Ikasan Dashboard User Manual

Version 1.0.0

EMAIL: info@ikasan.org

WEBSITE: www.ikasan.org

***Table of Contents***

1 Introduction 4

1.1 About 4

1.2 Audience 4

1.3 How to Use This Guide 4

1.4 Overview 4

2 Accessing the Ikasan Dashboard 5

3 Platform Setup 8

4 Menu Navigation 10

5 General 11

5.1 User Profile 11

5.2 Dashboard 12

6 Services 13

6.1 Topology View 13

6.1.1 Topology Tree 16

6.1.2 Categorised Errors 16

6.1.3 Start up Control 17

6.1.4 Component Configuration 18

6.1.5 Wiretap Configuration 19

6.1.6 Adding a New Server 19

6.1.7 Business Stream Tab 20

6.1.8 Wiretap Tab 21

6.1.8.1 Wiretap Details Window 22

6.1.9 Errors Tab 23

6.1.9.1 Error Occurrence Details Window 24

6.1.10 Exclusions Tab 25

6.1.10.1 Exclusion Event Details Window 26

6.1.11 Actioned Exclusions Tab 27

6.1.11.1 Actioned Exclusion Event Details Window 28

6.1.12 Systems Events Tab 30

6.1.13 Categorised Errors Tab 31

6.1.13.1 Categorised Error Occurrence Details Window 32

6.2 Mapping View 35

6.2.1 Creating a New Mapping Configuration Client 35

6.2.2 Creating a New Mapping Configuration Type 36

6.2.3 Creating a New Mapping Configuraiton Context 36

6.2.4 Uploading a Mapping Configuration 37

6.2.5 Mapping Configuration Search 37

6.2.6 Managing a Mapping Configuration 38

6.2.6.1 Mapping Configuration Controls 38

6.3 Monitoring View 40

7 Administration 42

7.1 User Administration 42

7.2 Group Administration 43

7.3 Role Administration 44

7.4 Policy Administration 45

7.5 Managing User Directories 46

7.6 Platform Configuration 48

# Introduction

## About

This document provides a user guide for the Ikasan Dashboard. This is part of the documentation suite for the Ikasan Enterprise Integration Platform.

This console is independently deployed as a self-contained WAR to the runtime container. This guide assumes packaging and deployment to runtime has been completed and focuses purely on the operations of the console itself from initial first time usage through to administration and management.

## Audience

This guide is targeted at users wishing to track and view business events flowing over one or more Ikasan integration modules as well as Ikasan associated services.

## How to Use This Guide

This guide provides a reference that can be read front to back or dipped into as required for the operation of the Ikasan User Console.

## Overview

The Ikasan User Console provides a web front end for searching and tracking events passing through Ikasan Integration Modules.

This guide covers the user operations within this console including:

