password as often as they want. |
| Maximum password age (days) | Defines the maximum number of days a user's password remains valid, after which they are forced to change it. If you enter 0, users will not be required to change their password. |
| Minimum password length | Enter the minimum number of characters the password must contain. This must be 1 or more. |
| Maximum password length | Enter the maximum number of characters the password must contain. This must be 20 or less, and equal to or greater than the value in the Minimum password length field. |
| Maximum password history count | Enter the number of passwords that should be stored in the password history for each user. This must be between 1 and 12. The default is 3. |
| Allow user name as password | Checking this field means that users will be able to use their Trade Innovation user name as their password. |
| Allow repeated characters? | Checking this field means that passwords will not be allowed that consist only of a string of the same, repeated, character (for example 'aaaaaaaa'). However strings containing repeated characters will be allowed, provided the string contains at least one other character (for example 'aaaaaaa1'). |
| Password case sensitive? | Checking this field means that passwords will be case sensitive. |
| Force both upper and lower case? | This field is relevant only if you have checked the previous field. Checking this field means that passwords will need to have a mixture of upper-case and lower-case characters. |
| Allow numerics? | Checking this field means that passwords are allowed to include numeric characters. |
| Force at least one numeric? | Checking this field means that passwords must include at least one numeric character. |
| Force at least one special character? | Checking this field means that passwords must include at least one special character. Special characters are defined using the next field. |
| Allowable special characters | Defines the special characters that are permitted in passwords. Special characters include the space character and the following characters:  ~ ` ! @ # $ % ^ & \* ( ) \_ + { } [ ] : ; " <> ' , . ? /  You can edit this list. |
| Ping interval (seconds) | Enter the number of seconds that the global application will send a ping message to all connected servers to check their connection. Enter a value between 10 and 999 seconds. |
| Connection timeout (seconds) | Enter the number of seconds that a server will use to determine if its connection to the global application has timed out. This time is compared to the last time a message was received from the global application (e.g. ping message). Enter a value between 10 and 999 seconds. It is advisable that this value be at least twice the ping interval. |
| Check connection timeout (seconds) | Enter the number of seconds that a server waits between checking whether the connection has timed out. Enter a value between 10 and 999 seconds. It is advisable that this value be at least the ping interval, and not more than the connection timeout value. |

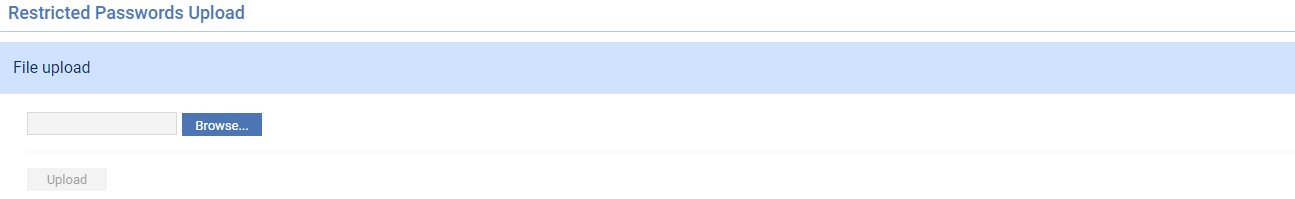
## Setting Up the Restricted Passwords List

Trade Innovation permits your bank to maintain a list of words and character strings that users are not allowed to use as passwords. Each time a user enters a new password, the value they enter is compared to entries in the list and, if a match is found, the user is prevented from using that value as a password.

These words and strings are set up in a text file using a suitable editor such as Notepad.

Each proscribed word or character string is typed on a separate line, and each of the lines must have the required number of characters to qualify as a valid password in your system. That is, if you have configured the system so that passwords must be a minimum of three characters, then each of the entries in your table must be at least three characters long. Similarly, entries must not exceed the maximum length set up for passwords on your system.

When you have completed your text file, it is loaded into the system using the Restricted passwords link from the Zones list page.

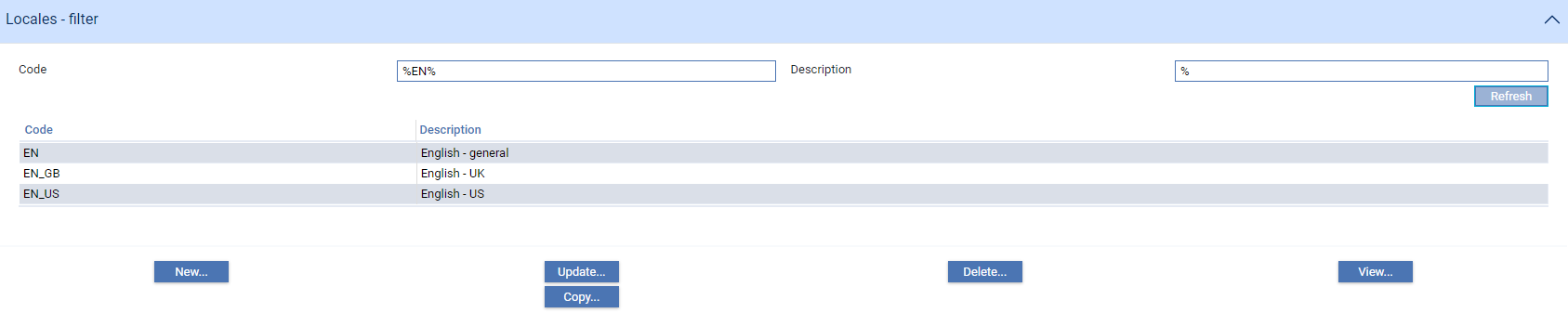


Use the Browse button to locate the text file and click **Upload**. Provided the text file is in a valid format and the entries in it the right lengths, the file is uploaded into the system and goes into immediate use. As you upload a file it replaces the previous one completely. Existing passwords are not affected.

## Locales

Locales define a user's geographical location and language. They consist of a two-character ISO country code and a two-character ISO language code, and are defined as part of the installation process. During run-time, they determine, for example, the character set and date format to be used.

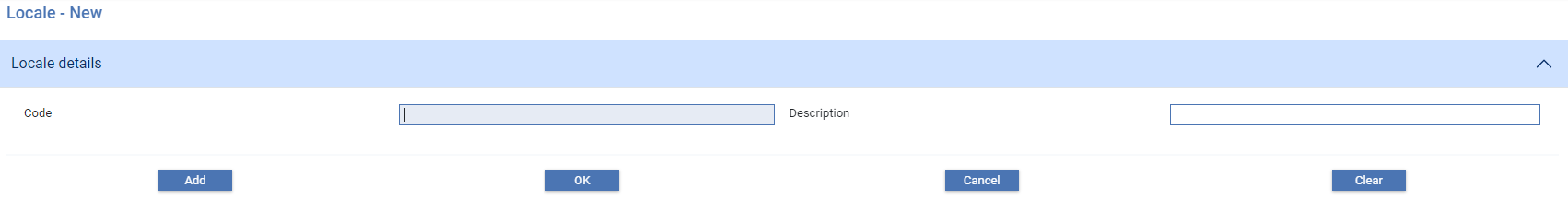
The system permits you to add to the list of locales set up during installation, and to amend or delete items in the list. This is done using the security application's Locales|Locales menu option.



You can use the window that is displayed to view, create, copy, amend and delete locales in the usual way.

To create a new locale click **New**.

### Setting Up a New Locale



Use the Code field to enter the language code, then the country code. The two codes must be separated by an underscore character, for example:

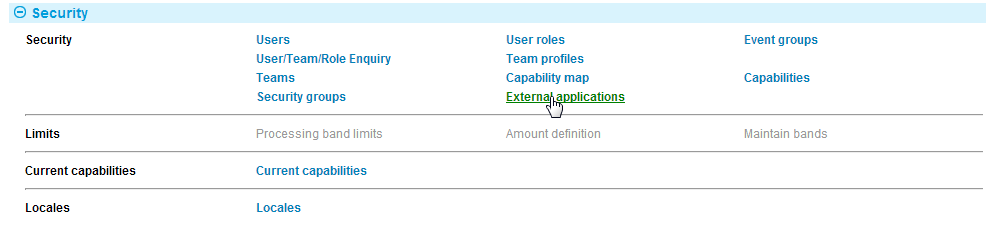
EN\_GB

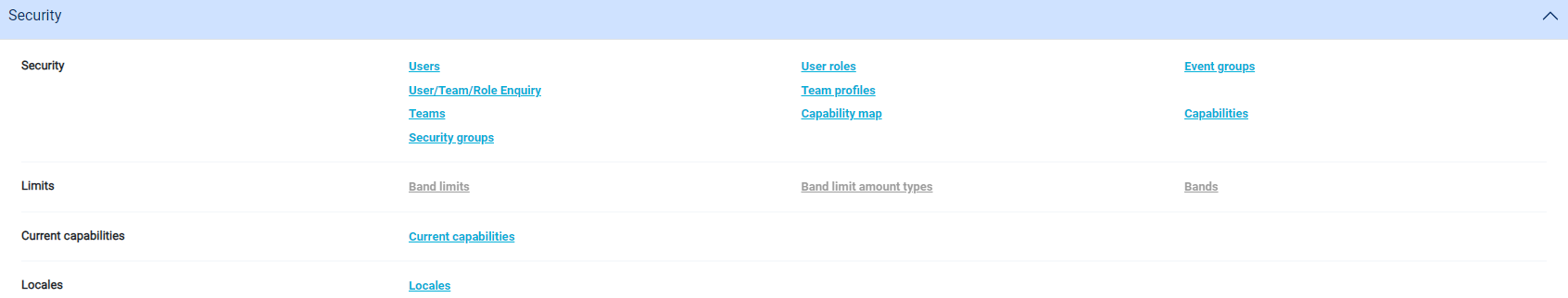
# External Applications

This chapter explains how to setup and maintain external applications.

Trade Innovation users can be allowed to access external applications in Trade Innovation. When configured, users can use the Trade Innovation application list to quickly launch other system application links.

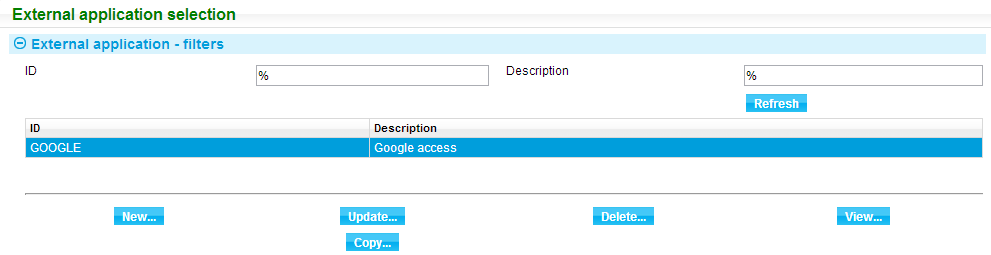
You can setup external applications clicking the Security application and then using the menu option Security|External application.





The External application screen is displayed showing all of the external links that you have configured. From here, you can:

* Create a new external application link
* Create a new external application link based on an existing link
* Update an external application link
* Delete an external application link

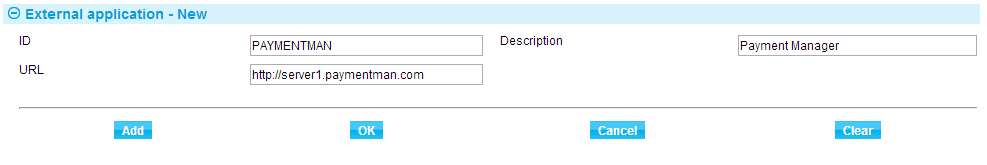


You can also filter your external application list by ID or by Description by clicking **Refresh**.

Select an external application and click **View** to display the details.

## Setting Up External Applications

You can create a new external application link either from scratch or based on an existing external application. To create a new external application, click **New**.



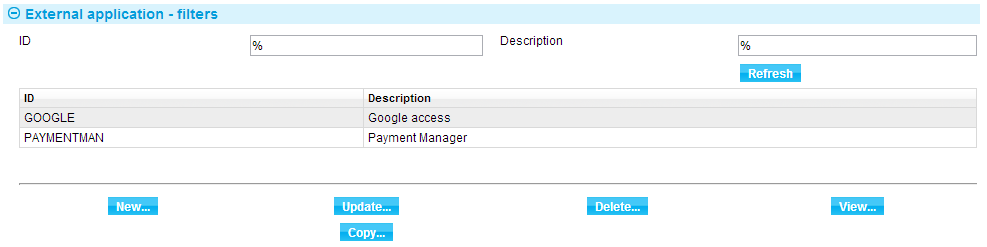
The following table explains what to enter into each of the fields in the window displayed to define a new external application:

|  |  |  |
| --- | --- | --- |
|  | Field | What to Enter |
|  | ID | The external application’s unique ID. |
|  | Description | The description of the external application. This field is used to define what is shown on the Trade Innovation application list. |
|  | URL | URL to the external application. |

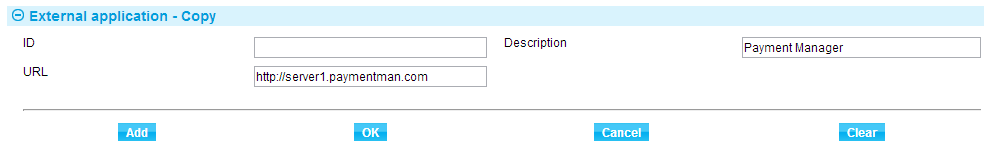
Click **OK** to save the external application.

Click **Add** to save the external application and add a new one.

The external application created is now added to the list.



To create a new external application based on an existing link, select the external application that you want to copy then click **Copy**.



Enter the ID of the new external application and modify the other fields as needed. Click **OK** to save the external application.

Click **Add** to save the external application and create a new copy.

### Required Capabilities

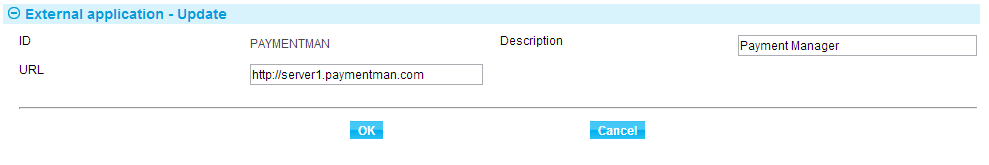
For each external application defined, a capability with the prefix ‘ApplicationList’ and the application ID as the suffix is also created.

For example: ApplicationListPAYMENTMAN

The capability must be made available for public access to display it in the Trade Innovation application list. To do this, see page 51.

## Updating External Applications

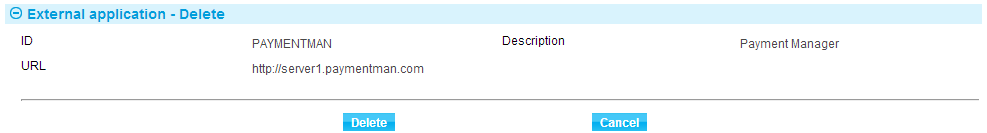
To update the fields of an external application, select the external application from the list then click **Update**. From the screen that is displayed, you can change the Description and URL field but not the ID.



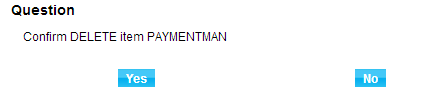
Click **OK** to complete the update.

## Deleting External Applications

To delete an external application, select the external application from the list then click **Delete**. A summary window is displayed showing the details of the selected external application.



Click **Delete** and a confirmation screen is displayed. Click **Yes** to delete.



The capability assigned to this external application is also deleted.

## Launching the External Application

When a user selects an external application from the Trade Innovation application list that system is accessed for use by the user. At this point the control is passed from Trade Innovation to that application. When the external application is closed control is not passed back to Trade Innovation. In other words the user cannot return back to the Trade Innovation application list unless the external application provides a means to do so - for further information see the *SDK - Systems Integration Guide* – Trade Innovation.

# Users

This chapter explains how to set up users:

* At the global level, so that they can log on to Trade Innovation
* Within Trade Innovation, so that their access to Trade Innovation functionality can be defined

## Registering Users

Trade Innovation users are registered in two stages, using the Trade Innovation security functionality and the Trade Innovation security application.

First, the user is set up at the global level, the level at which their access to the actual system is controlled. This involves defining which zones they can work in.

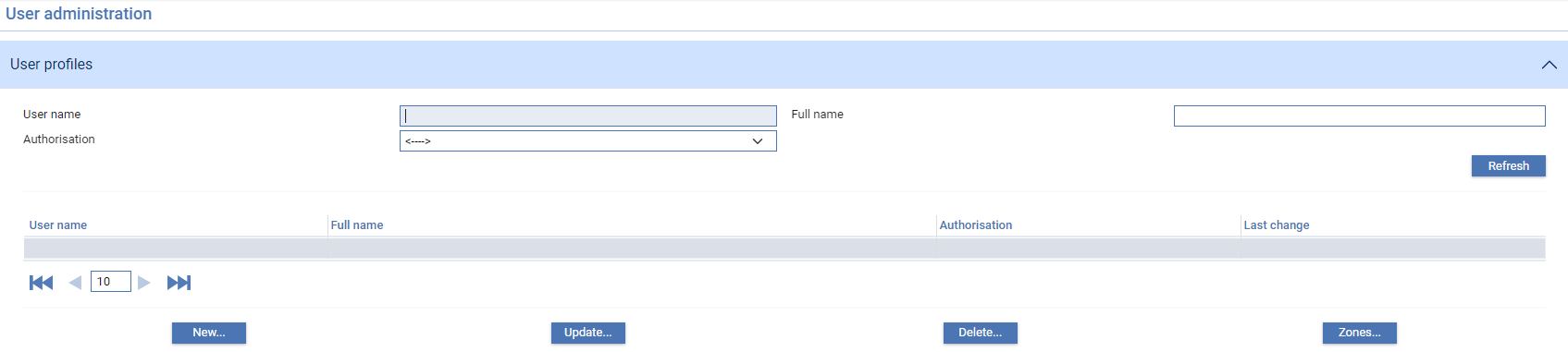
The user is then set up as a Trade Innovation user within the system in each of the zones in which they will work. Once this is done, you can define which specific Trade Innovation functionality each user can use by:

* Allocating them to user roles within teams (see page 27)
* Allocating them to security groups and/or staff bands (see page 25)

1. It is not mandatory to set the user up in this sequence.

## Setting Up a New User at the Global Level

Select the Trade Innovation system's User administration link.



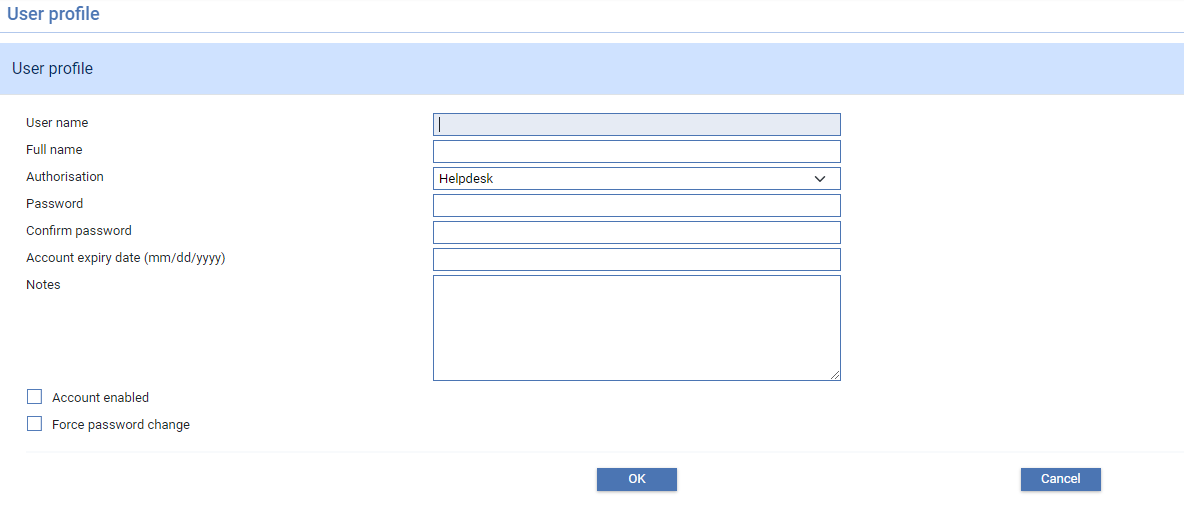
The first time you enter the page, no users will be shown. Click **Refresh** and you will be the only user listed in it. As you use the window to register users, it will list all registered users by their user ID and name. Subsequently it will list all the users registered on your system and you will be able to select user details for amendment and deletion. Special considerations apply when you delete user details.

The Zones button allows you to define which zones users will be able to access (see page 24).

To register a new user, click **New**.

The controls on the bottom right of the table provide the means to navigate through the list of users a page at a time. The controls are: first page, previous page, number of rows per page, next page and last page. The maximum number of rows per page is 50.

### Registering a New User



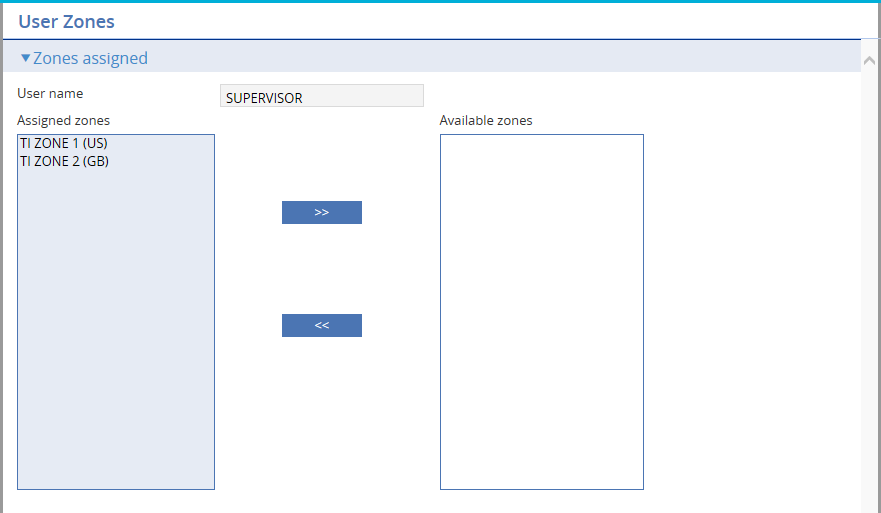
The following table explains what to enter into each of the fields in the window displayed to define a new user:

|  |  |  |
| --- | --- | --- |
|  | Field | What to Enter |
|  | User Name | The user's unique ID. |
|  | Full Name | The user's full name or job title, or any such narrative information, depending on your bank's procedures. |
|  | Authorisation | Select whether the user is a normal user, a security officer, an operator, a system administrator, a user administrator or a help desk user. |
|  | Password | Enter an initial password for this user. The length and format of the password are governed by global parameters (see page 14). The system keeps a history of the last passwords used for each user profile. If you are amending this value, the system will not allow you to reuse an old password until it has been replaced in this history. |
|  | Confirm Password | Re-enter the initial password for this user to confirm it. If the values entered in this and the previous field do not match the system will issue an error message when you attempt to save the new user details. |
|  | Account Expiry Date | The date on which the user profile will expire, if relevant. Once this date is reached, the user will no longer be able to log on using this profile.  This field cannot be set for security officers. |
|  | Notes | Any additional information about the user or user profile. |
|  | Account Enabled | Checking this field enables the user's account and allows them to start using the system. |
|  | Force Password Change | For a new user, check this box. This forces the user to change password next time they log on. |

1. The password related fields will only be shown if the application is configured to manage user passwords.

### Granting and Removing Access to Zones

Once you have registered users, you can define the zones each user will be allowed to access. This is done from within the User Profiles window. Select the user for whom you want to grant access to zones and click **Zones**.



The Available zones column lists all the Trade Innovation zones to which the user has not been granted access. The Assigned zones column lists all the Trade Innovation zones to which the user has been granted access. You can also grant a user access to a defined external or proxy zone.

To grant the user access to a zone select the zone in the Available zones column, then click the  button. The user is then granted access to that zone, and the zone is removed from the Available zones column and displayed in the Assigned zones column to reflect this.

To remove the user's access to a zone, select the zone in the Assigned zones column, then click the  button. The user's access to the zone is removed, and the zone is moved from the Assigned zones column to the Available zones column to reflect this.

Any amendments you have made to a particular user's access take effect immediately.

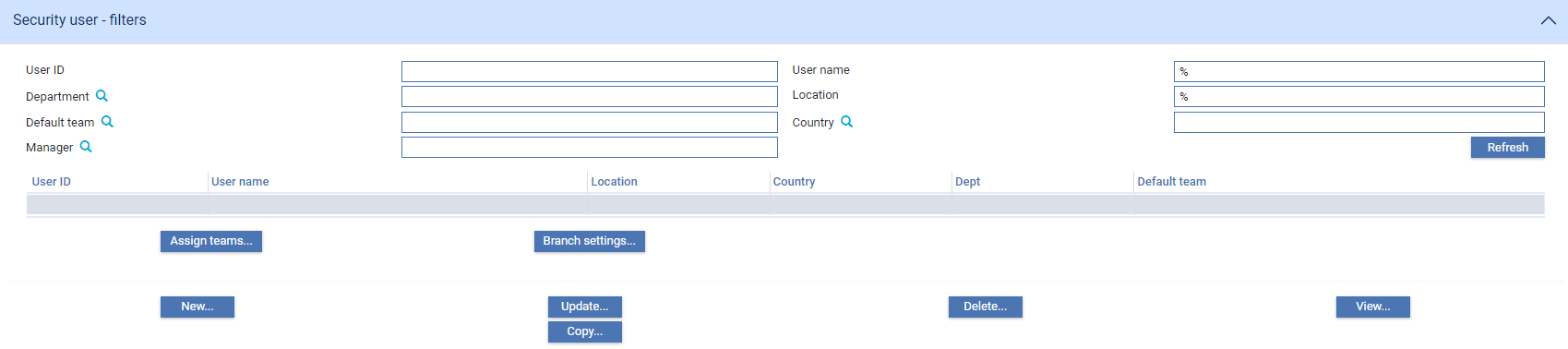
### Deleting Users at the Global Level

To delete a user, select the user entry from the list displayed in the User Profiles window, then click **Delete**. A pop-up window appears and prompts you to click either **Yes** to confirm the deletion, or **No** to abandon it. If you click **Yes**, the user is removed from the Trade Innovation system's user database.

1. You cannot delete a user whilst they are logged on. You will not be allowed to delete a security officer or to reduce their privileges to normal user if they are the only remaining registered user of that class. There must be at least one security officer registered on the system.

## Setting Up a New User in Trade Innovation

Each Trade Innovation user must be registered on the Trade Innovation database. This is done using the security application's Security|Users menu option. It does not matter which zone you run the security application from, since the database is shared across zones.

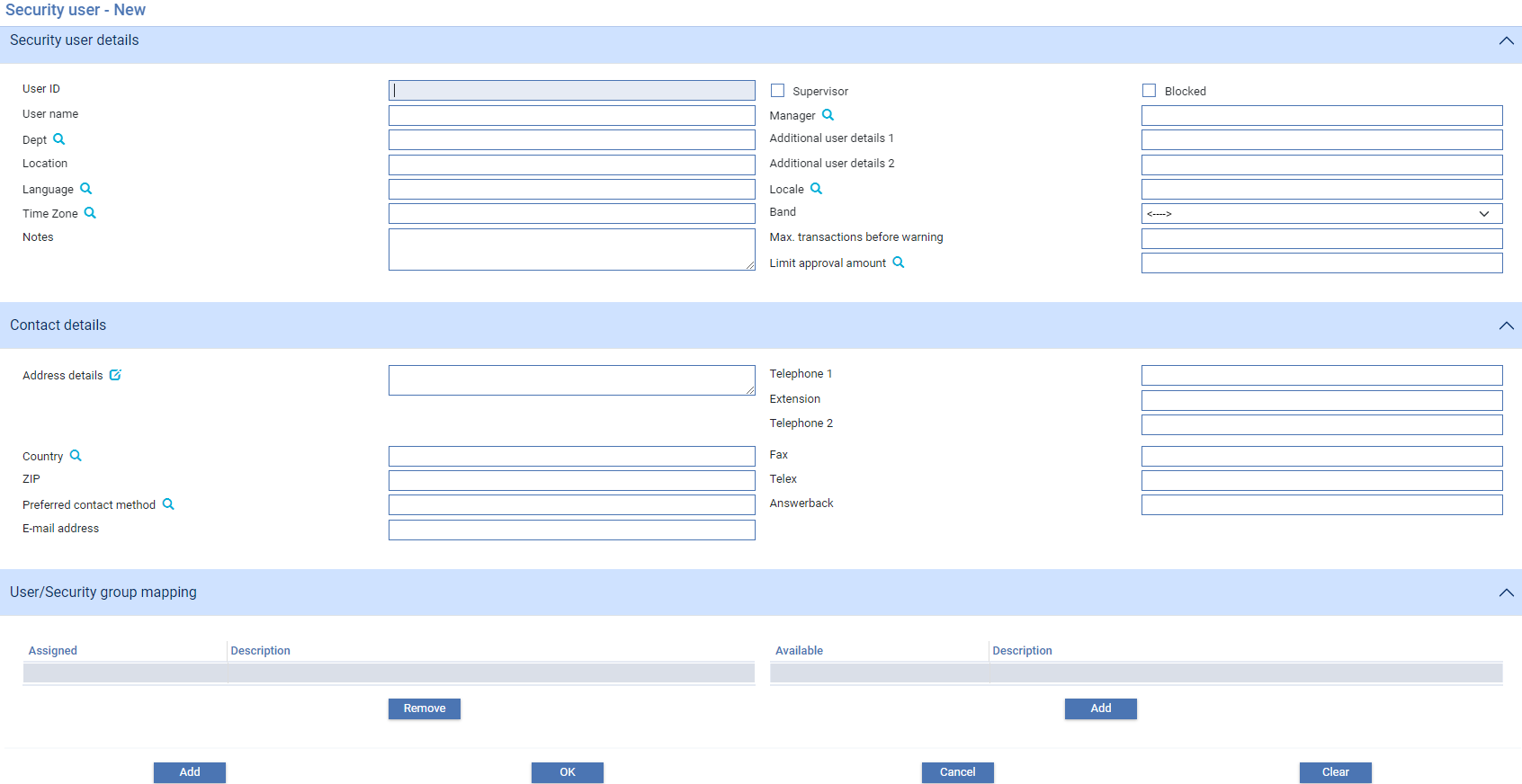


The window displayed when you select this option allows you to list all currently defined Trade Innovation users. The buttons can be used to view, amend and delete existing user details and to add new users in the usual way.

The **Assign Teams** button allows you to assign users to teams.

The **Branch Settings** button opens a window that allows you to view and amend a selected user's transaction branch and enquiry branch (see page 44).

To create a new user, click **New**.



The window that appears allows you to enter details of the new user and to assign them to a team and to a security group.

The User/Security Group Mappings pane shows which security groups the user currently belongs to. You can add a user to, or remove a user from, a team in this pane by highlighting the security group in the relevant list and clicking **Add** or **Remove**.

The following table explains what to enter into the fields in this window to register a new user:

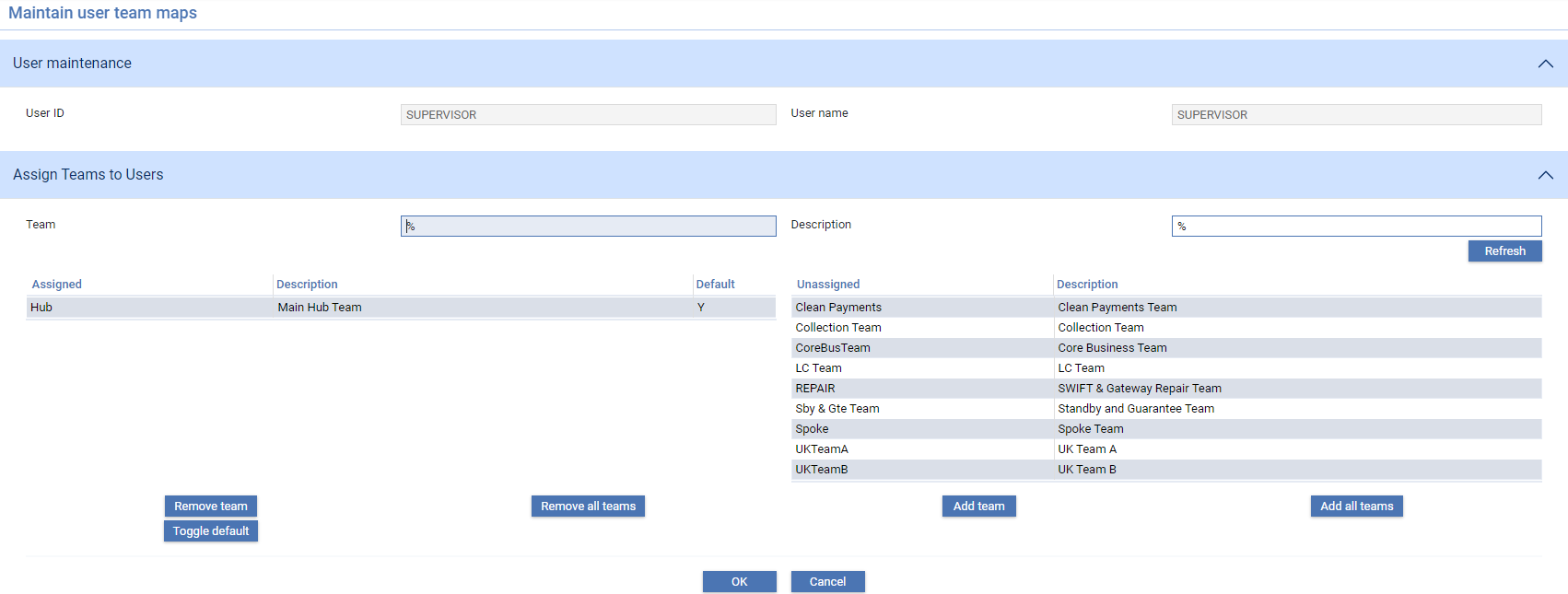
|  |  |  |
| --- | --- | --- |
|  | Field | What to Enter |
|  | User ID | The user's unique ID. This is the user ID already used when registering the user at the global level. |
|  | User Name | The user's name. |
|  | Dept | The code of the account officer or department associated with this user. |
|  | Location | The geographical location where the user is based. |
|  | Language | The user's language. |
|  | Time Zone | (reserved for future use) |
|  | Notes | Any notes against the user. |
|  | Supervisor | Check this field if the user is a supervisor. |
|  | Blocked | Used to block the user within Trade Innovation. This prevents work from being assigned to that user. |
|  | Manager | The user's manager (selected from the list of users already set up in the Trade Innovation database). |
|  | Additional User Details 1 and 2 | Any additional information about the user. |
|  | Locale | The user's locale. The system automatically converts input into this field into upper case characters. |
|  | Band | Define the staff band to which the user belongs. See Chapter 8 for more on how staff bands are used. |
|  | Max. Transactions Before Warning | This field is present only if your bank has Trade Innovation's SLA functionality implemented. It allows you to enter a maximum. Enter a figure here to define the maximum number of transactions that can be allocated to the user. Warning messages are generated during transaction processing is a transaction is allocated to this user that causes this limit to be breached. |
|  | Limit Approval Amount | If your system has Trade Innovation's credit risk management module implemented and the user is to be authorised to approve credit line utilisations, enter here the maximum overline amount the user will be permitted to approve, and the currency in which the amount is being exclicked. The system uses Trade Innovation's base currency as the default. During transaction processing, the user will be prevented from opening transactions awaiting approval if the maximum overline amount requiring approval is greater than the amount entered here.  If you leave this field blank, the system will permit the user to approve any overline amount - no maximum limit will be applied. |
|  | Address Details | The user's address. |
|  | Country | The user address's country. |
|  | Preferred Contact Method | The user's preferred method of contact. |
|  | E-mail Address | The user's e-mail address. |
|  | Telephone 1 | The user's main telephone number. |
|  | Extension | The user's extension at their main telephone number. |
|  | Telephone 2 | An alternative telephone number for the user. |
|  | Fax | The user's fax number. |
|  | Telex | The user's telex number. |
|  | Answerback | The user's answerback number. |
|  | Address Details | The user's address. |
|  |  | The user's ZIP code (or equivalent) at this address. |

1. An edit () icon is displayed near the Address field. Click this icon to edit the structured name and address details. When the structured name and address fields Name, Country and Postal Code are added, these details are copied to the fields User name, Country and ZIP in the Security User details pane and Contact details pane. These fields can then be edited only via the structured name and address details, i.e. using the edit icon.

### Assigning Users to Teams

You can add or remove users from teams using the Assign Teams button in the window displayed when you select the security application's Security|Users menu option.

Select the user whose team assignments you wish to review in this window and click **Assign** **teams**.



The window that is displayed allows you to add the user to a team or remove them from a team.

The Assigned list shows teams to which the user is already assigned.

The Unassigned list shows teams that have not yet been assigned to the user.

The Add Team button allows you to assign a team to the user - highlight the team in the Unassigned list, then click **Add** **team**. The team is moved from the Unassigned list to the Assigned list. The Add All Teams adds all the teams in the Unassigned list to the user in one go.

The Remove Team and Remove All Teams buttons allow you to select and remove teams in the same way.

The Toggle Default button is used to set the current team as the default team for the user. The Default column in the Assigned list indicates whether the current team is their default team (Y) or not (N). Select the team in the Assigned list and click **Toggle default**. If the current team is not already the user's default team (N), then it is made the default (Y). If it is already the default, then its status as default team is removed.

# User Roles

This chapter covers user roles. It explains what they are and how they are set up in conjunction with event groups.

## Users, User Roles and Event Groups

User roles are used to determine what transaction processing functionality individual bank staff need to access in order to do their jobs. User roles correspond to the actual work roles members of a team perform during transaction processing. They are set up using event groups, and then assigned to teams. As individual users are assigned to a team they are assigned one or more user roles within that team.

Event groups bring together all the events (within and/or across products) that actual users performing a particular role within your bank might be expected to process.

To determine which users roles are required your bank needs to ascertain for each of its employees:

* What Trade Innovation products they work with
* Which events within each product they are allowed to process
* The step(s) at which they are allowed to process each event
* What master-level tasks they are allowed to perform

You should then be able to produce a matrix showing which users work with which events:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Product | Event | User A | User B | User C | User D |
| ILC | Pre Advise |  |  |  |  |
|  | Issue |  |  |  |  |
|  | Amend |  |  |  |  |
|  | Claim Received |  |  |  |  |
|  | Outstanding Claim |  |  |  |  |
| ELC | Pre Advise |  |  |  |  |
|  | Advise |  |  |  |  |
|  | Amend |  |  |  |  |
|  | Documents Presented |  |  |  |  |
|  | Outstanding Presentation |  |  |  |  |

This allows your bank to determine which event groups it needs to set up. The table above identifies the need for two event groups. The first event group (LC Issuance) contains the following events:

* ILC Pre Advise
* ILC Issue
* ILC Amend
* ELC Pre Advise
* ELC Issue
* ELC Amend

The second event group (LC Payment) contains the following events:

* ILC Claim Received
* ILC Outstanding Claim
* ELC Documents Presented
* ELC Outstanding Presentation

Having identified and created the necessary event groups you can then create the actual user roles. This involves taking into account the steps at which each individual user can work with the events in each event group.

A separate user role can then be set up for every permutation of steps that can be carried out against the events in a particular event group.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Product/event | Step | User A | User B | User C | User D |
| ILC |  |  |  |  |  |
| Pre Advise | Log step |  |  |  |  |
| Pre Advise | Input step |  |  |  |  |
| Pre Advise | Review step |  |  |  |  |
| Pre Advise | Authorise step |  |  |  |  |
| Issue | Log step |  |  |  |  |
| Issue | Input step |  |  |  |  |
| Issue | Review step |  |  |  |  |
| Issue | Authorise step |  |  |  |  |
| Issue | Final print step |  |  |  |  |
| Amend | Log step |  |  |  |  |
| Amend | Input step |  |  |  |  |
| Amend | Review step |  |  |  |  |
| Amend | Authorise step |  |  |  |  |
| Claim Received | Log step |  |  |  |  |
| Claim Received | Input step |  |  |  |  |
| Claim Received | Review step |  |  |  |  |
| Claim Received | Authorise step |  |  |  |  |
| Outstanding Claim | Log step |  |  |  |  |
| Outstanding Claim | Input step |  |  |  |  |
| Outstanding Claim | Review step |  |  |  |  |
| Outstanding Claim | Authorise step |  |  |  |  |
| ELC |  |  |  |  |  |
| Pre Advise | Log step |  |  |  |  |
| Pre Advise | Input step |  |  |  |  |
| Pre Advise | Review step |  |  |  |  |
| Pre Advise | Authorise step |  |  |  |  |
| Advise | Log step |  |  |  |  |
| Advise | Input step |  |  |  |  |
| Advise | Review step |  |  |  |  |
| Advise | Authorise step |  |  |  |  |
| Amend | Log step |  |  |  |  |
| Amend | Input step |  |  |  |  |
| Amend | Review step |  |  |  |  |
| Amend | Authorise step |  |  |  |  |
| Documents Presented | Log step |  |  |  |  |
| Documents Presented | Input step |  |  |  |  |
| Documents Presented | Review step |  |  |  |  |
| Documents Presented | Authorise step |  |  |  |  |
| Outstanding Presentation | Log step |  |  |  |  |
| Outstanding | Input step |  |  |  |  |
| Outstanding | Review step |  |  |  |  |
| Outstanding | Authorise step |  |  |  |  |

In the table above, there are two permutations of steps against each of the two event groups, requiring the creation of four separate user roles:

|  |  |  |  |
| --- | --- | --- | --- |
| User role | Event grouping | Steps | What the User can Do |
| LC Issue Input | LC Issuance | Log step  Input step  Final print | Log and input Pre Advise, Issue and Amend events for import letters of credit.  Log and input Pre Advise, Advise and Amend events for export letters of credit. |
| LC Issue Authorise | LC Issuance | Review step  Authorise step | Review and authorise Pre Advise, Issue and Amend events for import letters of credit.  Review and authorise Pre Advise, Advise and Amend events for export letters of credit. |
| LC Payment Input | LC Payment | Log step  Input step | Log and input Claim Received and Outstanding Claim events for import letters of credit.  Log and input Documents Presented and Outstanding Presentation events for export letters of credit. |
| LC Payment Authorise | LC Payment | Review step  Authorise step | Review and authorise Claim Received and Outstanding Claim events for import letters of credit.  Review and authorise Documents Presented and Outstanding Presentation events for export letters of credit. |

Once user roles have been set up they are used to build teams of users for each branch. Each team is assigned one or more user roles. Actual bank staff are then assigned to each team, and are assigned one or more user roles within that team. See Chapter 6 for information on creating the linkages between teams, users and user roles.

### Master-level Tasks

In addition to the event-specific functionality described in the previous section, user roles are also used to set up access to functionality used during transaction processing that is not linked to a particular event. This includes, for example, the functionality used to:

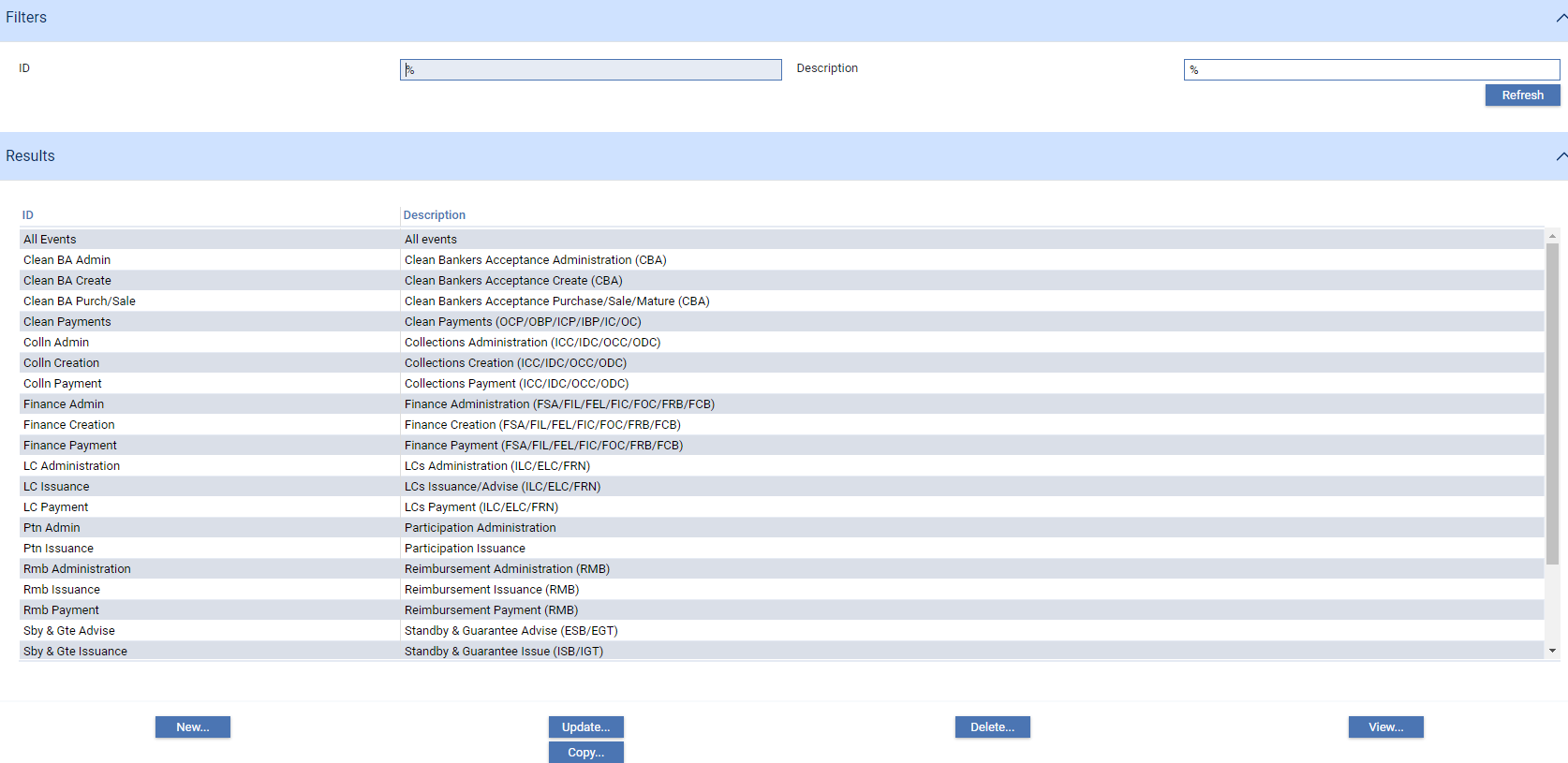
* Amend and delete automatically generated diary entries
* Change notes entered against an event
* Use the More button on the Master Summary window

A full list of these master-level tasks is provided (see page 66).

## Setting Up Event Groups

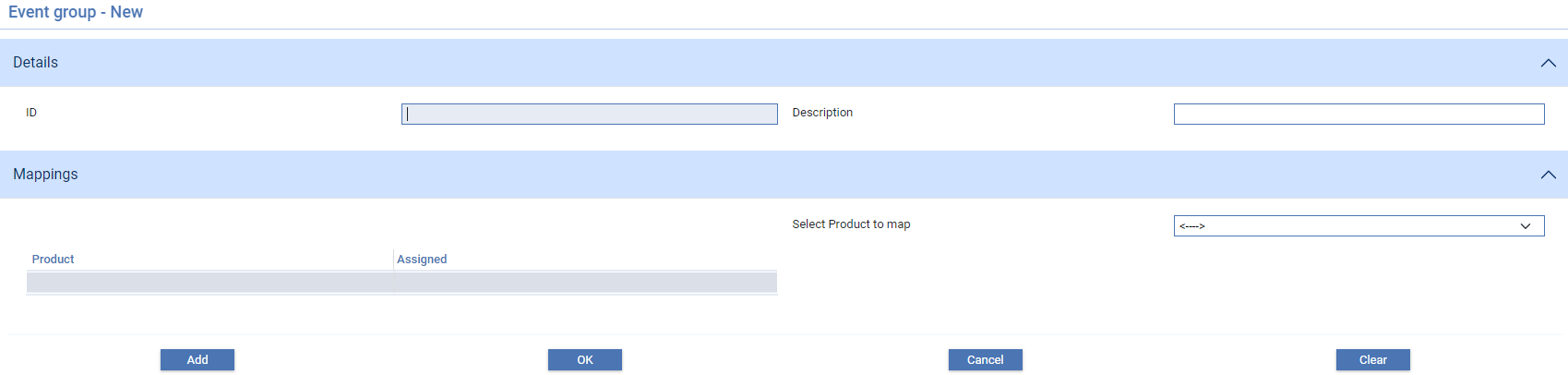
Event groups are used to control what events users performing a particular user role can work with. They are used in conjunction with user roles, and must be set up before the user roles that will use them can be created.

To set up an event group, in the security application select the Security|Event Groups menu option.



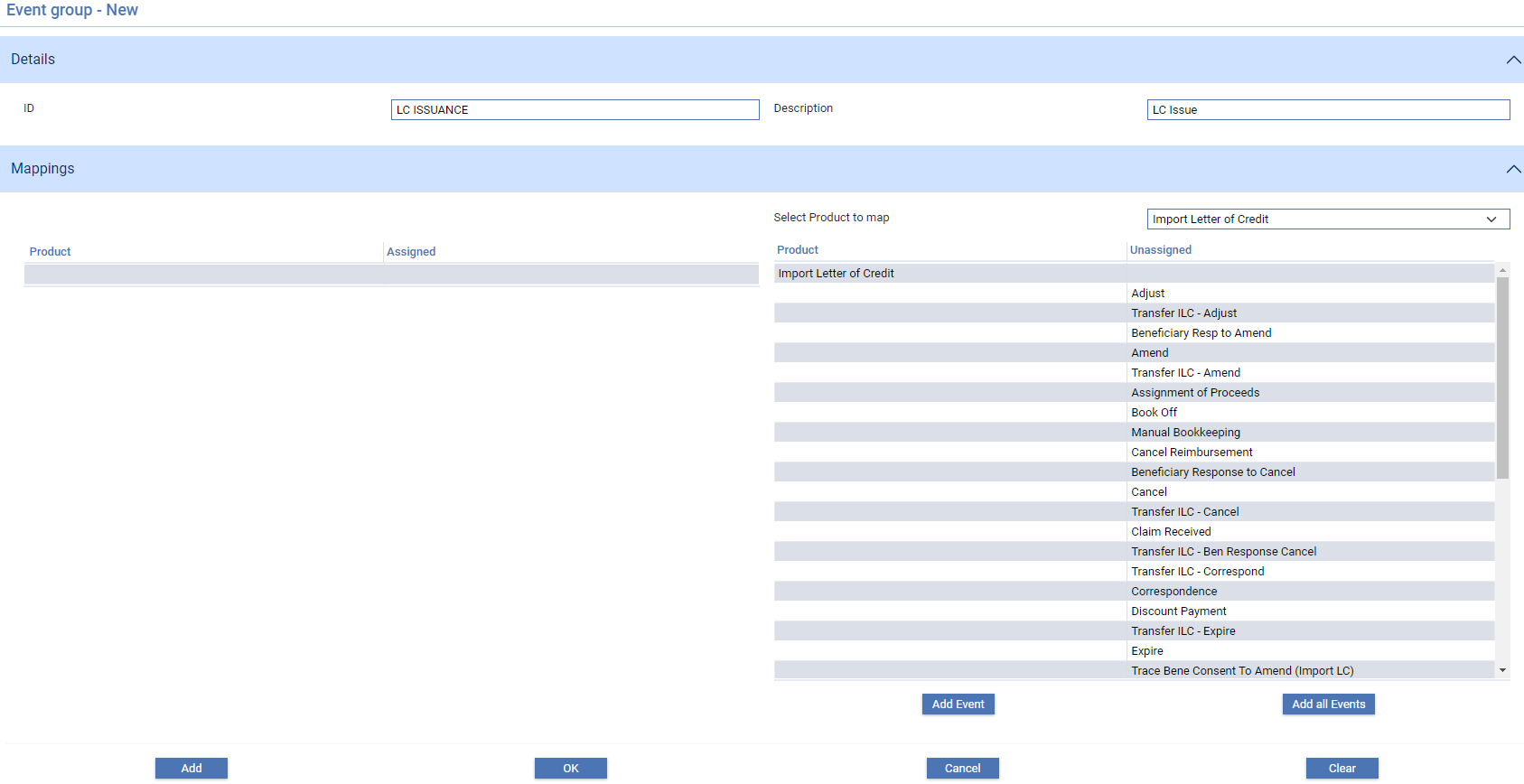
The window displayed when you select this menu option lists all the event groups already set up on your system.

To set up a new event group click **New**.

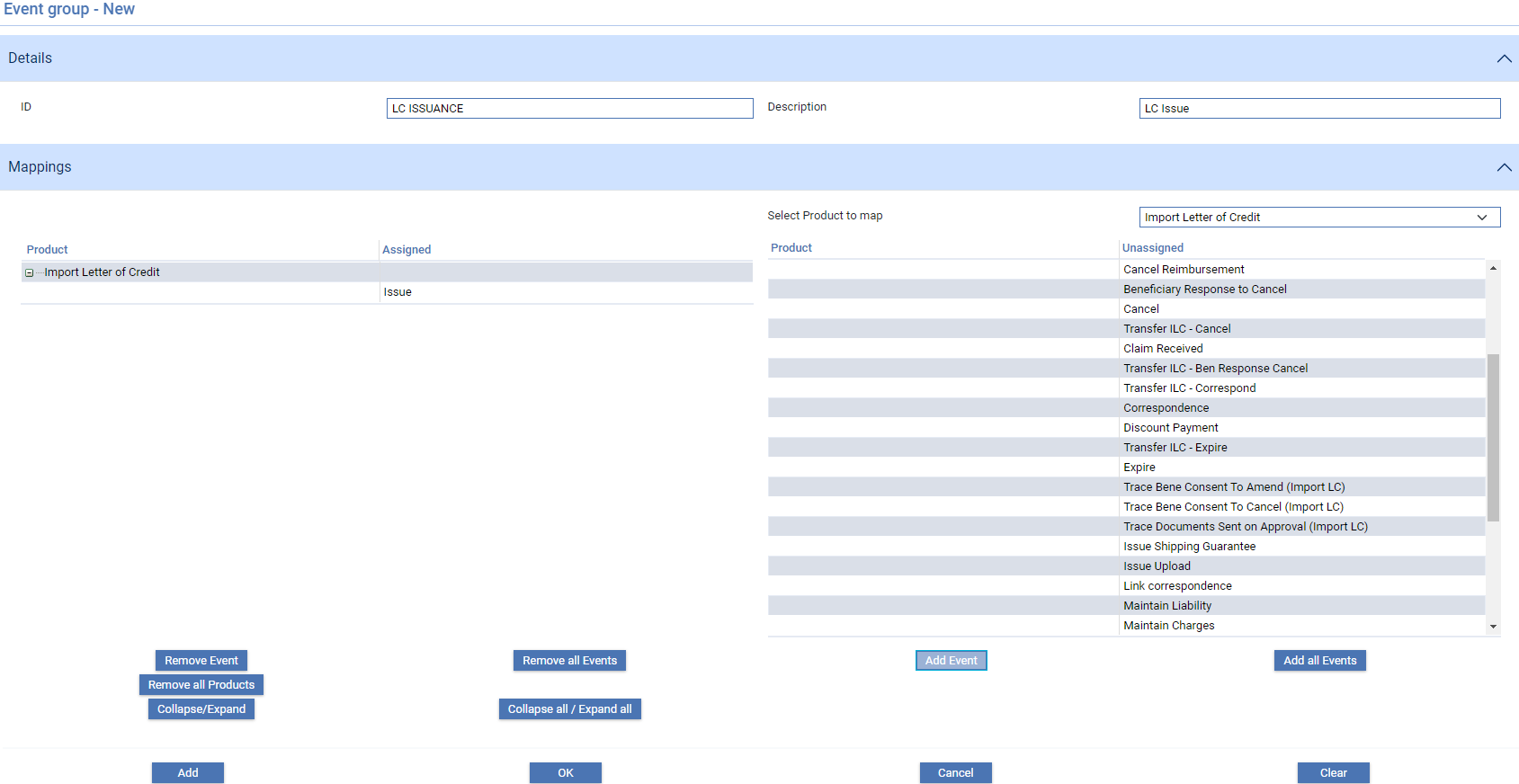


Enter a unique ID and description for the event group. Both fields are mandatory. Once you have entered this information you can select each product, and the events from it, in turn to add to the event group.

Select the product in the Product field. The system lists all the events in that product.



Highlight the one to add to the event group, then click **Add**. The selected event is moved to the list of events included in the event group.



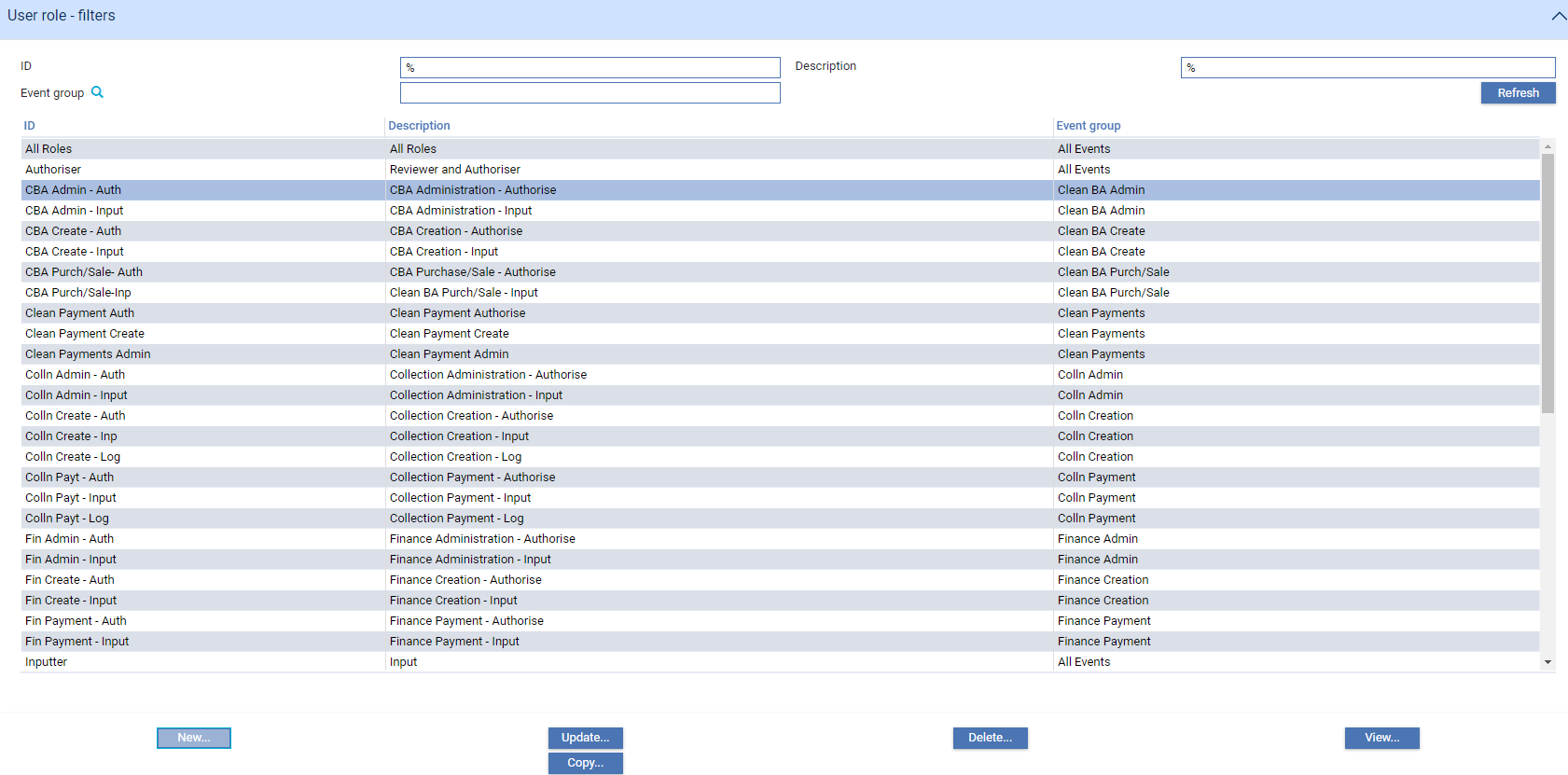
The Add All button allows you to add all the events to the event group in one go.

The Remove and Remove All buttons allow you to select events in the list of events included in the event group and remove them in the same way.

Once you have selected all the events for a product you can select another product to be added to the event group in the Product field and repeat the process for that product.

## Setting Up User Roles

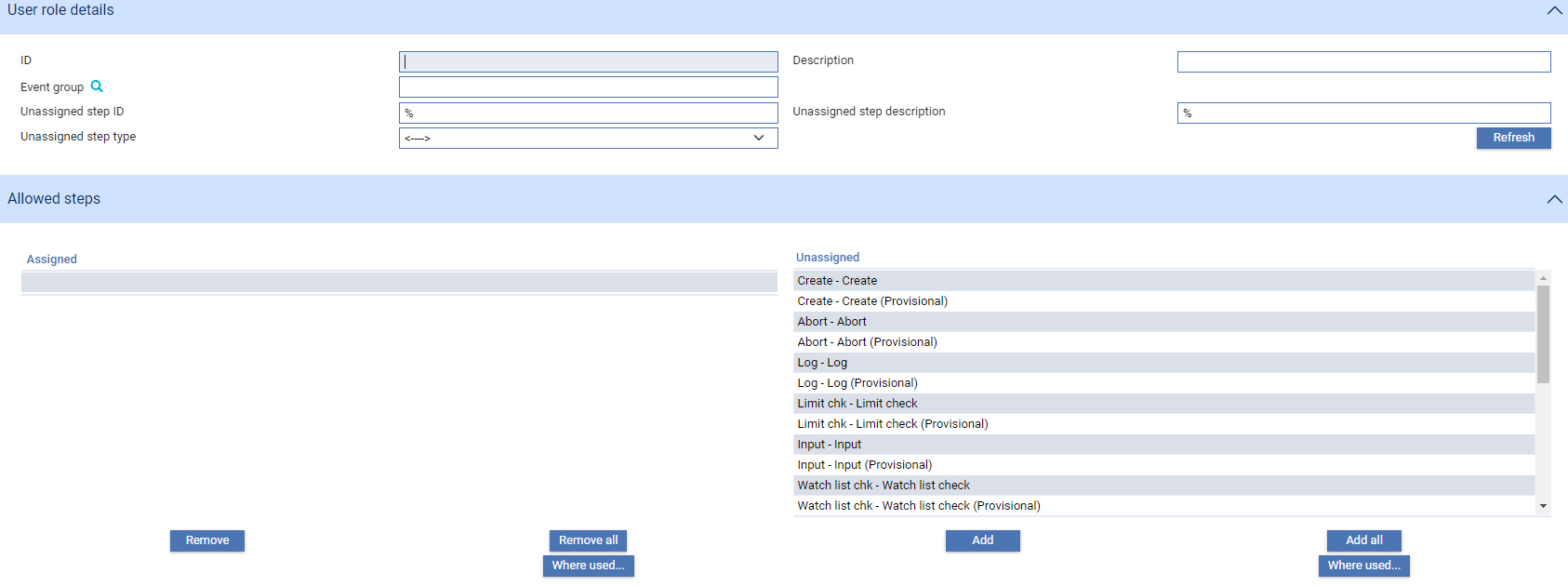
User roles are set up using the security application's Security|User Roles menu option.



When you select this menu option the system lists all the user roles currently set up on your system.

1. The View button opens a window that displays information about the selected user role in the usual way. In addition, a View button on the Event Groups field in that window allows you to see details of the product/event combinations included in each event group assigned to the user role.

To set up a new user role click **New**.

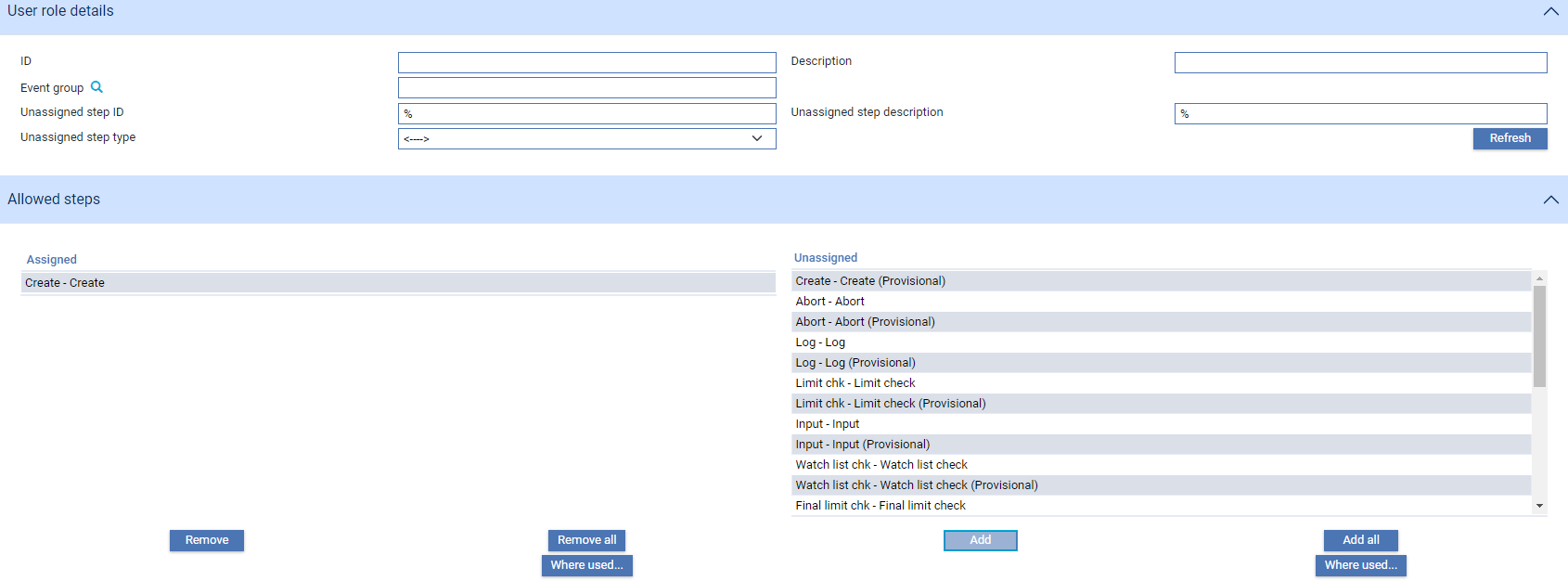


Enter a unique ID for the user role and then a description into the first two fields.

Select the relevant event group in the Event Group field.

In the Unassigned list of event steps highlight the step at which users assigned to this user role will be able to process the events in the selected event group, then click **Add**. For user roles handling provisional events, select the provisional instance of the steps required.

The selected step is moved to the Assigned list.



The Add All button allows you to add all the steps in one go.

The Remove and Remove All buttons allow you to select steps in the Assigned list and remove them in the same way.

The Common Functionality pane lists capabilities that control access to master-level tasks. These are listed in page 66. You can add capabilities to the user role in the same way as described above for event steps.

# Teams

This chapter explains how to set up teams and map them to branches, users, user roles and key customers.

## Overview

Teams provide the mechanism in Trade Innovation by which your bank's staff are linked to the branches on whose transactions they will work, and to the user roles that will govern what work they can perform.

You need to assign at least one team to each branch.

Once teams are set up you:

* Assign the required user roles to that team
* Assign actual bank staff to teams. If a user is assigned to more than one team, one of those teams is designated their default team. You can also assign them a transaction branch and an enquiry branch
* Assign each bank staff member at least one user role within the team (except for supervisors, who do not need a user role)

If a user is assigned to more than one team, you must designate one of those teams as their default team. You can also assign a transaction branch and an enquiry branch (see page 5) to each user for each team/branch combination.

Team structures may be flat or hierarchical, or a combination of both. They are used in conjunction with branch hierarchies to control what transactions a user can access, in the following way.

Access at transaction level is controlled by branch/team linkages in the following way:

* If a user is logged on as a member of a team that has no other teams below it in your bank's team hierarchy, they will be able to work only with transactions belonging to the branch(es) linked to that team
* If a user logs on using a team that has other teams below it in your bank's team hierarchy they will be able to work with transactions belonging to the branch(es) linked to that team. In addition they will be able to work with transactions belonging to branches linked to child teams below the one they are currently using, provided that those branches are children of the branch(es) linked to the team they are currently using. Further:
* If they are a member of any of these child teams, their user role within each child team determines how they can process transactions assigned to those teams
* If they are not members of a child team, they will be able to open transactions assigned to those teams in view-only mode

Users may also be restricted to working with transactions belonging to their own branch; or may be prevented from working with events beyond a certain amount. These restrictions apply in addition to the access control provided by branch/team assignments described above.

### Teams and Extended Business Hours Processing

You can allow extended business hours processing on transactions in one of two ways:

* By setting up a team for the relevant branches that includes bank staff from each of the separate time zones necessary to ensure extended coverage
* By assigning the branch to different teams in different time zones

### Teams and Workflow

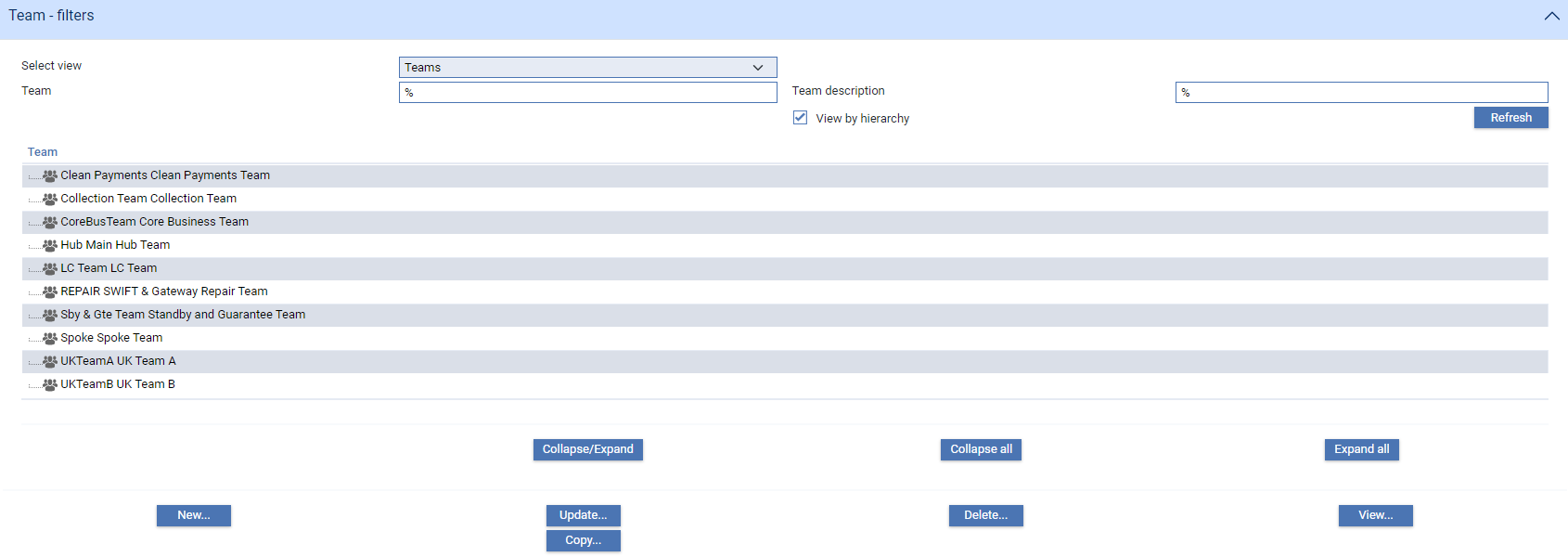
For products that use SLA functionality the system provides a way of routing transactions to the teams that will work on them at each stage in their life-cycle. By associating rules with each event/SLA combination your bank can determine which team an event should be routed to at each point in its life-cycle. See the System Tailoring User Guide – Trade Innovation for instructions.

### Teams and Key Customers

When setting up teams your bank can identify specific customers as being of more than usual relevance to a particular team. These are termed that team’s key customers. During transaction processing, the Dashboard can be used to show information for all customers with transactions assigned to your team; or only for your key customers.

## Teams

Teams are set up using the security application's Security|Teams menu option. When you select this option the system opens a browser window that lists the teams already set up.

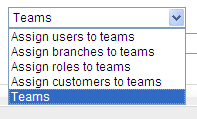


Teams are initially listed hierarchically. Teams that have users assigned to them or teams below them are indicated by a . The Expand All button displays the information in expanded view, and the Collapse All button displays just the top-level entries.

You can collapse or expand the information shown for individual teams by selecting an entry in the list and clicking **Collapse/Expand**.

If you uncheck the View By Hierarchy field, teams are listed instead alphabetically, with no indication of their place in the hierarchy or of whether they have users assigned to them.

The Select View field allows you to select what aspect of setting up a team you wish to work with.



You can:

* Set up a new team (by clicking **Add** - see the next section)
* Assign user roles to a team (see page 27)
* Assign branches to a team and set the team's accounting branch (see page 39)
* Assign users to a team (see page 42)
* Assign user roles to users (see page 43)
* Assign transaction and enquiry branches to users (see page 44)
* Assign key customers to a team (see page 46)

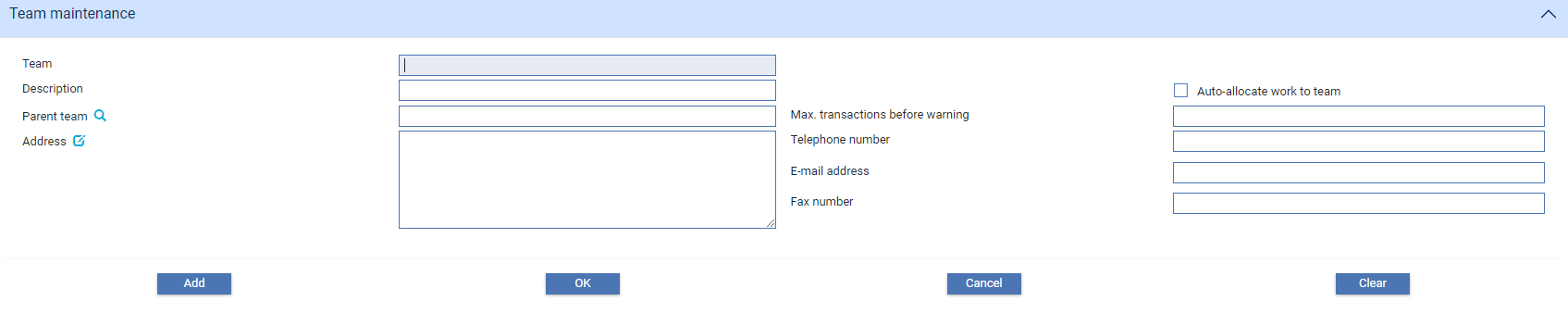
The information listed in this window varies depending on what you select in the Select View field. The following icons are displayed against entries in the lists to indicate what type of entries they are:

|  |  |
| --- | --- |
| Field | What to Enter |
|  | Branch |
|  | Customer |
|  | Team |
|  | User |
|  | User role |

The above table show the graphics delivered with Trade Innovation; your bank may change these.

The security application's Security|User/Team/Role Enquiry menu option allows you, as security officer, to view information about your and other users' access to Trade Innovation's transaction processing functionality (see page 62).

### Setting Up a New Team

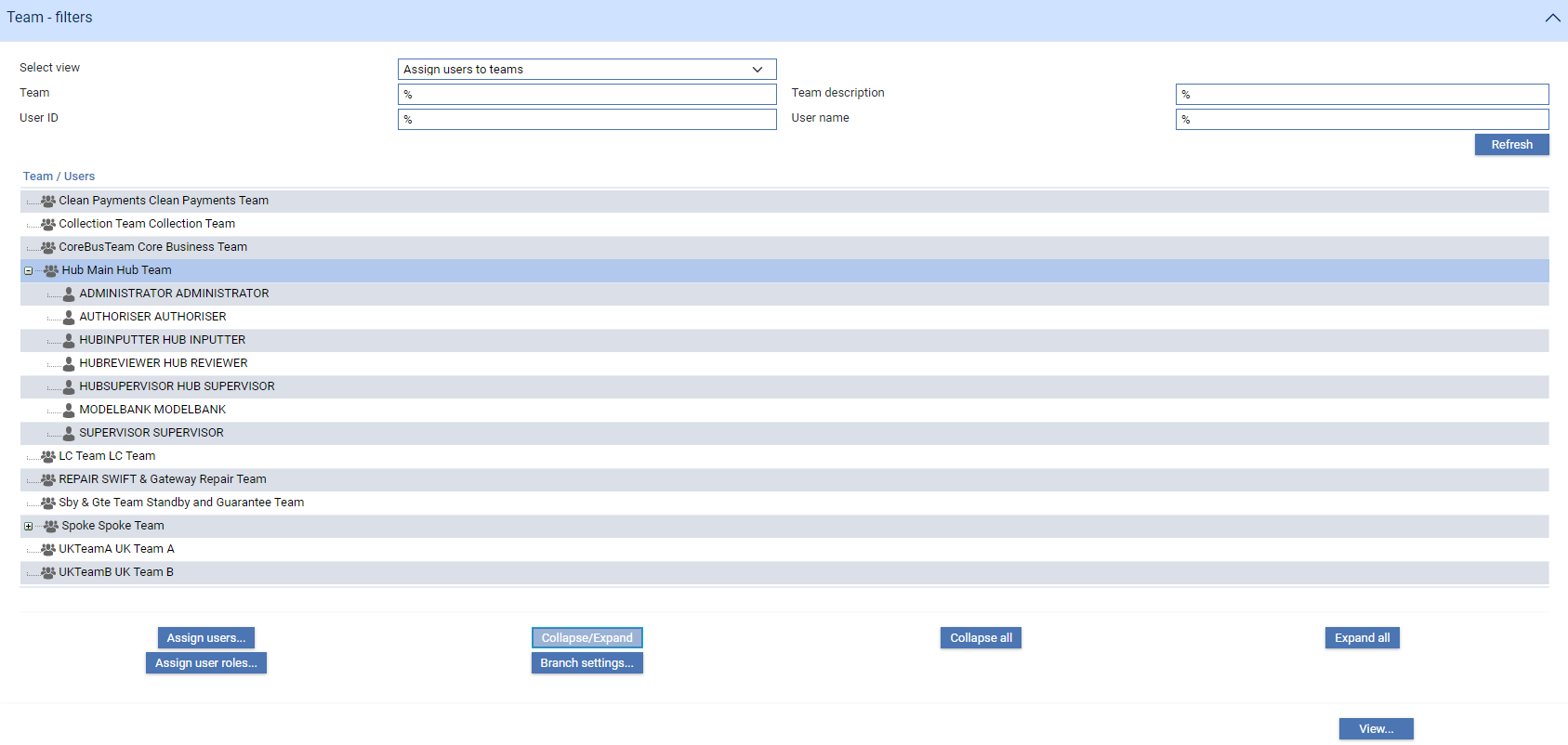


The following table explains what to enter into the fields used to set up a new team:

|  |  |  |
| --- | --- | --- |
|  | Field | What to Enter |
|  | Team Name | The team’s unique ID. |
|  | Team Description | A description of the team. |
|  | Parent Team | If the team is in a hierarchy, identify the team directly above it in that hierarchy. |
|  | Auto-allocate work to team | When ticked, the system will automatically allocate transactions to teams on a round-robin basis |
|  | Address | The team's address, up to five lines, used for mailing purposes. |
|  | Max. Transactions Before Warning | You can enter a figure here to define the maximum number of transactions that can be allocated to the team. If you do so, warning messages are issued during transaction processing if a transaction is allocated to the team that causes this limit to be breached. |
|  | Telephone | The team's address, up to five lines, used for mailing purposes. |
|  | Email | The team's email address at this address. |
|  | Fax | The team's fax number at this address. |

### Assigning User Roles to a Team

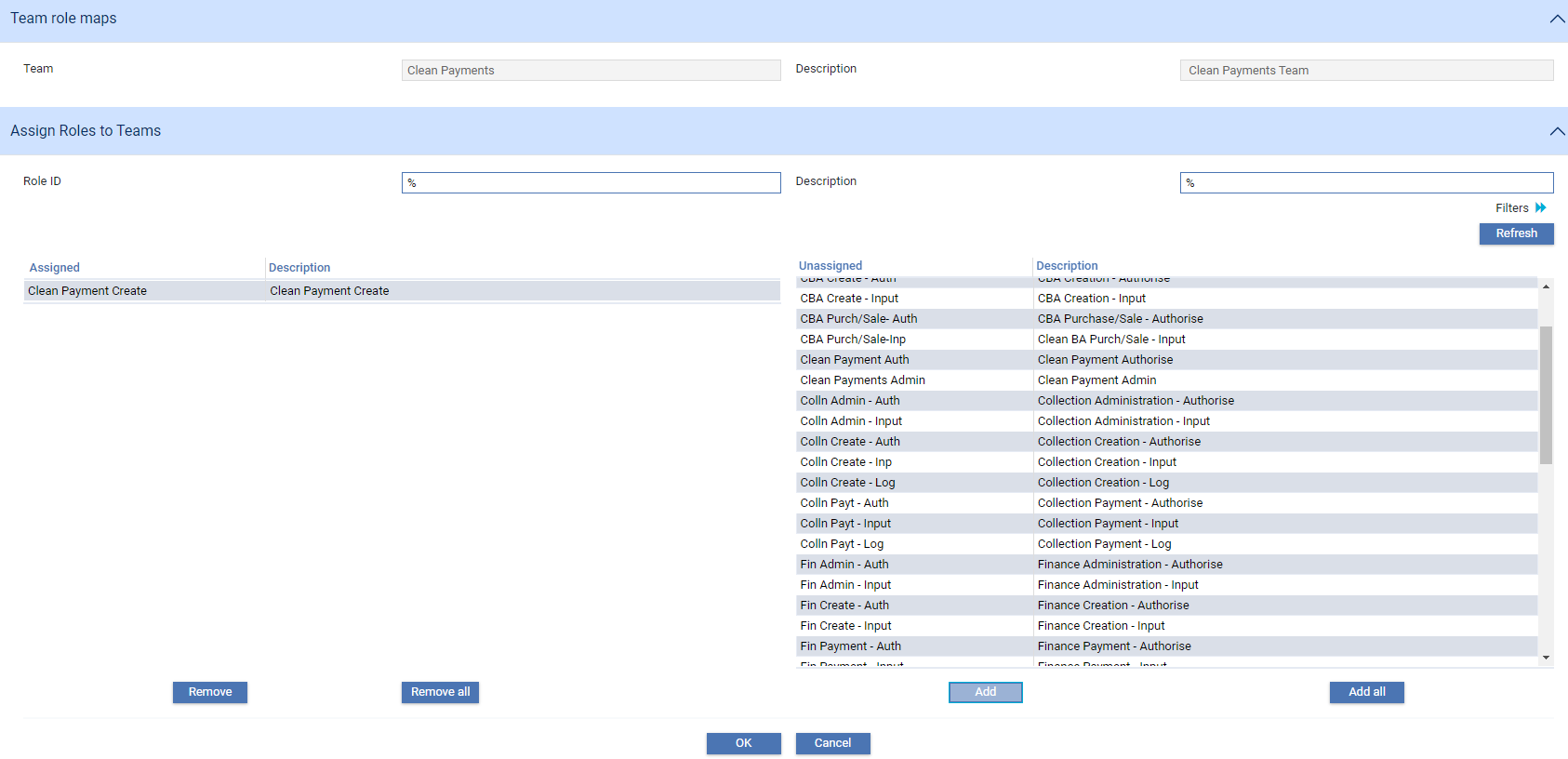
Select 'Assign Roles to Teams' in the Select View field. The window changes to display new buttons and filter fields that you can use to search for the team to which you want to add user roles.



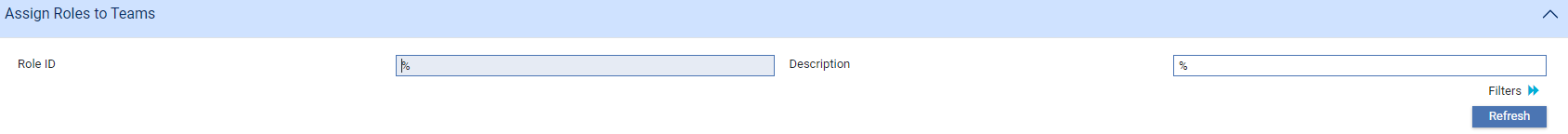
If you perform a search, the system displays each team that meets your search criteria.

To assign a user role to a team highlight the team, then click **Assign** **roles**.

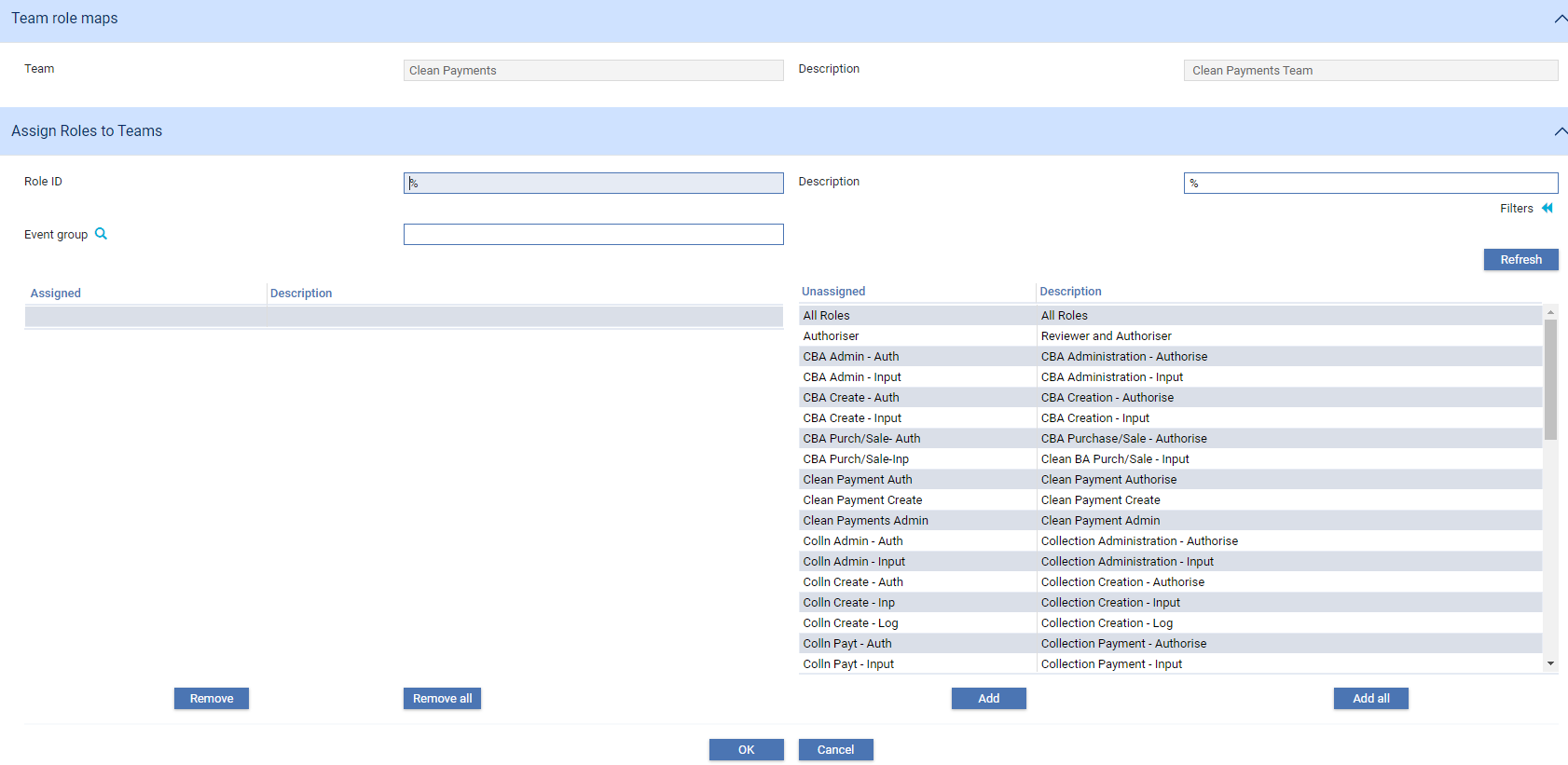
The window that is displayed lists all the user roles that have already been assigned to that team and those that have not.



Filter fields allow you to narrow the list of user roles not assigned to the team to those meeting certain criteria. The window initially displays filter fields for the unique ID and description. Clicking the  toggle button displays an additional filter field for event group.



The system returns user roles matching the criteria you have entered and lists them.



The Assigned list shows user roles already assigned to the team.

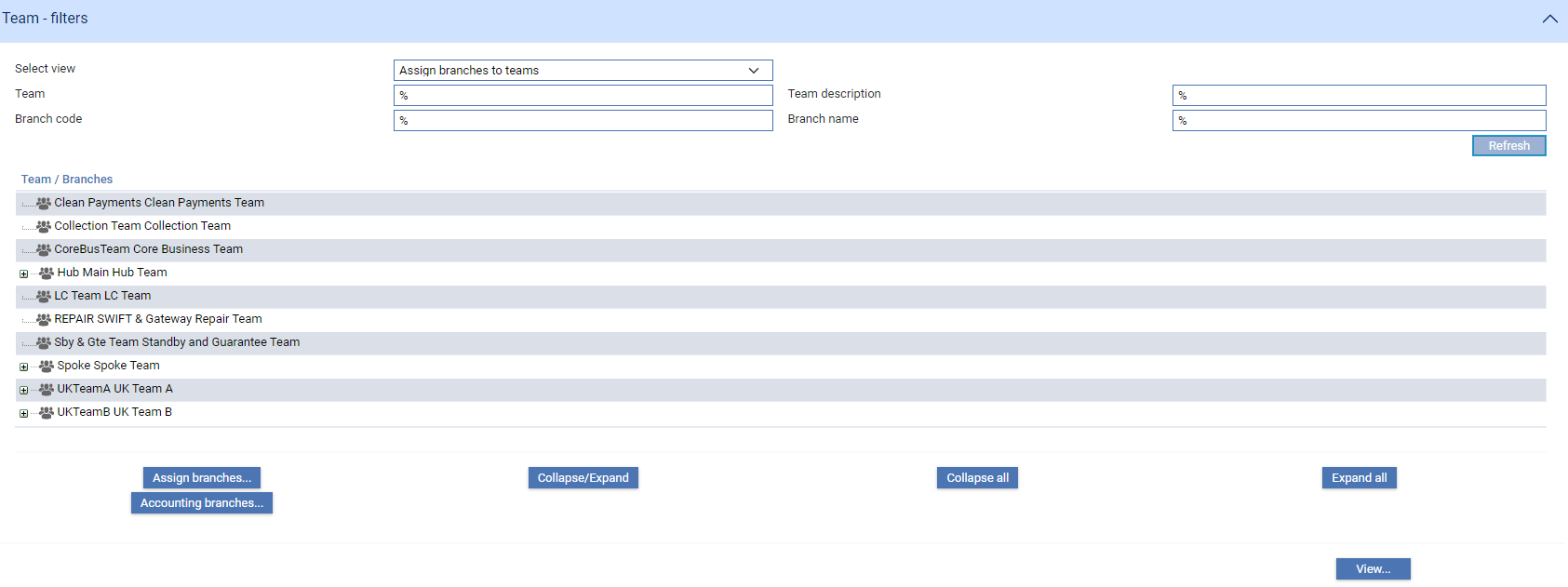
The Unassigned list shows user roles that have not yet been assigned to the team.

The Add button allows you to assign a user role to the team - highlight the user role in the Unassigned list, then click **Add**. The user role is moved from the Unassigned list to the Assigned list. The Add All adds all the user roles in the Unassigned list to the team in one go.

The Remove and Remove All buttons allow you to select and remove user roles in the same way.

### Assigning Branches to a Team

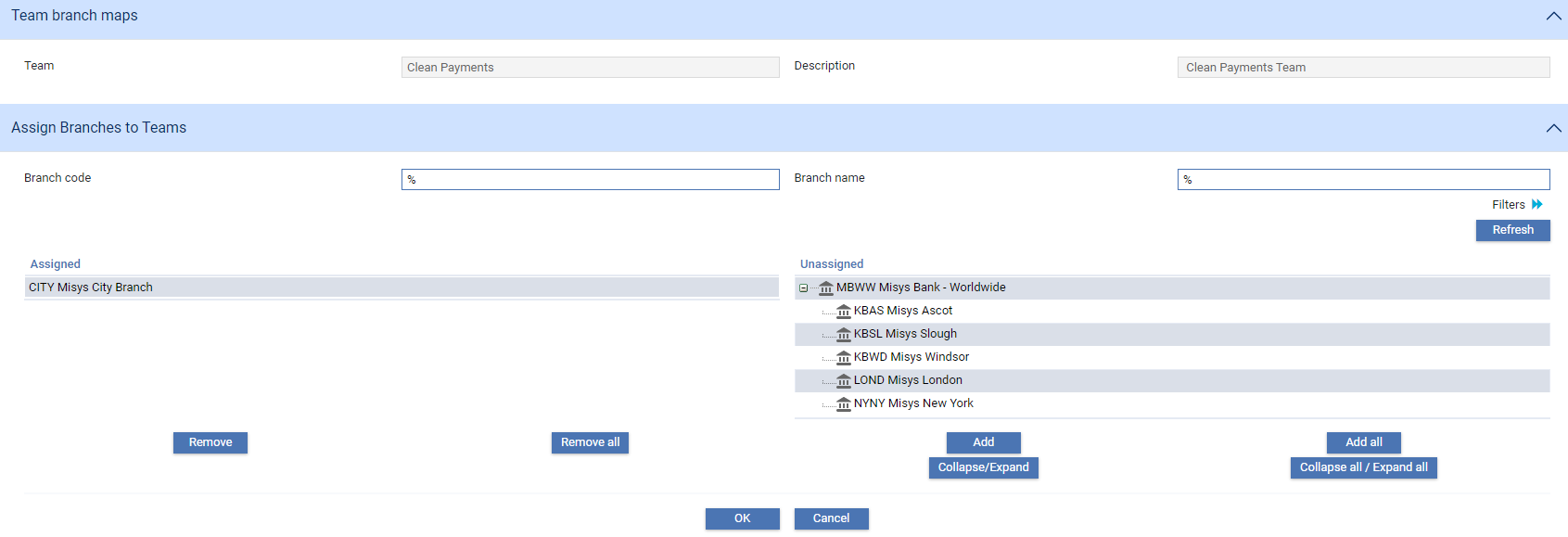
Select 'Assign Branches to Teams' in the Select View field. The window changes to display different buttons, and filter fields that you can use to search for the team to which you want to assign a branch.



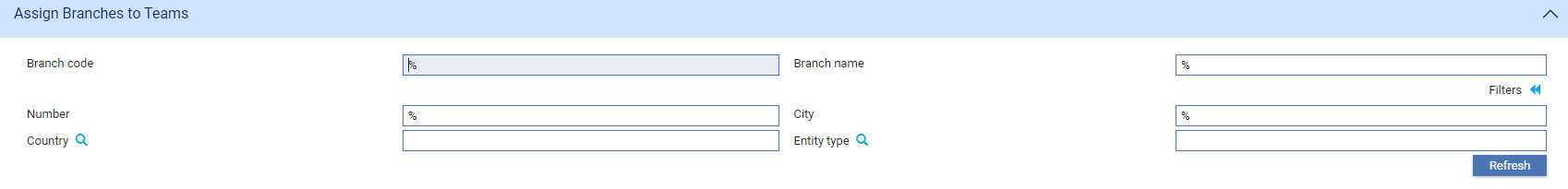
If you perform a search, the system displays each team that meets your search criteria.

To assign a branch to a team highlight the team, then click **Assign branches**.

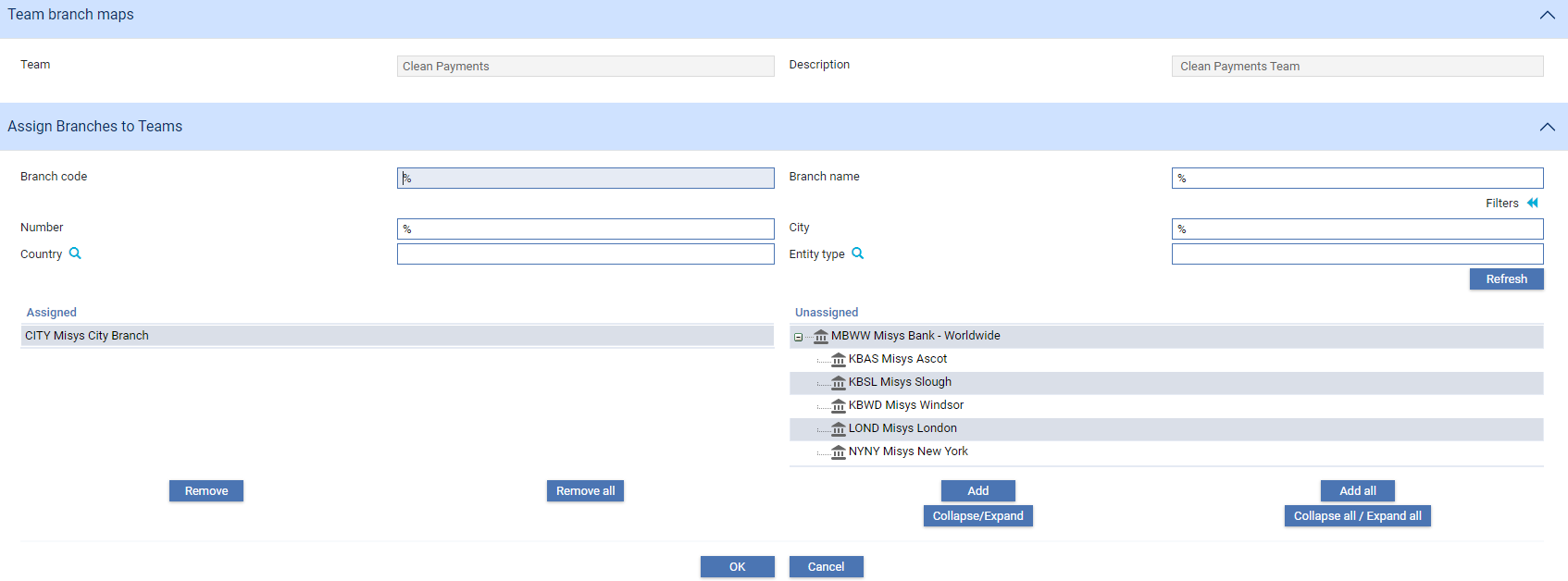
The window that is displayed lists all the branches that have already been assigned to that team, and those that have not.



Filter fields allow you to narrow the list of branches not assigned to the team to those meeting certain criteria. The window initially displays filter fields for unique branch ID and name. Clicking the  toggle button displays additional filter fields for branch number, country, city, and entity type.



The system returns branches matching the criteria you have entered and lists them.



The Assigned list shows branches already assigned to the team.

The Unassigned list shows branches that have not yet been assigned to the team.

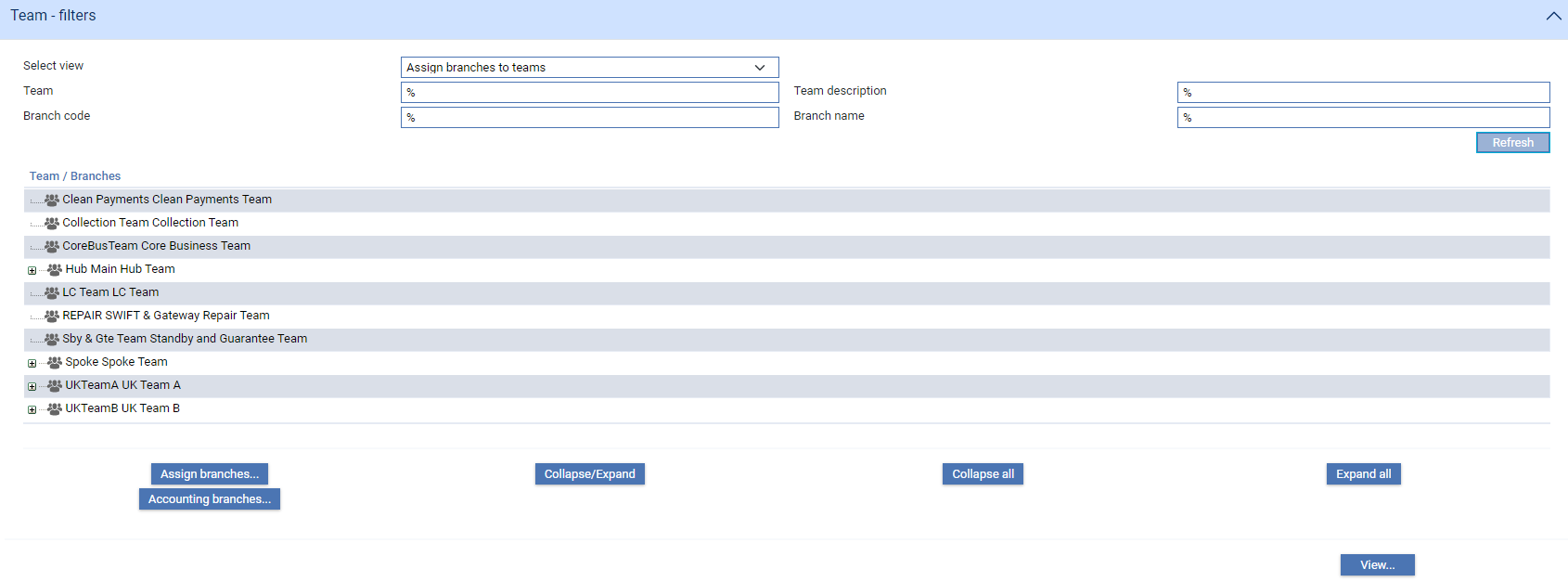
The Add button allows you to assign a branch to the team - highlight the branch in the Assigned list, then click **Add**. The branch is moved from the Unassigned list to the Assigned list. The Add All adds all the branches in the Unassigned list to the team in one go.

The Remove and Remove All buttons allow you to select and remove branches in the same way.

1. When you assign a branch to a team, if that branch has child branches, then these child branches are also added to the team and are moved from the Unassigned to the Assigned column.

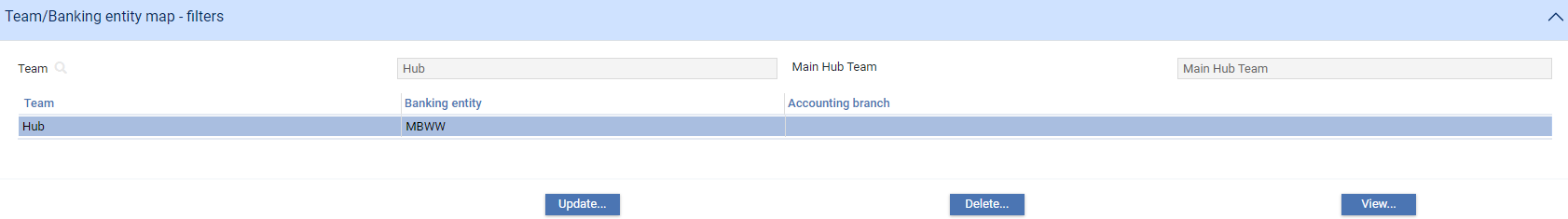
#### To Set the Team's Accounting Branch

To set a team's accounting branch select 'Assign Branches to Teams' in the Select View field. The window changes to display different buttons, and filter fields that you can use to search for the team to which you want to assign an accounting branch.

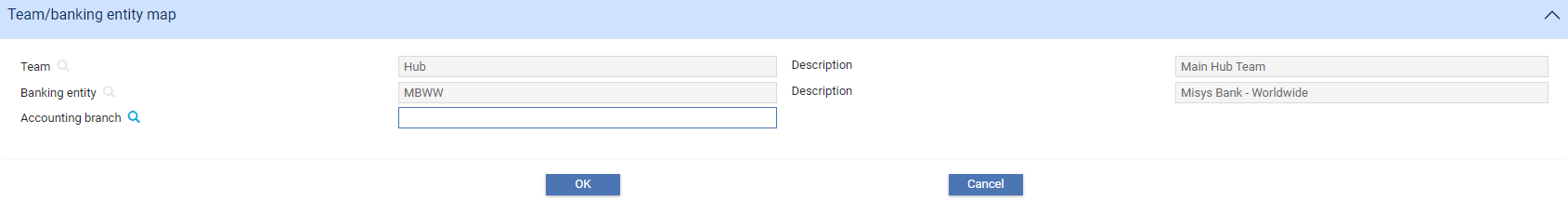


If you perform a search, the system displays each team that meets your search criteria.

To assign an accounting branch to a team highlight the team, then click **Accounting branches**.



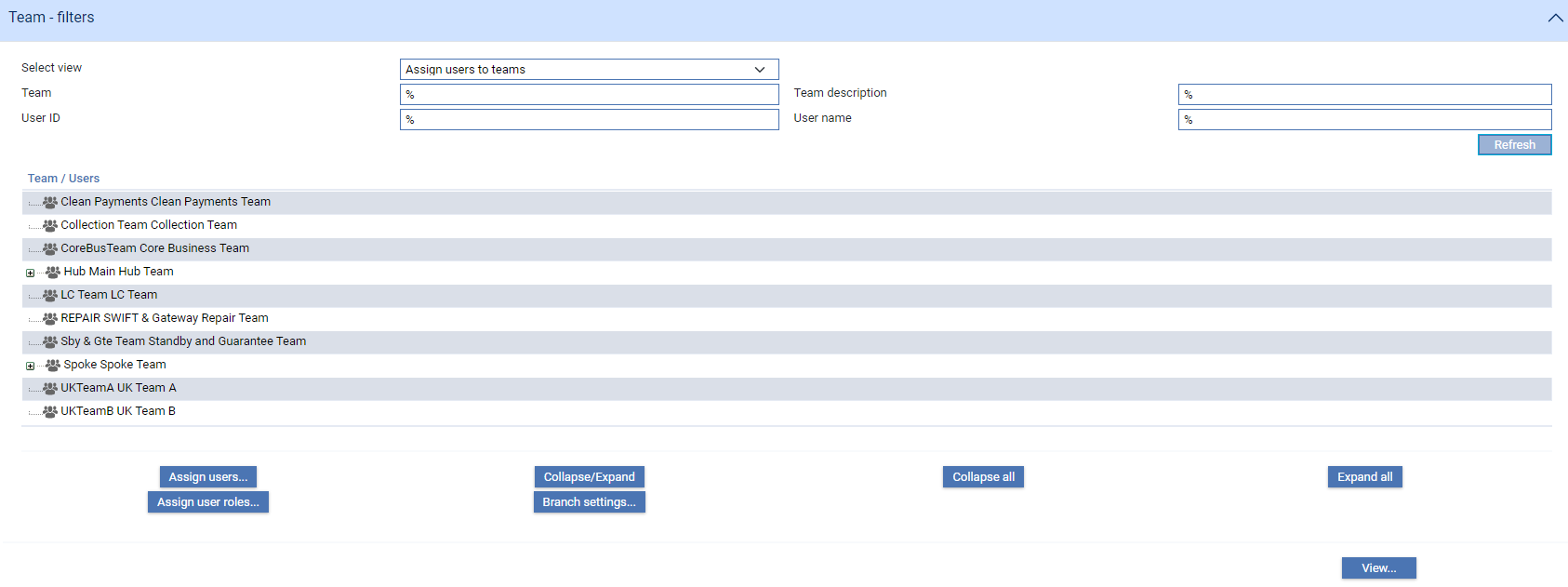
In the window that appears click **Update**. This displays a window that allows you to set the accounting branch for the selected team.



In the window that appears use the Accounting Branch field to identify the team's accounting branch.

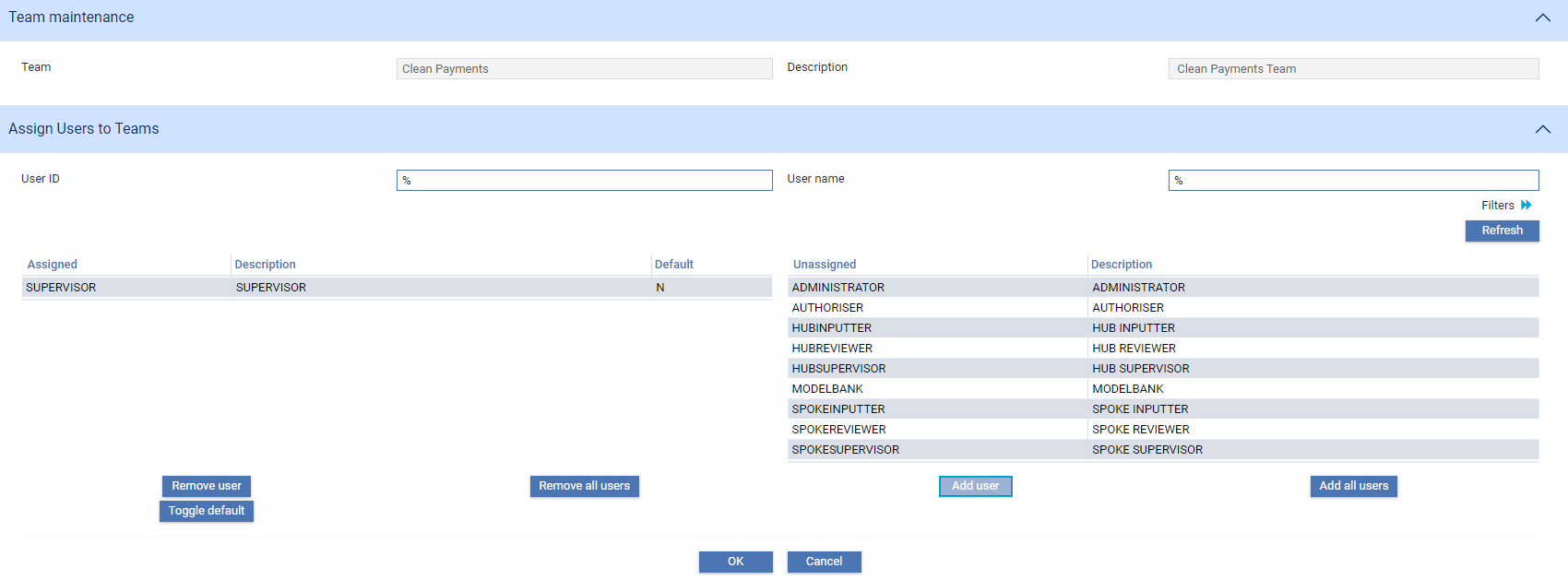
### Assigning Users to a Team

Select 'Assign Users to Teams' in the Select View field. The window changes to display new buttons and filter fields that you can use to search for the team to which you want to add users.

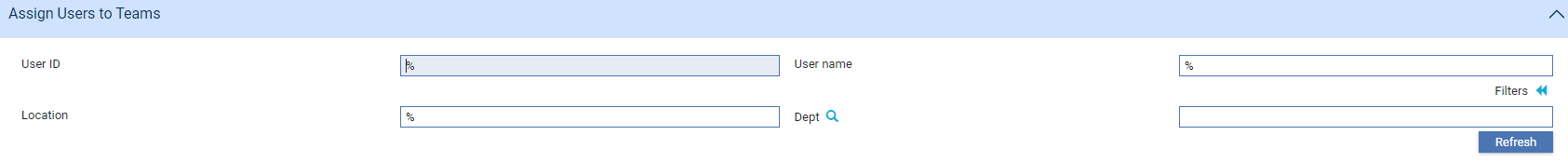


To add a user to a team highlight the team, then click **Assign users**.

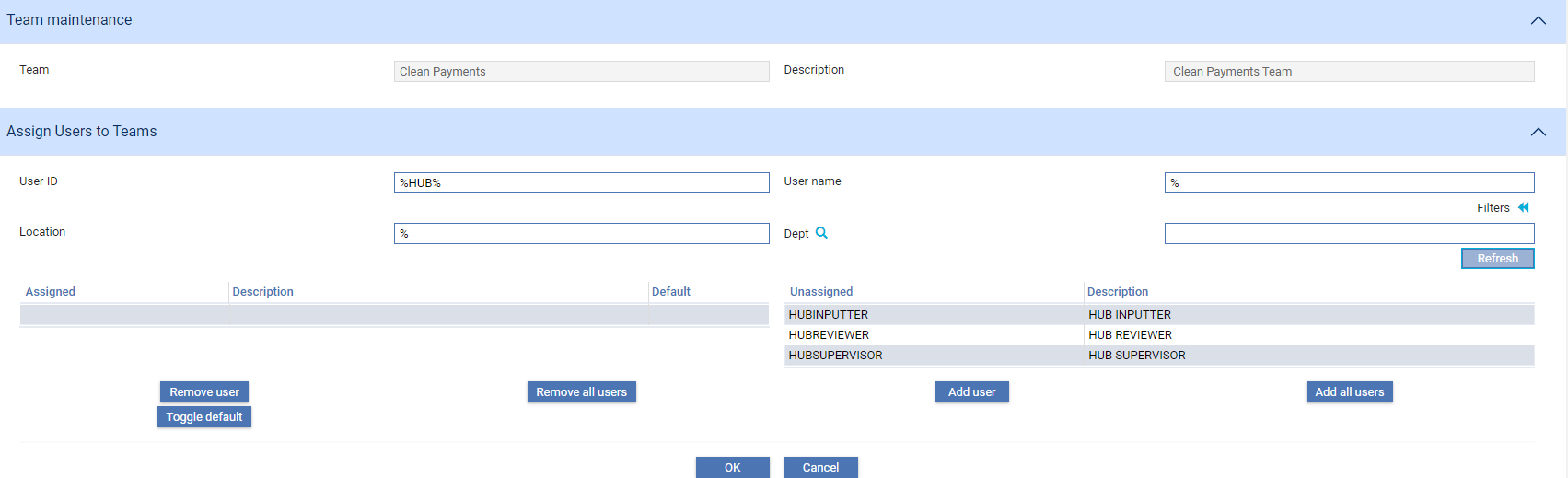
The window that is displayed lists all the users that have already been assigned to that team, and those that have not.



Filter fields allow you to narrow the list of users not assigned to the team to those meeting certain criteria. The window initially displays filter fields for unique user ID and user name. Clicking the  toggle button displays additional filter fields for location, branch and department.



The system returns users matching the criteria you have entered.



The Assigned list shows users already assigned to the team.

The Unassigned list shows users who have not yet been assigned to the team.

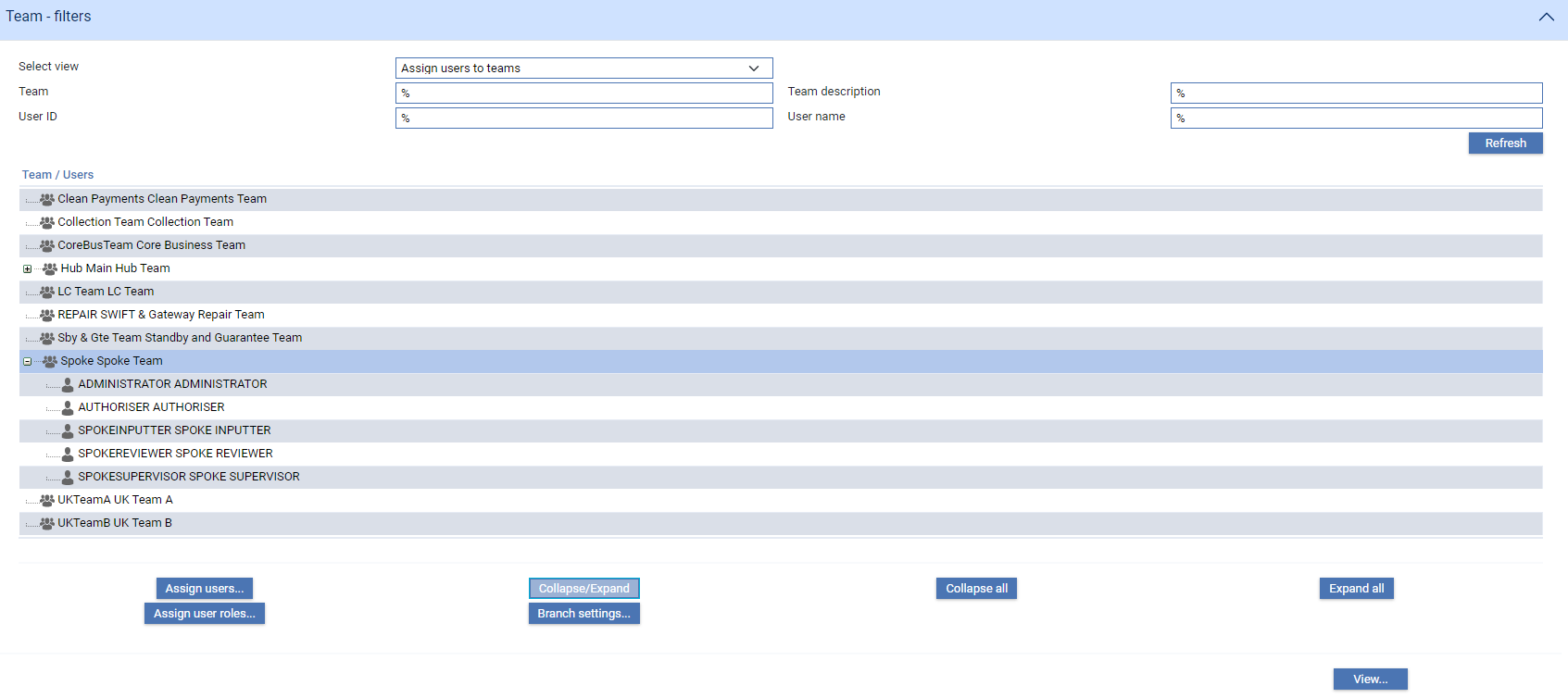
The Add User button allows you to assign a user to the team - highlight the user in the Unassigned list, then click **Add user**. The user is moved from the Unassigned list to the Assigned list. The Add All Users adds all the users in the Unassigned list to the team in one go.

The Remove User and Remove All Users buttons allow you to select and remove users in the same way.

The Toggle Default button is used to set the current team as the default team for a user. The Default column in the Assigned list indicates whether the current team is their default team (Y) or not (N). Select the user in the Assigned list, then click **Toggle default**. If the current team is not already the user's default team (N), then it is made the default (Y). If it already the default, then status as default team is removed for the selected user.

### Assigning User Roles to Users

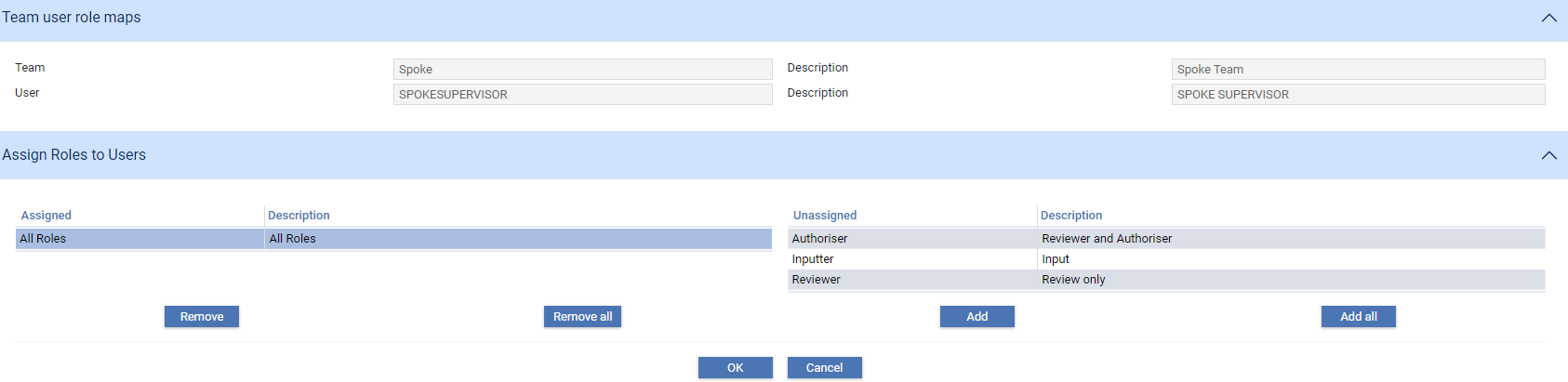
Select 'Assign Users to Teams' in the Select View field. The window changes to display new buttons and filter fields that you can use to search for the team for whose users you want to assign user roles.



If you perform a search, the system displays each team that meets your search criteria, with the users already in each team listed below it.

Highlight the user to whom you want to assign user roles, then click **Assign user roles**.

1. Since users may be members of more than one team, ensure that you select the correct team/user entry.



The Assigned list shows user roles already assigned to the user in this team.

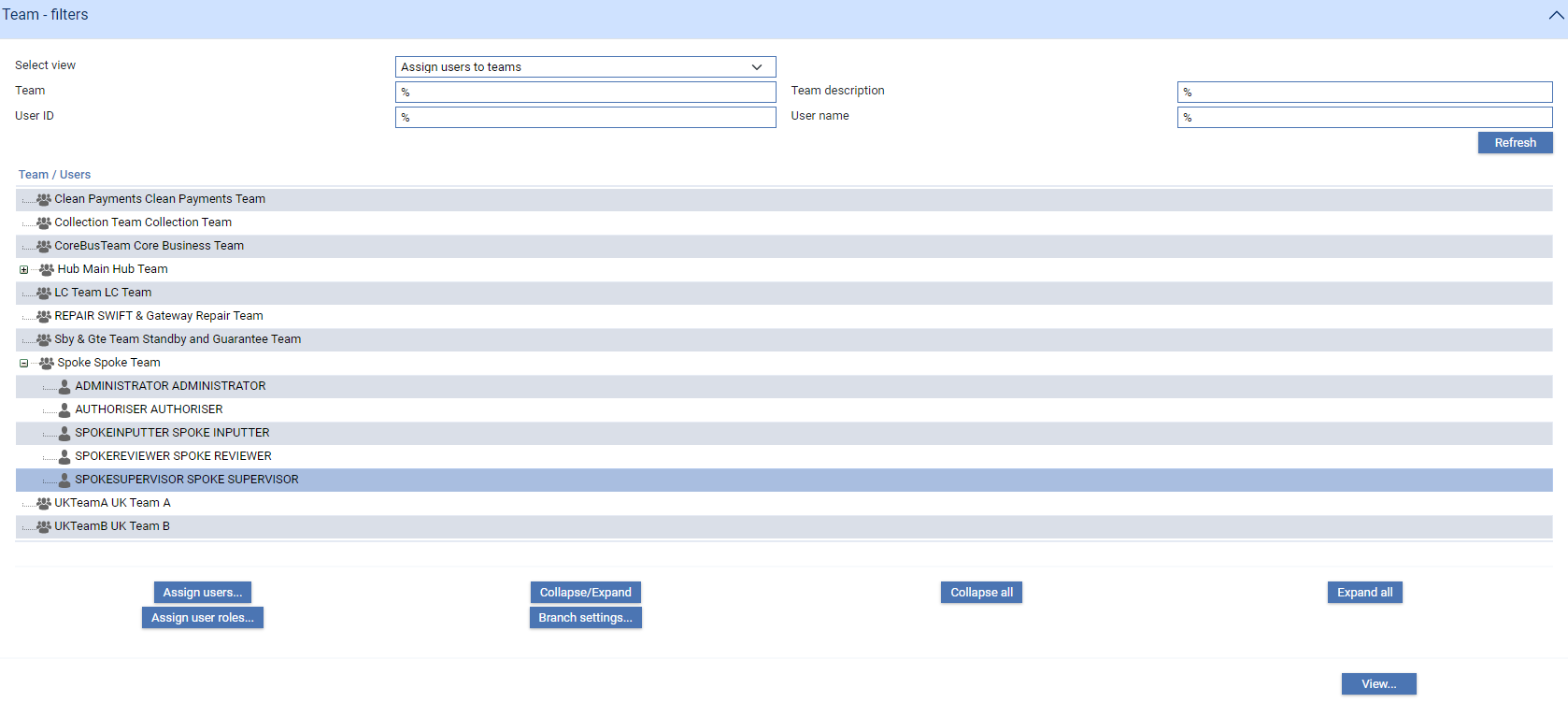
The Unassigned list shows user roles assigned to the team but not to the user.

The Add button allows you to assign a user role to the user- highlight the user role in the Unassigned list, then click **Add**. The user role is moved from the Unassigned list to the Assigned list. The Add All adds all the user roles in the ID list to the user in one go.

The Remove and Remove All buttons allow you to select and remove user roles in the same way.

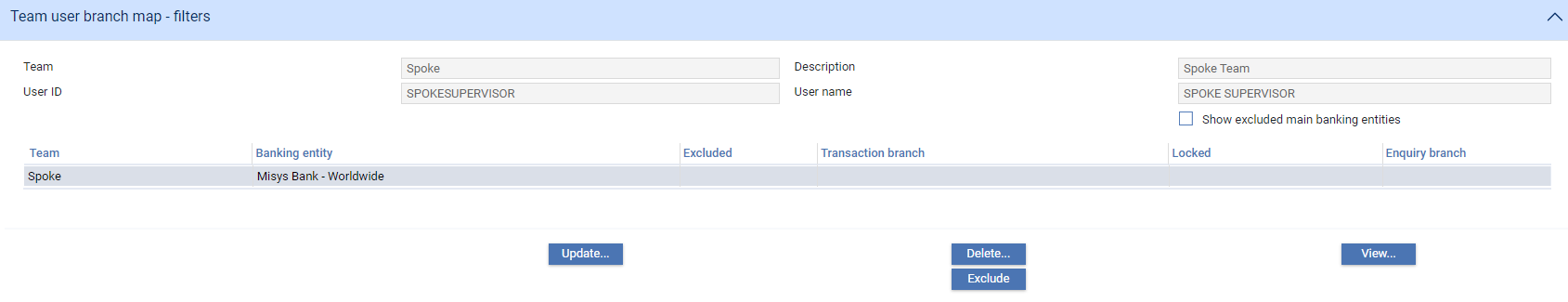
### Assigning Transaction and Enquiry Branches to Users

Select 'Assign Users to Teams' in the Select View field. The window changes to display new buttons and filter fields that you can use to search for the team to which you want to add users.



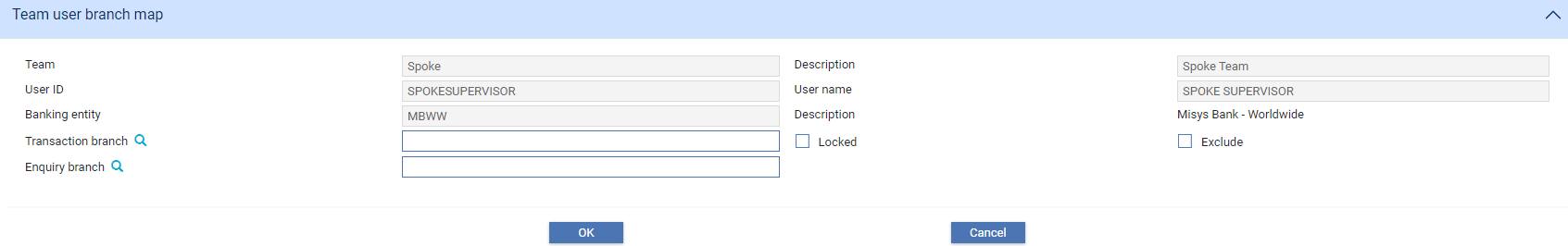
To assign branches to a user highlight the user, then click **Branch settings**.

1. Since users can belong to different teams, and since you can set different transaction and enquiry branches for a user within different teams, ensure that you select the user entry listed under the correct team here.



In the window that is displayed the system provides information about the selected team and user, and lists all the banking entities assigned to that team. Any settings already entered for that user are also displayed.

You can set a different transaction branch and enquiry branch for each banking entity assigned to the team. Highlight the banking entity for which you want to enter settings, then click **Update**.



The ‘Lock’ feature enables you to limit the branches that a user can enter transactions for to just the single branch entered for the main banking entity that the branch belongs to.

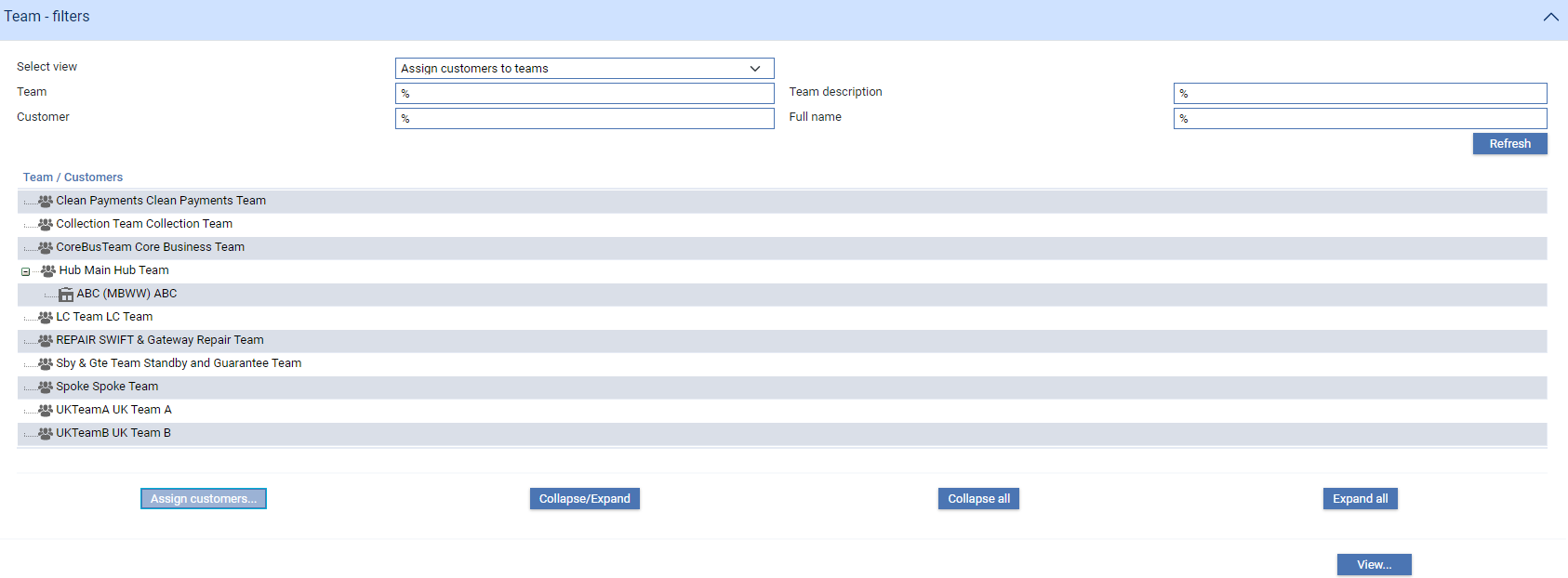
There may be more than one banking entity shown in the list for the team, where a team is able to process transactions on behalf of more than one part of the bank’s business.

The ‘Exclude’ button enables you to lock the user out completely from one or more of the main banking entities listed. This means they cannot work with any of the transaction branches associated with that main banking entity. This enables you to set up a team covering a particular process in the business across more than one main banking entity, Users can then be granted rights to all or some of the entities as required. Within non excluded entities, rights can be tailored down to an individual branch access level, where required for individual users.

### Assigning Key Customers to a Team

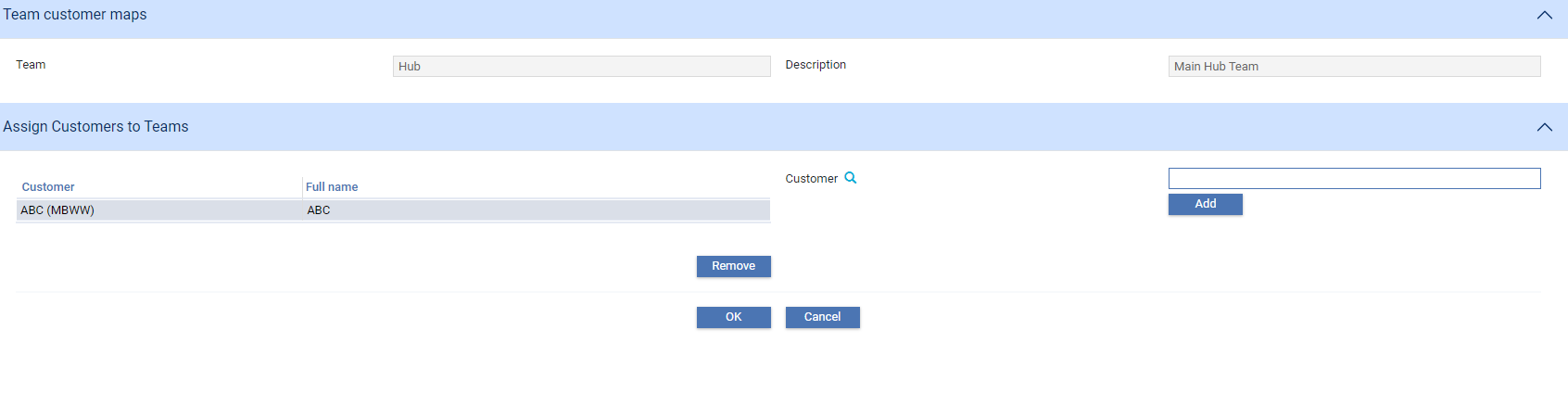
A key customer is defined as a significant customer that you want to view at a detailed level on the SLA dashboard graphs when viewing work for a team. Any team can have one or more such customers identified.

Select 'Assign Customers to Teams' in the Select View field. The window changes to display new buttons and filter fields that you can use to search for the team to which you want to add key customers.



If you perform a search, the system displays each team that meets your search criteria. If a team has already has key customers assigned to it, they are listed below it.

To assign a key customer to a team highlight the team, then click **Assign** **customers**.

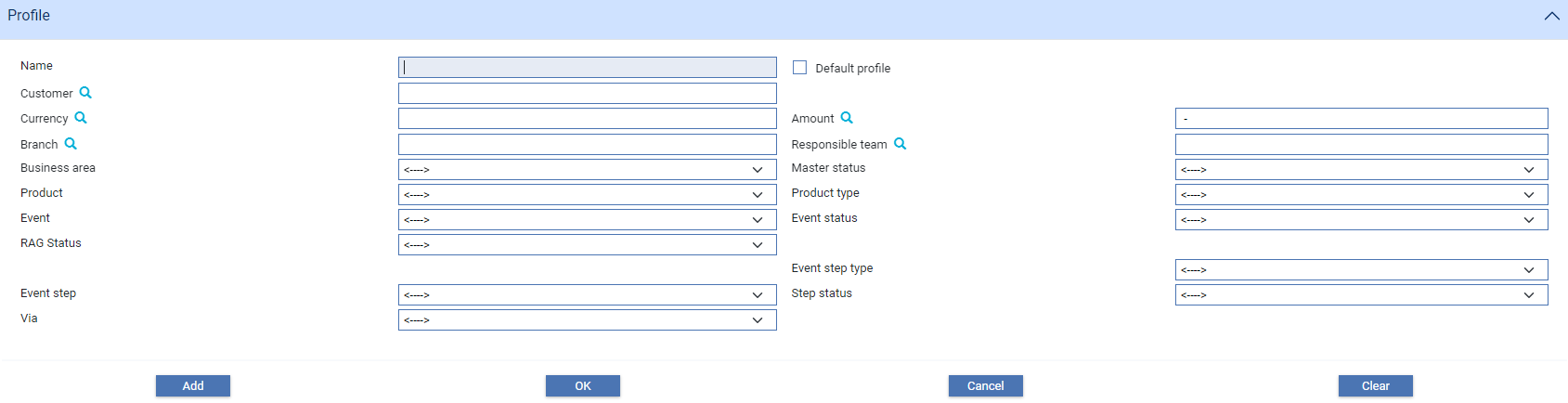


The window that is displayed lists any key customers already assigned to the team. The Customer field allows you to browse for additional customers to add to the list. As you close the browser, the code of the customer you selected is displayed in the Customer field. Click **Add** to add it to the list of key customers for this team.

The Remove button allows you to delete a key customer from the list - highlight the customer to be deleted, then click **Remove**. The customer is removed from the list immediately.

## Setting Up Team Profiles

The Security|Team Profiles menu option allows you to set up profiles for a team, amend or delete existing ones, and change a team's default working profile. Working profiles provide default values for the filter fields in the Masters window. See the Common Facilities User Guide – Trade Innovation for information on how working profiles are used.



To create a new working profile, select the team you wish to create the profile for using the Team field. Then set the filter fields as required - the table at the end of this section explains what to enter into the fields in this window.

You can also base a team profile on an existing one. Use the Select Profile field to select an existing working profile, on which the new one is to be based. When you click **Refresh** the fields in the Details pane change to show the values for the selected working profile. Overtype these values as required.

To save the new working profile, type its name into the Save Profile As field and click **OK** to save it.

|  |  |
| --- | --- |
| Field | What it Determines |
| Branch | Limits the display to transactions belonging to a particular branch. (Available only if the security officer has specified that you can work with master records belonging to branches other than your own.) |
| Responsible Team | Limits the display to transactions whose master record belongs to a particular team. (Available only if the security officer has specified that you can work with master records belonging to teams other than your own.) |
| Assigned Team | Limits the display to events belonging to a particular team. (Available only if the security officer has specified that you can work with master records belonging to teams other than your own.) |
| Business Area | Used to select the business area that includes the product(s) and events you wish to work with. |
| Product | Limits the display to transactions belonging to a specific product. If you have specified a business area in the Area field, then the field will include products in that business area only. |
| Product Type | Limits the display to products belonging to a particular product type. |
| Event | Limits the display to transactions for which the specified event exists. You must specify a product first and click Refresh.  Using the Event filter field enables the Event Step and Event Status filter fields, allowing you to search for events which are active at a particular step or with a particular status. This allows you, for example, to look for events that are awaiting review or authorisation. |
| Event Step | Used in conjunction with the Event field to specify whether the event defined there must be active at a particular step or not. |
| Master Status | Limits the display to transactions whose master records have the specified master status. |
| Step Status | Used in conjunction with the Event and Step fields to limit the display to events including the specified active step at a particular status. |
| Priority | Limits the display to events with the specified priority setting. |
| Watch List Check - User Action | Limits the display to events with the selected watch list checking user action. |
| Customer | Limits the display to transactions for customers matching the criteria provided. The system matches the criteria entered against either the principal party or the non-principal party in the master record. |
| Currency | Limits the display to transactions in the specified currency. |
| Amount | Limits the display to transactions for the specified amount. |

To change the default working profile for a team, select the new default working profile in the Select Profile field. Then check the Default Profile For This User/Team field. When you click **OK** to close the window, the new default working profile takes immediate effect for all users who subsequently log on to Trade Innovation.

# Capabilities and Security Groups

This chapter covers capabilities and security groups. It explains how they control access to Trade Innovation functionality, and provides instructions on setting them up.

1. Capabilities are used to control access to functionality used for purposes other than transaction processing. Access to transaction processing is controlled by user roles and master-level tasks, as described in Chapter 5. The security groups described in this chapter are used in conjunction with capabilities, but not user roles or master-level tasks.

## Access Rights within Trade Innovation

Access to Trade Innovation's transaction processing functionality is controlled by user roles and how they are assigned to users within teams.

Access to other Trade Innovation functionality is controlled by capabilities.

Each Trade Innovation application (other than the transaction processing application) has a capability that controls access to it. Additional capabilities can then control access to certain functionality within that application. For example, all users with access to the static data maintenance application can view existing static data; but the functionality used to amend static data can be restricted to certain users only.

See page 68 for the list of all the Trade Innovation capabilities and what each of them controls.

Each capability has a default availability mode, which can be set to be one of the following values:

|  |  |
| --- | --- |
| Mode | What It Allows |
| Public access | By default, the functionality is available to all users who have access to the relevant application. It can be performed by all users, except those who are explicitly denied access to it.  Public access cannot be assigned to a ‘Security’ capability |
| Security controlled access | By default, the functionality is unavailable. It can be performed only by users who have access to the relevant application and who are explicitly permitted access to it. |

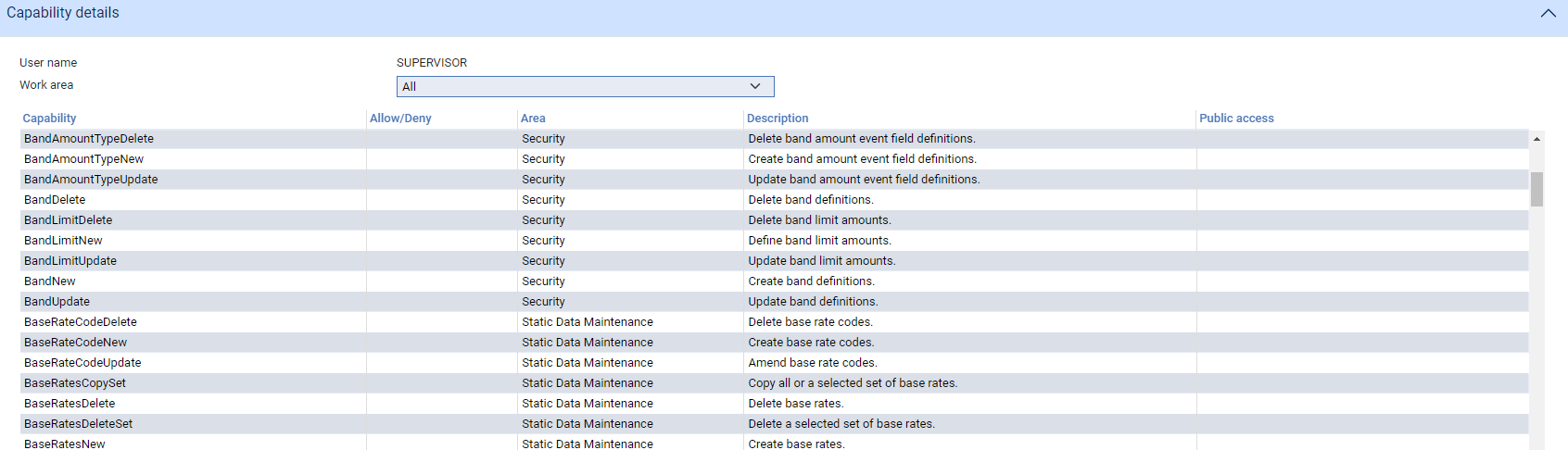
When the Trade Innovation is first installed, each capability has a default mode of 'unavailable', meaning that no-one can access the functionality it controls. Your bank can change this mode to 'public access' to allow all users to access that functionality, or leave the access as 'unavailable' and then set the capability for individual users.

At run-time, the system checks what functionality the user is permitted to use as they log on. It displays only those applications that they have access to; and, when they open an application it makes available only the functionality that either is not capability-protected or is capability protected but has been made available to that user.

For users without permission to use certain capabilities either the menu options and buttons are disabled, or else the system displays an error message when the user attempts to access them.

### Viewing Your Own Capabilities

While in Trade Innovation's security application you can view your own capabilities using the Current Capabilities|Current Capabilities menu option.



The system lists all the capabilities you are authorised to use. You can scroll through the list, but you cannot change anything.

You can use the Work Area field to limit the display to capabilities for a certain business area only, see page 68.

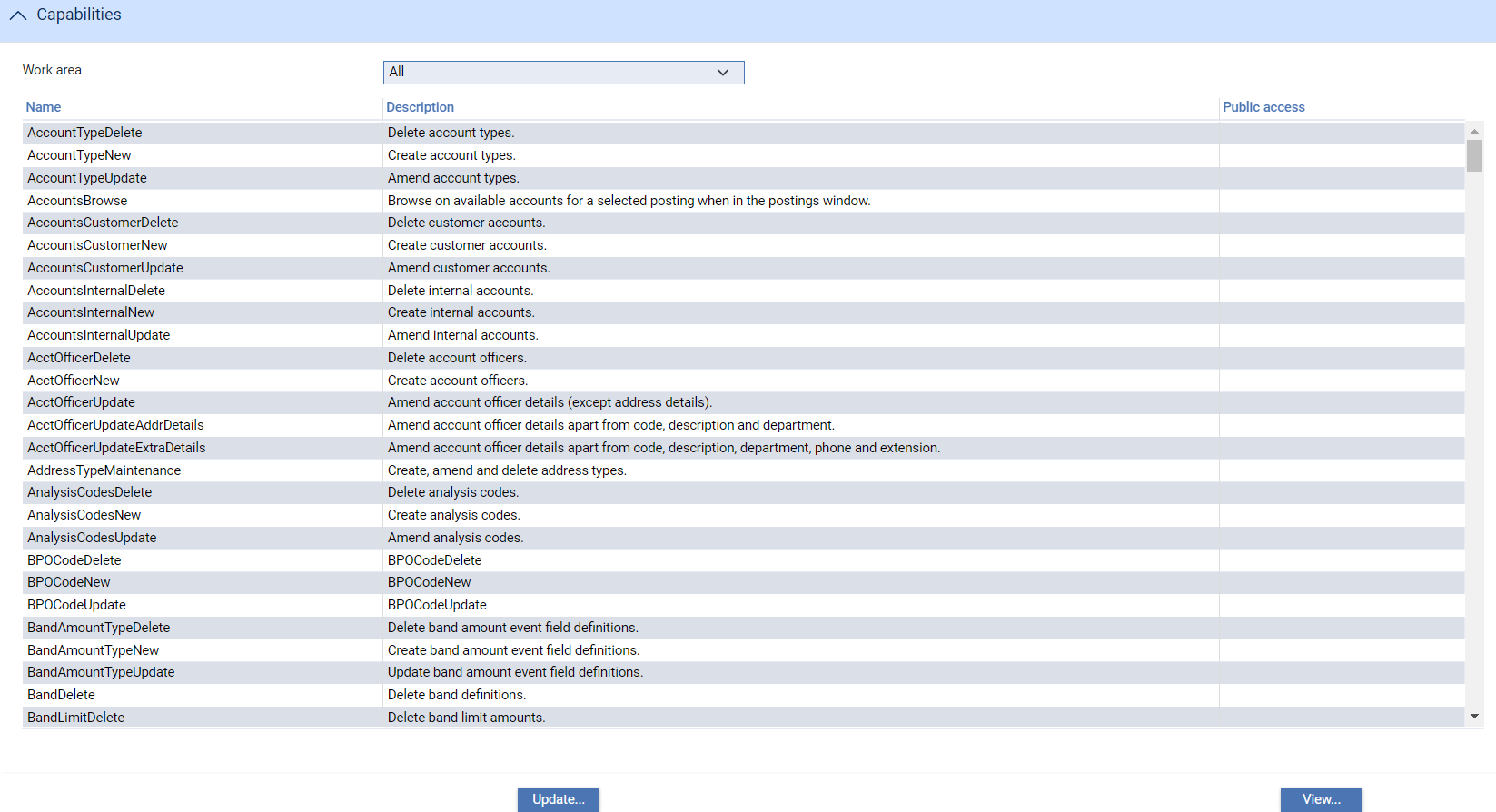
### Security Groups

The Trade Innovation security application allows you to organise users together into security groups and then set capability-controlled access rights at group level (see page 51), as well as at individual user level. This allows your bank to set capabilities up for a number of users at the same time, rather than having to set them for each individual user in turn.

Each user within a security group is able to use all the functionality available to that group. Users can belong to more than one security group; and additional access rights can be set for individual users outside of any security groups to which they belong.

## Setting the Default Availability Mode for Capabilities

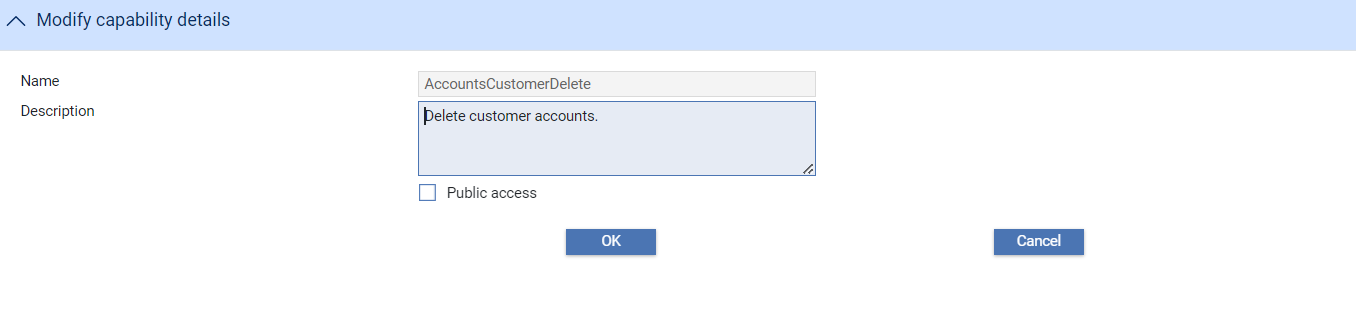
In the Trade Innovation security application, select the Security|Capabilities menu option.



This window lists all capabilities, but can be restricted to capabilities for a particular business area using the Work Area field.

To view details of a capability, and to change its settings, select it and click **Update**.

### Viewing and Amending Capabilities



In the window that is displayed when you click **Update** you can amend the description of the capability and its public access mode.

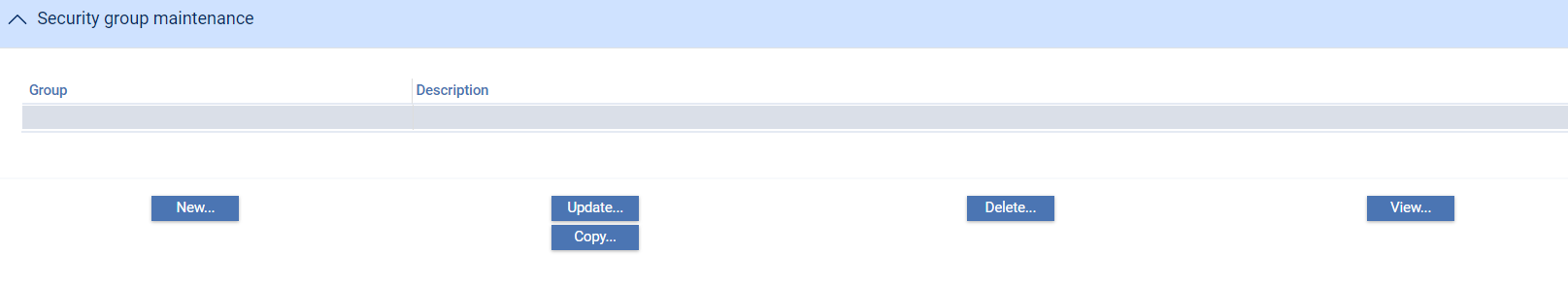
If the Public Access box is blank, then the functionality is by default unavailable. It can be performed only by those users who are explicitly permitted access to it.

If the Public Access box is checked, then the functionality is available to all registered users by default. It can be performed by all users, except those who are explicitly denied access to it.

## Defining Security Groups

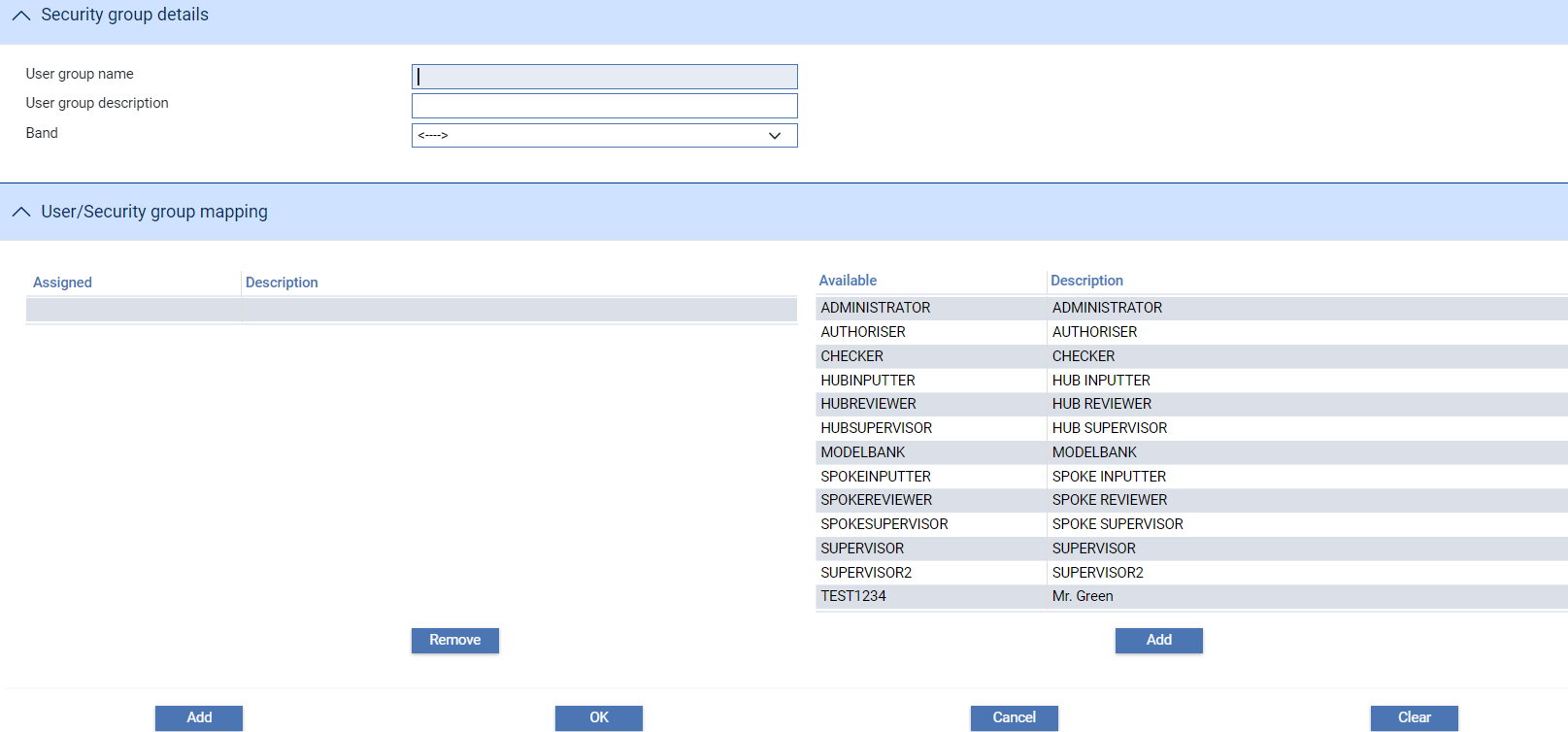
Trade Innovation users can be grouped together for administrative convenience when setting up capability-controlled access rights. If your bank employs a large number of users who all need access to the same capabilities, this enables you to group them all together and then set and maintain access rights for that group, rather than for each of the users within it individually. Users can be assigned to security groups as the users are set up or when a security group is defined, as explained in this section.

In the Trade Innovation security application select the Security|Security Groups menu option.



When you select this option, the system lists all currently defined security groups. The buttons can be used to view, amend and delete existing user details and to add new users in the usual way.

To define a new group, click **New**.



The following table lists the fields in this window and explains what to enter into them to define a new security group and assign users to it:

|  |  |  |
| --- | --- | --- |
|  | Field | What to Enter |
|  | User Group Name | A unique identifier for the security group. |
|  | User Group Description | A description of the security group. |
|  | Band | The staff band to which the user belongs. See Chapter 8 for more on how staff bands are used. |
|  | Assigned/Available | These panes are used to assign users to the security group. The Available pane lists all the users set up on your system who are not assigned to this security group. To assign the user to a security group, select the user in the Available pane and click **Add**. The entry is moved to the Assigned pane. |
|  |  | When you subsequently view the security group's details, the Assigned pane will show the users assigned to the group, and the Available pane the users not assigned to the security group.  You can remove a user from a security group by selecting the user in the Assigned pane and clicking **Remove**. |
|  |  | Users can also be assigned to security groups via the menu option used to enter and amend user details. |

## Setting Access Rights for Users and Security Groups

By default, users have access to restricted capabilities according to the availability mode set for each area. As security officer you can override the availability mode either to deny individual users or security groups access to publicly available functionality, or to allow them access to functionality that is not publicly available.

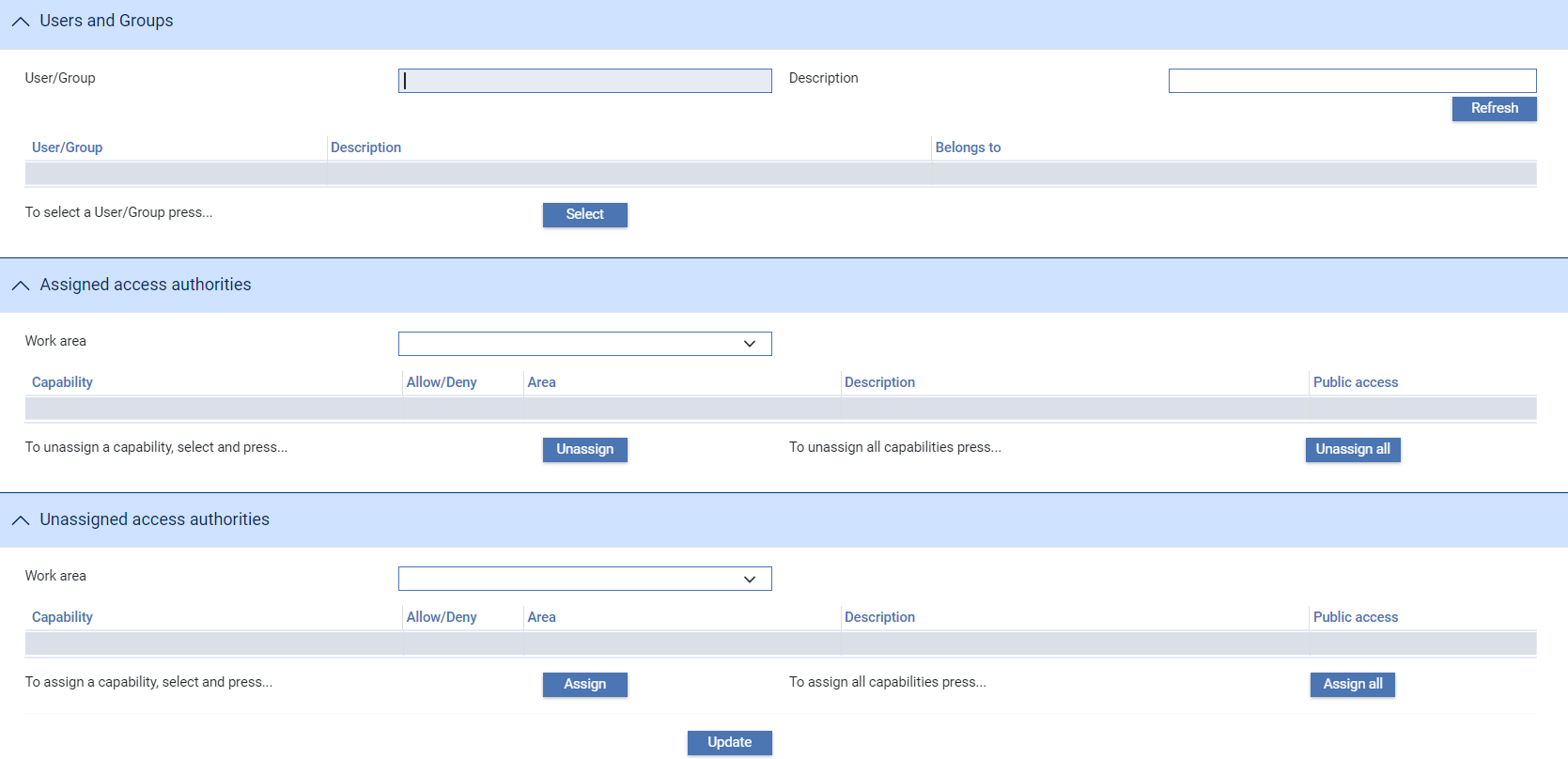
The simplest way of setting access rights is to leave the default availability mode for each capability set to 'unavailable', as it is when the system is first installed. You can then override the availability mode setting to make each capability available to certain users or groups of users only.

It is possible to assign a capability to a user or a security group, but to still deny individuals within that group permission to use it.

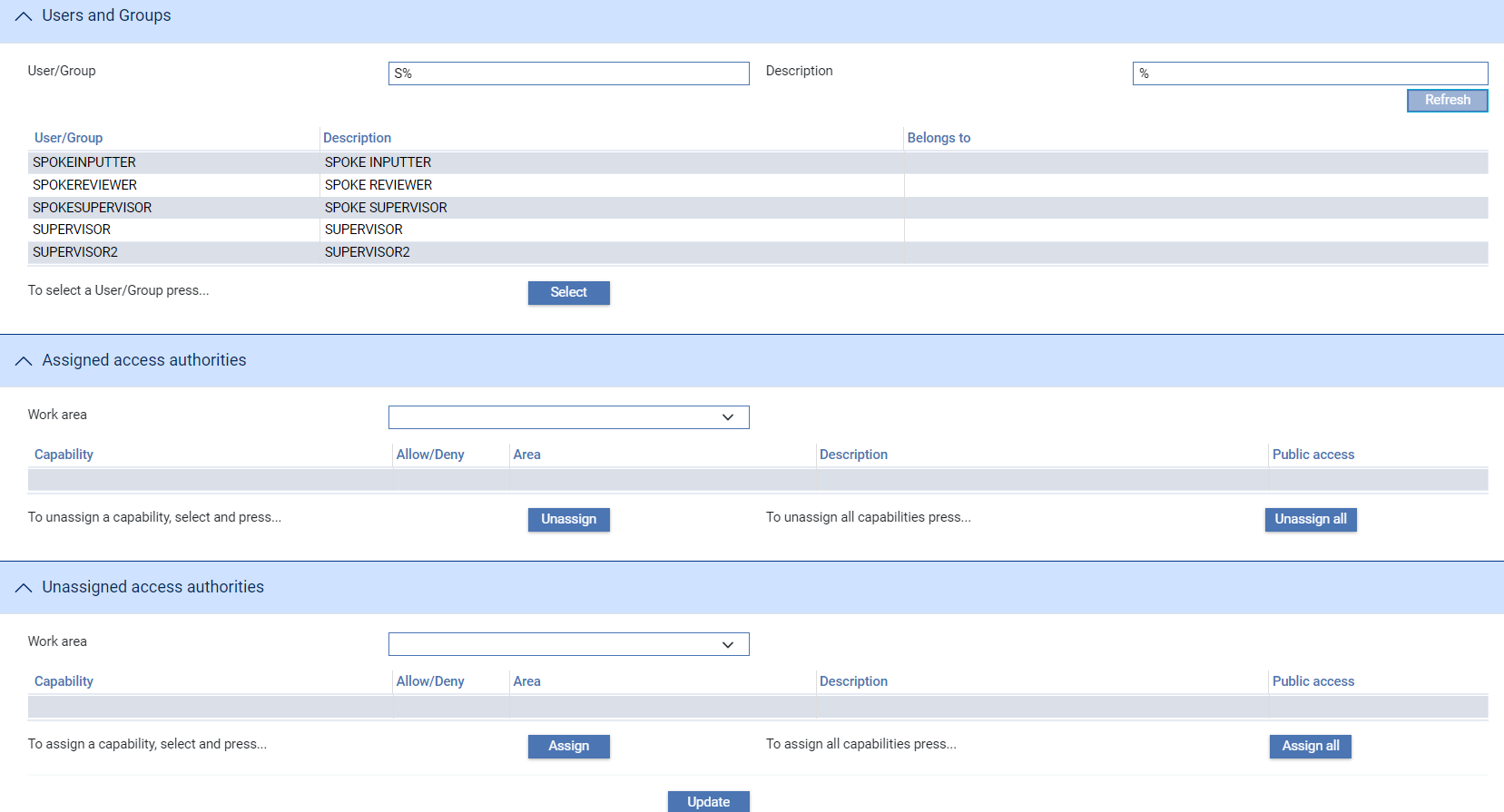
At run-time, the system establishes which capabilities a user has access to in the following way:

* Access rights set at individual user level override or extend access rights set at security group level or by a capability's default mode
* Access rights set at security group level override access rights set by a capability's default mode
* A capability's default mode is applied as the default for all users for whom no overriding permission has been set at either user or group level

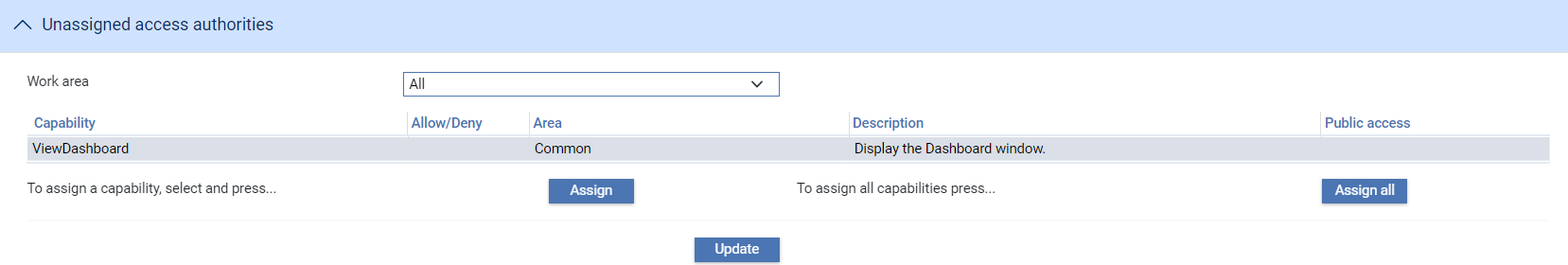
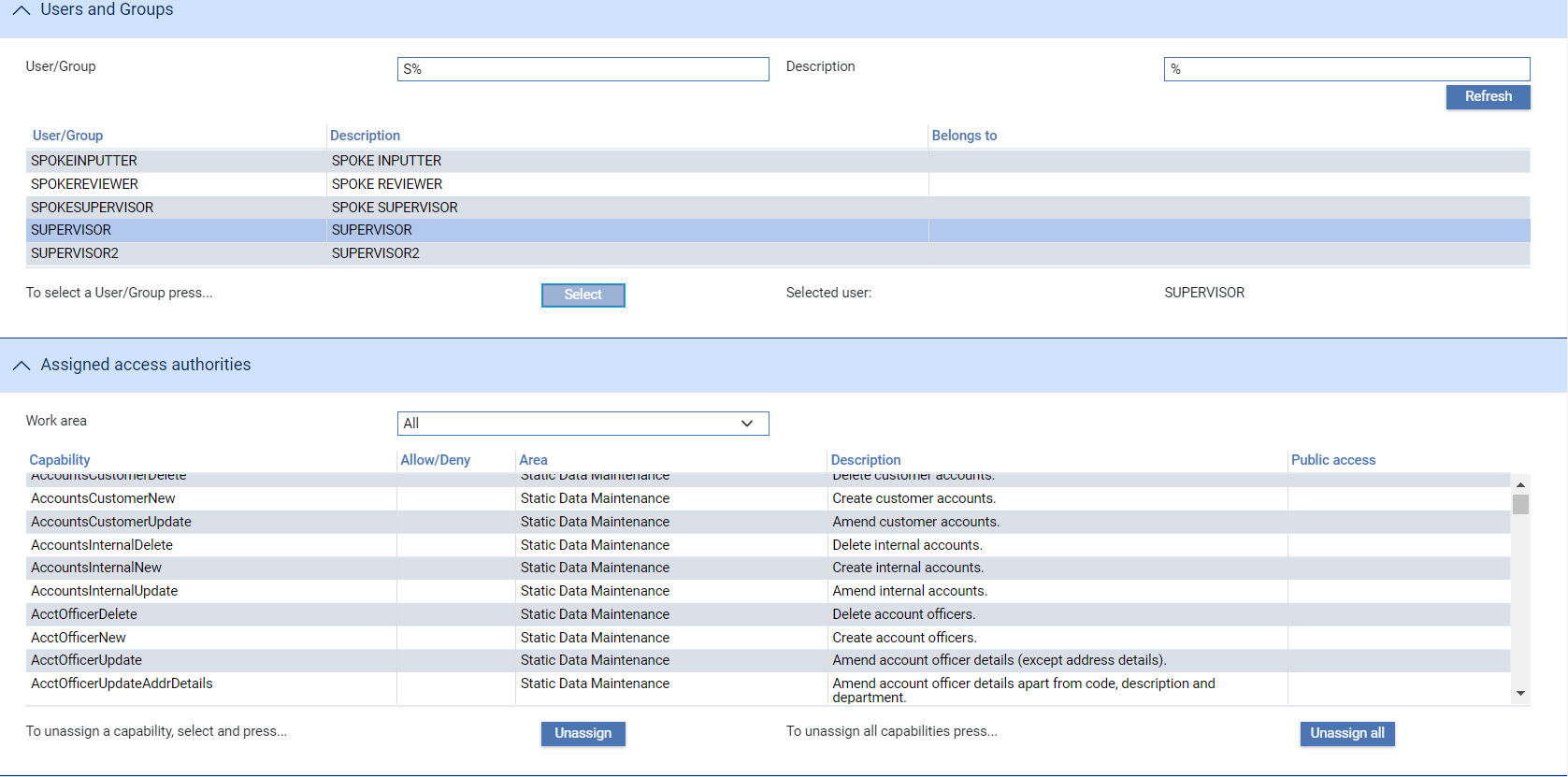
To assign capabilities to users and security groups select the Security|Capability Map menu option.



Use the filter fields at the top of the window, if required, then click **Refresh**. The Users and Groups pane lists all the security groups and users set up on your system. If you used the filter fields this list will be limited to those matching the criteria you entered. For users, the Belongs To panel lists any security groups to which the selected user belongs.



When you highlight a user or security group and click **Select**, the Assigned Access Authorities pane displays all capabilities already assigned to them, and the Unassigned Access Authorities panel all capabilities not assigned to them.



In the Unassigned Access Authorities panel, the Allow/Deny column indicates whether a capability is publicly available (in which case the column displays the text 'Public') or whether it is by default unavailable (in which case the column is blank).

In the Assigned Access Authorities panel, the Allow/Deny column indicates whether the selected security group or user is authorised to use a capability, and whether authorisation is at security group level or an individual user level. The following table lists all the values that may appear in this column and explains what they mean.

|  |  |
| --- | --- |
| Value | What it Indicates |
| Public | A publicly available capability has been assigned to the user with no denial override. The user is therefore authorised to use the capability. |
| (blank) | A capability that is not publicly available has been assigned to the group or user with no denial override. The user is therefore authorised to use the capability. |
| Group Allow | Displayed for users only.  A capability that is not publicly available has been assigned to a group to which the user belongs. The user is therefore authorised to use the capability by virtue of their membership of that group. |
| Deny (Group Allow) | Displayed for users only.  A group to which the user belongs has been authorised to use a capability that is not publicly available. However, the user has been denied authorisation. The user cannot therefore use the capability, since user-level settings override group-level ones. |

To assign capabilities to a new user or security group, select the relevant entry in the Users and Groups pane and click **Select**.

In the Unassigned Access Authorities pane highlight each of the capabilities to be assigned to the user or security group in turn and click **Assign**.

The capability is moved from the Unassigned Access Authorities pane to the Assigned Access Authorities pane.

A capability can subsequently be removed from a user by highlighting it in the Assigned Access Authorities pane and clicking **Unassign**.

The Assign All and Unassign All allow you to assign and unassign all capabilities in one go.

Click **Update** to save the changes you make to each individual user or security group.

# Restricting Access by Event Amount

This chapter explains how to use Trade Innovation to restrict user access to events at the step level by amount.

## Restricting Access by Event Amount - Overview

The system is delivered with security features which permit you to restrict user access to events at the step level. These features permit you to create a staff banding structure which defines, for each band, the maximum amounts users in that band are permitted to input, review and authorise.

Users are then allocated to a staff band, either individually or via their user group.

You identify those events to which you wish to restrict access by selecting the field that is to be used for comparison with the amounts set up for staff bands.

When a user attempts to open an existing event, the system first checks whether the event is protected in this way.

If so, it then checks the user's staff banding level and identifies the maximum amount set up for that band for the step at which the user is attempting to open the event. It compares that amount with the amount in the field identified as the one to be used for comparison for this event. If the event field amount is the same as or less than the staff banding amount for the relevant step the user is permitted to open the event and complete the step; otherwise an error message is issued and the user is prevented from opening the event.

If the user has an individual limit approval amount set up then, if it is greater than the amount provided by the user's staff banding level, it is used instead in the checks described above.

Where the amounts involved are in different currencies, the system converts the transaction amount to the currency of the staff banding amount.

For new events which are protected in this way, the amount involved will not be known until the event has been opened and the amount entered.

When the user attempts to complete an Input step of a new event, the system again checks whether the event is protected the way described in this chapter. If so, it compares the maximum amount set up for an event's Input step on the staff band to which the user belongs against the relevant event amount field. If the event amount is the same as or less than the staff band amount the user can complete the Input step; otherwise an error message is displayed and the event is saved at the Log step instead.

1. Staff bands can also be used to restrict what transactions a user can input, review and authorise, regardless of the amount involved by setting up bank-defined error messages and warning messages. The database field Current User Band can be used to define the error messages to be produced if a user who does not have the required staff banding level attempts to complete a step. This facility can be used where, for example, a band limit is generally applicable to most products but your bank wants to ensure that, for certain products, the user needs to belong to a higher staff band to be able to perform review or authorisation. See the System Tailoring User Guide – Trade Innovation for instructions.

## Implementing Amount-based Security

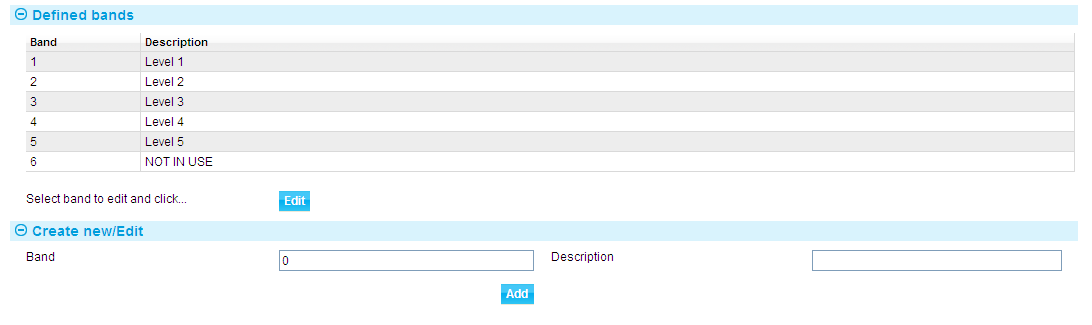
The security features described in this chapter are implemented using the UseEnhancedSecurity system option, as described in the System Tailoring User Guide – Trade Innovation. Until you set this system option to 'Yes', the menu options described in this chapter are greyed out.

Implementing event-level security has the following stages:

* First set up the staff bands
* Then set up the limits to be applied for users in that band at the Input, Review and Authorise (Final review) steps
* Identify each of the events that is to be protected and, for each event, identify the field to be used for comparison against users' limits
* Finally, you must ensure that each Trade Innovation user is allocated to a staff band

## Setting up Staff Security Bands

Staff security bands are set up using the Limits|Maintain Bands menu option.



When you first use this menu option the Defined Bands pane will be empty. Subsequently it will list those bands your bank has already set up.

For each band in your structure, enter the number of the band into the Band field and a description into the Description field, then click **Add**. The band is added to the list in the Defined Bands pane.

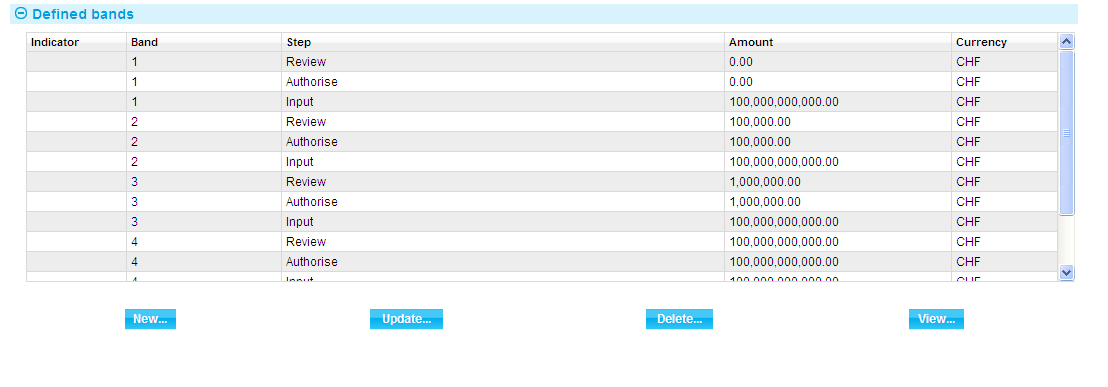
The values you enter are listed in the Defined Bands column in numerical order.

If you need to amend either of the values for a particular band you can do so by highlighting the relevant entry in the list and clicking **Edit**. The existing values are displayed in the input fields, where you can overtype them. Click **Update** to save any changes.

You can enter up to 99 bands. Once a band has been added it cannot be deleted. If a band becomes obsolete, you can change its number and description to values that indicate this.

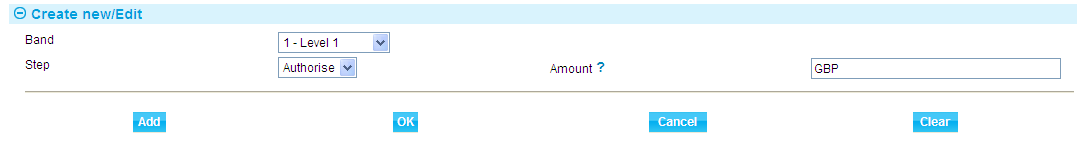
## Setting Limits for Staff Bands

Limits are set up against staff bands using the Limits|Processing Band Limits menu option.



When you first use this menu option the Defined Bands pane will be empty. Subsequently it will list those bands for which your bank has already set up limits. You can amend and delete them in the usual way.

To set up limits click **New**.

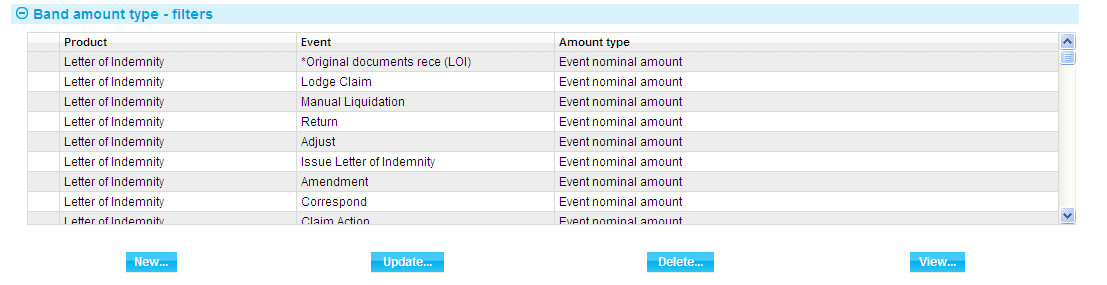


In the window that is displayed select the first band for which you wish to set up limits using the Band field and select an event step in the Step field. Enter the amount (with currency) to be used as a maximum limit for users in this band for that step into the Amount field. Click **Add** to save your input. You can now repeat the process for the second (and subsequent) bands.

When you close the window the information you have entered is listed in the Defined Bands panel.

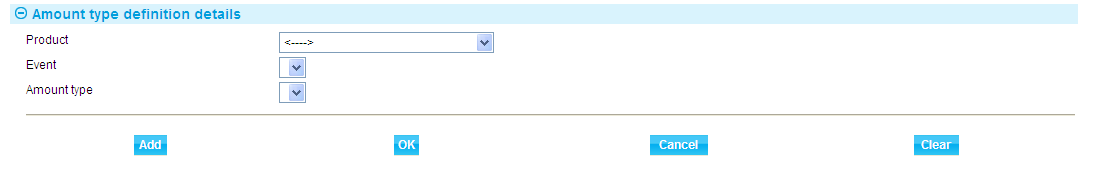
## Identifying the Events to be Protected

To identify the events to be protected and the fields to be used in comparisons select the Limits|Amount Definition menu option.



When you first use this menu option the Band Amount Type pane will be empty. Subsequently it will list the products and events for which your bank has already set up limit amounts. You can amend and delete them in the usual way.

To identify further events for which limit amounts are to be set click **New**.



Use the fields in the window displayed to select in turn each product and event to which access is to be restricted, then use the Amount Type field to identify the event field to be used in comparisons with staff band limit amounts. Click **Add** to save the information for each event.

## Allocating Users and Groups to a Band

Users are allocated to staff bands using the Security|Users menu option and the Security|Security Groups menu option. If you have security features described in this chapter implemented, a Band field is displayed when you select these menu options, which permits you to allocate a user or group to a staff band.

If a user is allocated one staff band, and then placed in a security group which has a different staff band allocated to it, the band defined by the user is used at run-time.

# User Management

This chapter explains how to use Trade Innovation to manage users and user log-on problems.

## Overview

The most common log-on problems users will encounter can be resolved by reference to user information set up at the global level using the User administration link (see page 22).

User profiles also include two flags that you can use to bar users from accessing the system, and to force a change of password. These are:

* The Account Enabled flag. When this flag is unchecked, it prevents users from logging on. This flag is unchecked automatically by the system whenever a user exceeds the maximum number of permitted log-on attempts. You must then reset it to allow the user to log on again. You can also set the flag manually to bar a user.
* The Force Password Change flag. When this flag is set, the user is required to change their password immediately after their next successful log-on. Until they do, they are prevented from performing any action other than logging off. This flag is set automatically when a change of password is due. You can also set it manually.

As a security precaution, if the user's password was changed by a different user, the force password check box will be automatically checked and will no longer be editable. This will then force the user to change their password when they log in to Trade Innovation.

A security officer can still override this by re-editing the user details and un-checking the force password change check box.

## User Log-On Problems

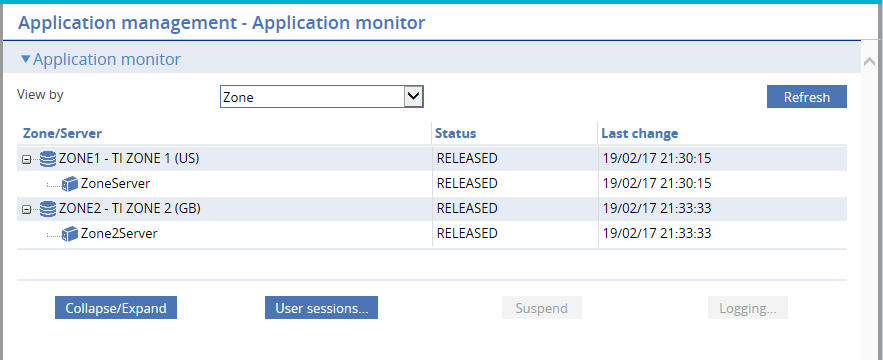
This section describes the most common log-on problems users will encounter and explains how you should handle them if Trade Innovation has been configured to manage user passwords.

1. As security officer you should be especially careful not to forget your user ID or password. If you are the only user registered with security officer privileges and you forget either your user ID or your password, you will not be able to log on. You will need to apply to Finastra International Banking Systems Ltd for assistance in regaining access to Trade Innovation.

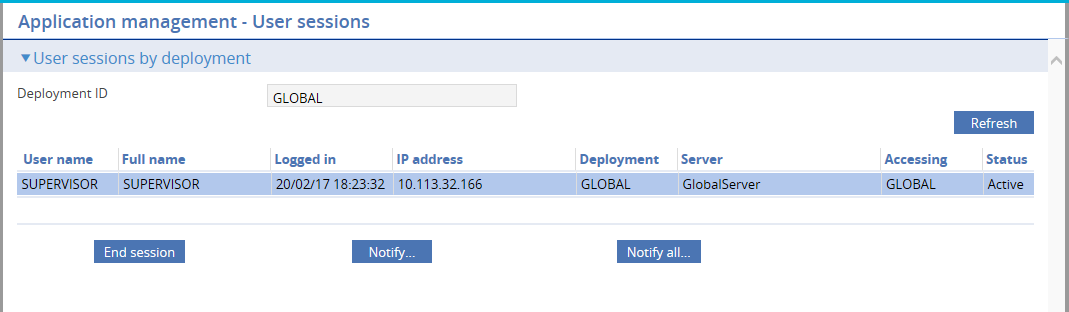
|  |  |
| --- | --- |
| If a user forgets their user ID | |
|  | User IDs are listed in the window displayed when you select the User Administration link. The user's name will allow you to identify the correct entry in this window and to provide the user with the correct user ID. |
| If a user forgets their password | |
|  | Access the user's profile using the User Administration link. Enter a new password.  Tell the user the password you have just entered for them. They will be able to use this password to log on, but will need to change it immediately after their next successful log-on. |
| If a user is barred after unsuccessful log-on attempts | |
|  | The user will have attempted to log on and will have failed after the permitted number of attempts.  Remind the user of their user ID. If they have forgotten their password, enter a new one for them, as described under the previous problem. |
| If a user is barred for some other reason | |
|  | The user may be barred because the Account enabled flag has been unchecked manually by you or by another security officer; or because their profile has been disabled because it has remained inactive too long or has reached its expiry date. Whether or not you remove the bar (by checking the field) depends on the reason why the user was barred.  As security officer you can reactivate a user profile whatever the reason for the Account enabled flag being unchecked; help desk users cannot reactivate user profiles that have been disabled because they reached their expiry date. |

## Monitoring User Sessions

The application monitor provides a security officer or system administrator with the ability to view users currently accessing the system by zone, deployment or server.



The Application monitor l link displays the status of servers within zones. This view may be changed by selecting Deployment or Server from the dropdown. On any view, the User sessions… button may be clicked after selecting an entry to show the users currently accessing that zone, deployment or server. The list of users may be restricted to those users accessing a particular server for a deployment or zone, depending on which row is selected.



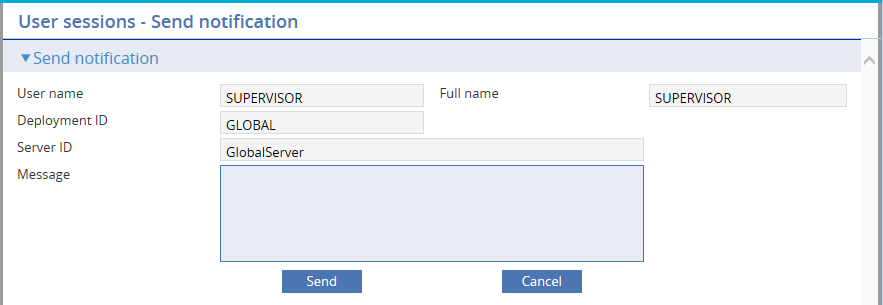
The page shows:

* The deployment, server or zone being accessed
* The user's log-on name
* The user's full name
* The date and time the user logged on. If they are logged on to a zone, this shows the time they logged on to the zone; otherwise it shows the time they logged on to the global process
* The IP address of the machine they are using to access the system
* The deployment they are currently using
* The server their session is located
* The ID of the zone they are accessing (GLOBAL reserved for the global application)
* Their current status – usually Active, though if there is currently a temporary outage to the deployment or server, they are marked as Unknown. Their details will be refreshed once the deployment or server re-establishes connection

The page allows you to end a user session, and to send a message to one or to all users.

To end a user session, select the relevant session and click **End session**. The user will be informed that their session has been ended, and logged off when they next access the server.

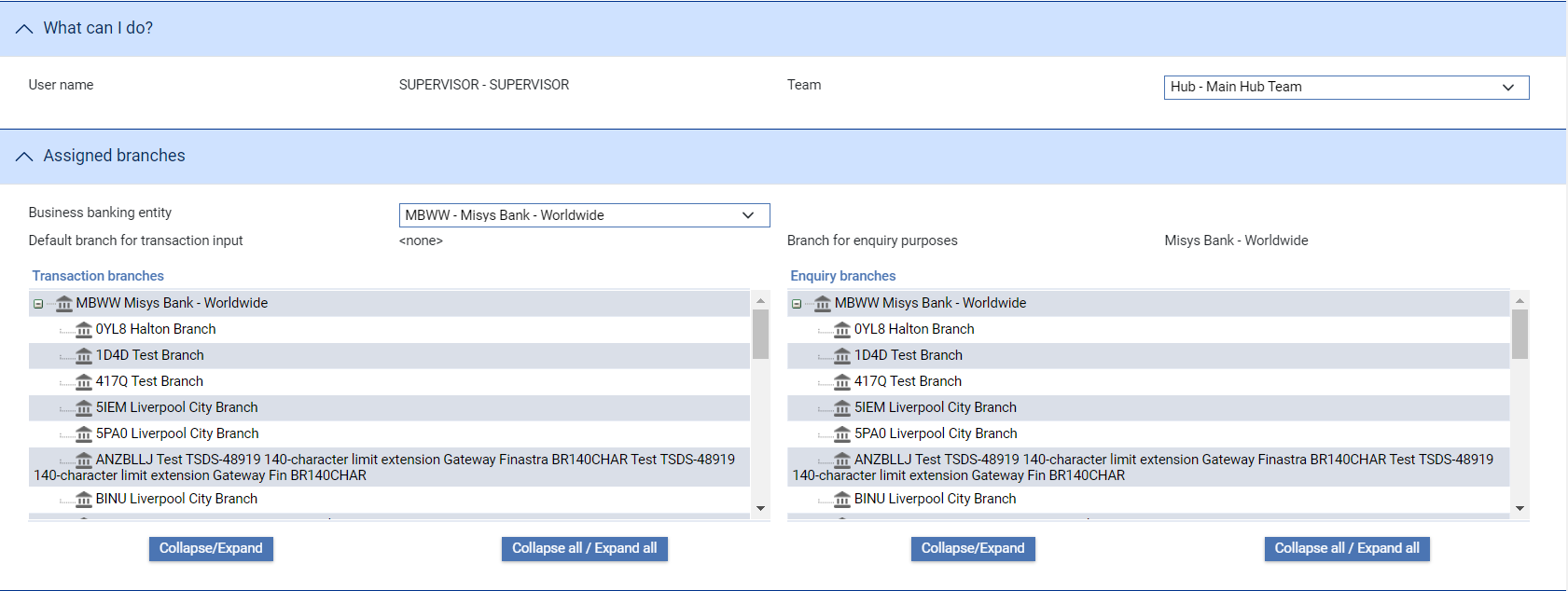
To send a message to an individual user session, select the session, then click **Notify…**. To send a message to all user sessions listed click **Notify all…**.

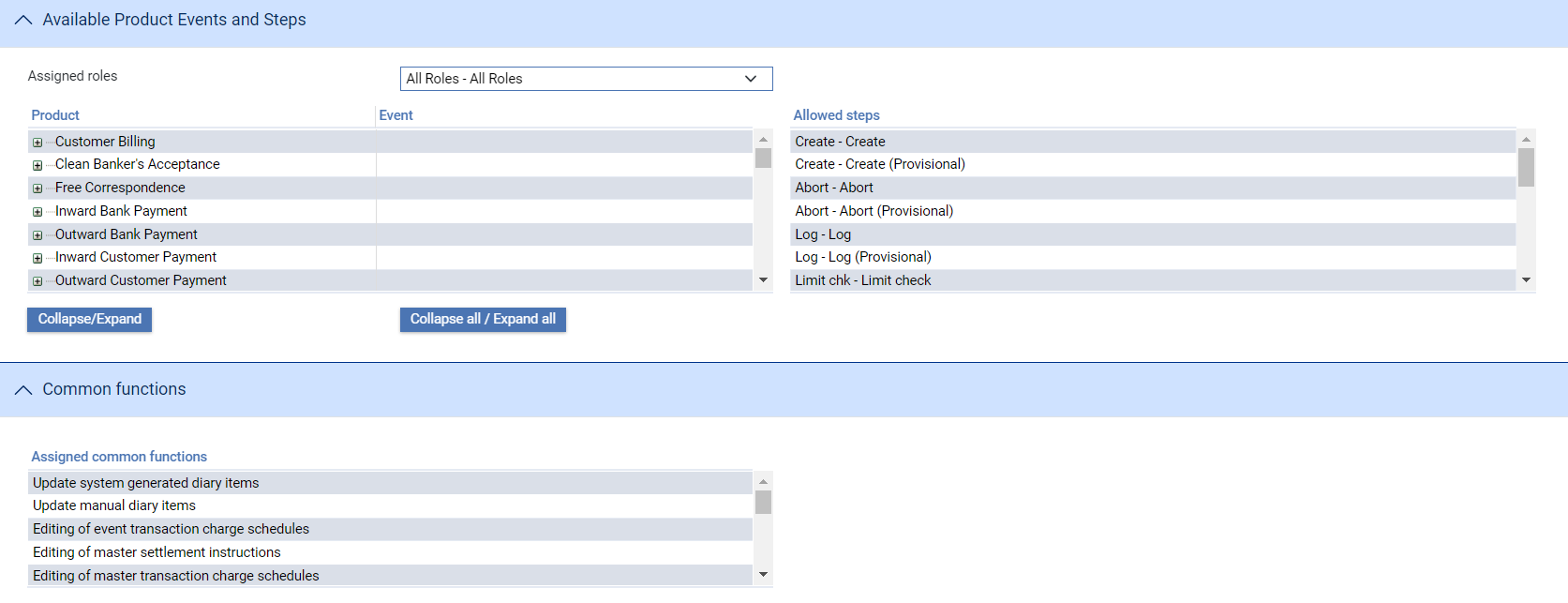


On the page that appears type your message, then click **Send**.

### Viewing What Other Users Can Do

The security application's Security|User/Team/Role Enquiry menu option allows you, as security officer, to view information about your, and other users', access to Trade Innovation's transaction processing functionality.





When you initially open this window it shows information for yourself.

The Teams drop-down field lists all the teams you are assigned to. When you select a team the Business Banking Entity drop-down list is populated with the business/banking entities that the team is associated with. When you select a team and business banking entity the columns in the Assigned Branches pane show information for the selected combination:

* The Transaction Branches column lists all the branches whose transactions you can work on (your transaction scope)
* The Enquiry Branches column lists all the branches whose transactions you can view but not work on (your enquiry scope)

The Available Products Events and Steps pane includes a drop-down list of the user roles available to you for the selected combination. When you select a user role, the Available Product Events and Steps pane shows information on the products and events that user role allows you to work with, and at what step. The Common Functions pane lists the master-level tasks the user role allows you to perform.

This functionality is available to all users. As security officer, it allow you in addition to view this information for all Trade Innovation users.

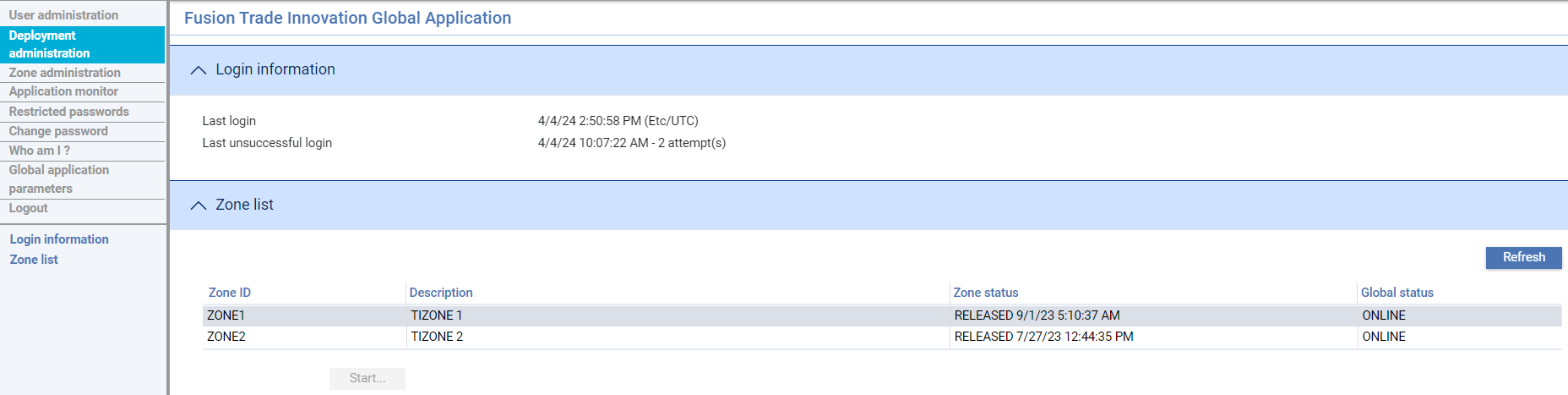
Select the user for whom you want to see information using the User Name field, then use the drop-down list fields described above to see information for them.

## Re-enabling a User Profile as a Help Desk User

As security officer, you can re-enable a disabled user profile using the User administration link, then selecting the user profile and updating it so that the Account enabled flag is reset.

Help desk users can also re-enable disabled user profiles (but not profiles that have expired).

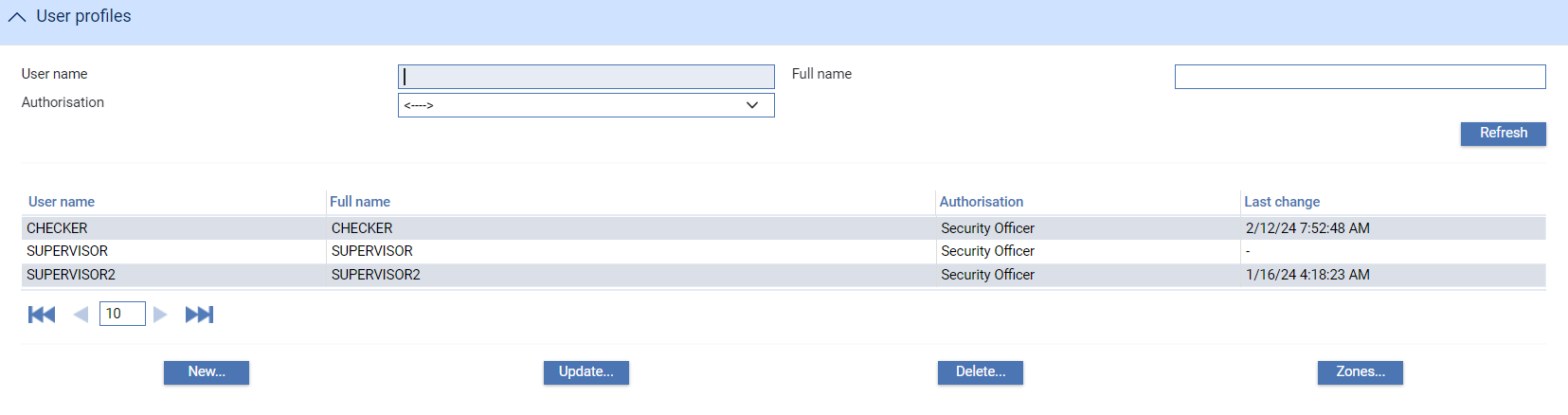
When you log on as a help desk user, the system logs you on at the global level.



The window displayed uses a sub-set of the functionality available to security officers.

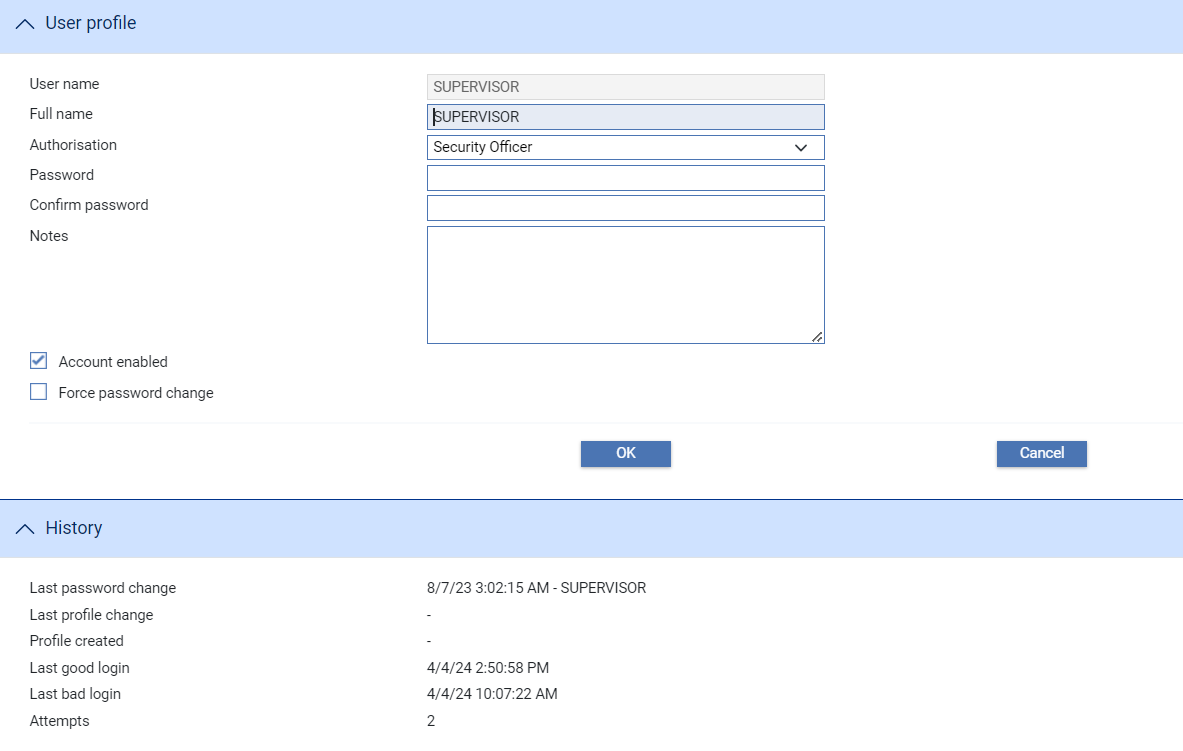
1. Helpdesk users can be assigned to zones – though you may restrict this if their role is solely to enable user profiles.

Select the User administration link. When the list of user profiles is shown, click **Refresh**.



The system displays a list of disabled user profiles.

Select the one you wish to re-enable and click **Update**.



Details of the user profile are displayed, but only the Account Enabled field is available for input (and only if the user profile was disabled for a reason other than that it reached its expiry date). Check this field and click **OK** to re-enable the account.

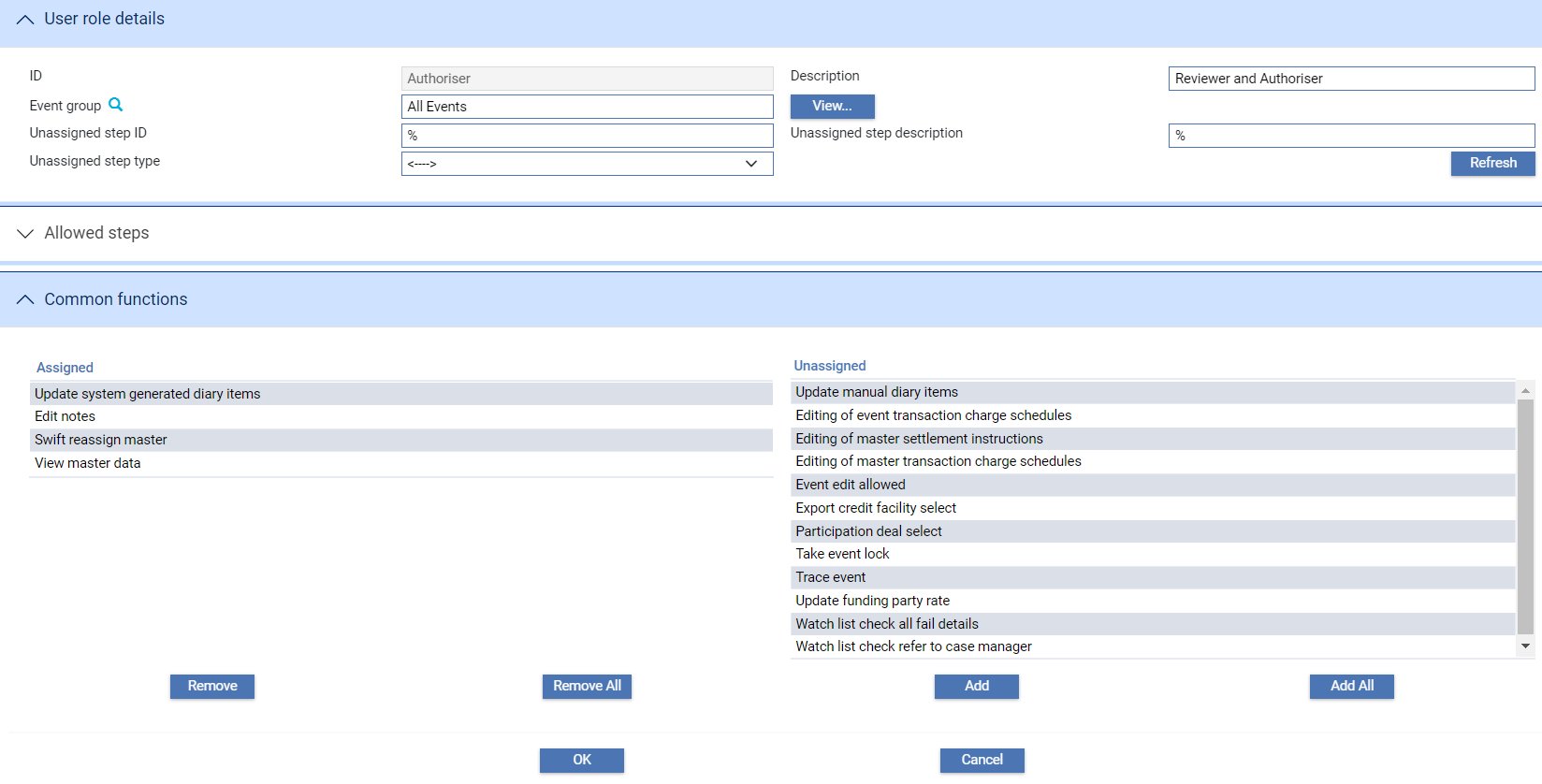
# Master-level Tasks and Capabilities

This chapter covers the security functions and capabilities available to map to users. These consist of the following:

* Master-level tasks that govern access to common functionality used during transaction processing
* Capabilities used to control access to functionality not related to transaction processing

## Master-level Tasks

Master level tasks are mapped as part of the user security configuration within user roles. Select **Security** | **User roles** and create or update the role required. Common functions can be assigned and unassigned.



Master level tasks available to a user are visible under the ‘What can I do?’ under the assigned common functions.

The following table lists all the master-level tasks that govern access to common functionality used during transaction processing and explains what each controls:

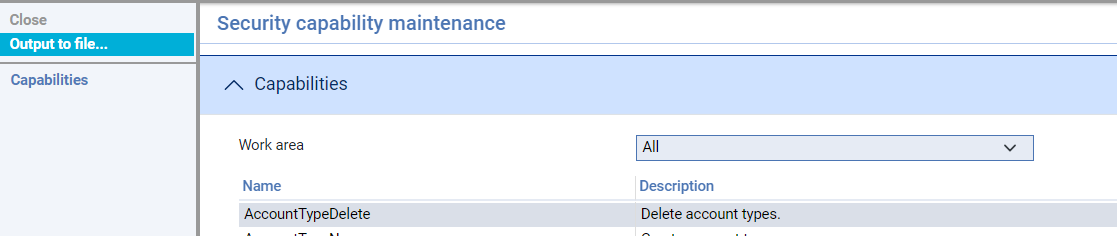
|  |  |
| --- | --- |
| Permission | Allows Users to |
| Editing of event transaction charge schedules | Set up event-level charge schedules. |
| Editing of master settlement instructions | Set up master-level settlement instructions. |
| Editing of master transaction charge schedules | Access and amend master-level charge schedules. |
| Edit notes | Change notes entered against an event. |
| Event edit allowed | Return an event that is at a step in its life-cycle later than data capture back to an Input step. |
| Export credit facility select | Select a credit facility to a financing transaction. |
| Participation deal select | Select a participation deal from within a participated transaction. |
| SWIFT reassign master | Reassign a message to another master, if the event it was originally used to create is aborted. |
| Take event lock | Open an event that has been opened by another user.  This functionality is provided for use in cases where an event has been opened by a user who has subsequently not been able to close the event in an orderly manner (as a result, for example, of a PC crash or network failure). It is intended to allow your bank to unlock such events. It is not intended for use in other circumstances. |
| Trace event | Create a tracer (including all user-created tracer events). |
| Update funding party rate | Amend the interest rate used to calculate the cost of funding for funding parties during Create, Amend, Adjust and Repay events. Note that the setting applied on the product type will override the capability setting here. |
| Update manual diary items | Amend or delete manually entered diary entries. |
| Update system generated diary items | Amend or delete automatically generated diary entries. |
| View master data | Use the More button on the Master Summary window. |
| Watch list check all fail details | See full details of a Watch List Check step where the transaction has failed checking. Without this capability users are able to see only that the transaction has failed. |
| Watch list check refer to case manager | Reserved for future use. |

## Capabilities

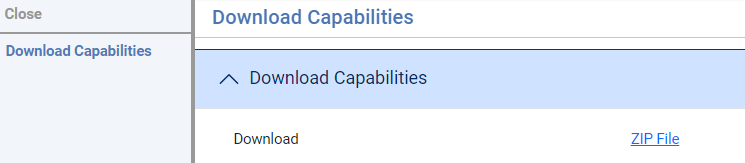
Capabilities are used to control access to functionality related to non-transaction processing. These capabilities are organised according to the application to which they relate.

You can download the list capabilities applicable to your software version from the Security application as follows:

1. Select Security | Capabilities option.
2. Select the option **Output to file…** on the left hand side menu.



1. When the output has been generated, select the **ZIP File** link. The select action allows you to Open or Save the zip file. The file contains the file **all capabilities.csv**.



1. You can then review the file in your local directory.

The resulting file **all capabilities.csv** is ordered into the following areas:

|  |  |
| --- | --- |
| Area | What the Capabilities Control |
| Applications | Controls access to the Trade Innovation applications available to the user on entry to the zone. |
| Common | Controls access to common transaction related functionality and to the use of the Dashboard. |
| Departmental Limits | Controls access to the Departmental Limits application functions. |
| Financing Transactions | Controls access to functions controlling group differential rate maintenance. |
| Gateway | Controls access to the Gateway application functions within the Message manager application. |
| Housekeeping | Controls access to all users’ print records. |
| Rate Fixing Application | Controls access to the Rate Fixing application functions. |
| Security Application | Controls access to the Security application capabilities. The first security officer created on your system has automatic access to the functionality of the security application. Additional security officers must be authorised to use the Security capability. |
| Static Data Maintenance | Controls access to the Static Data maintenance application functions.   1. If your bank uses static data replicated from a back office system then you should ensure that the relevant capabilities are not assigned to any user. |
| Supply Chain Finance | Controls access to the Supply Chain Finance application functions. |
| SWIFT | Controls access to the SWIFT application functions within the Message manager application. |
| System Tailoring | Controls capabilities relating to system tailoring, batch and batch setup applications. |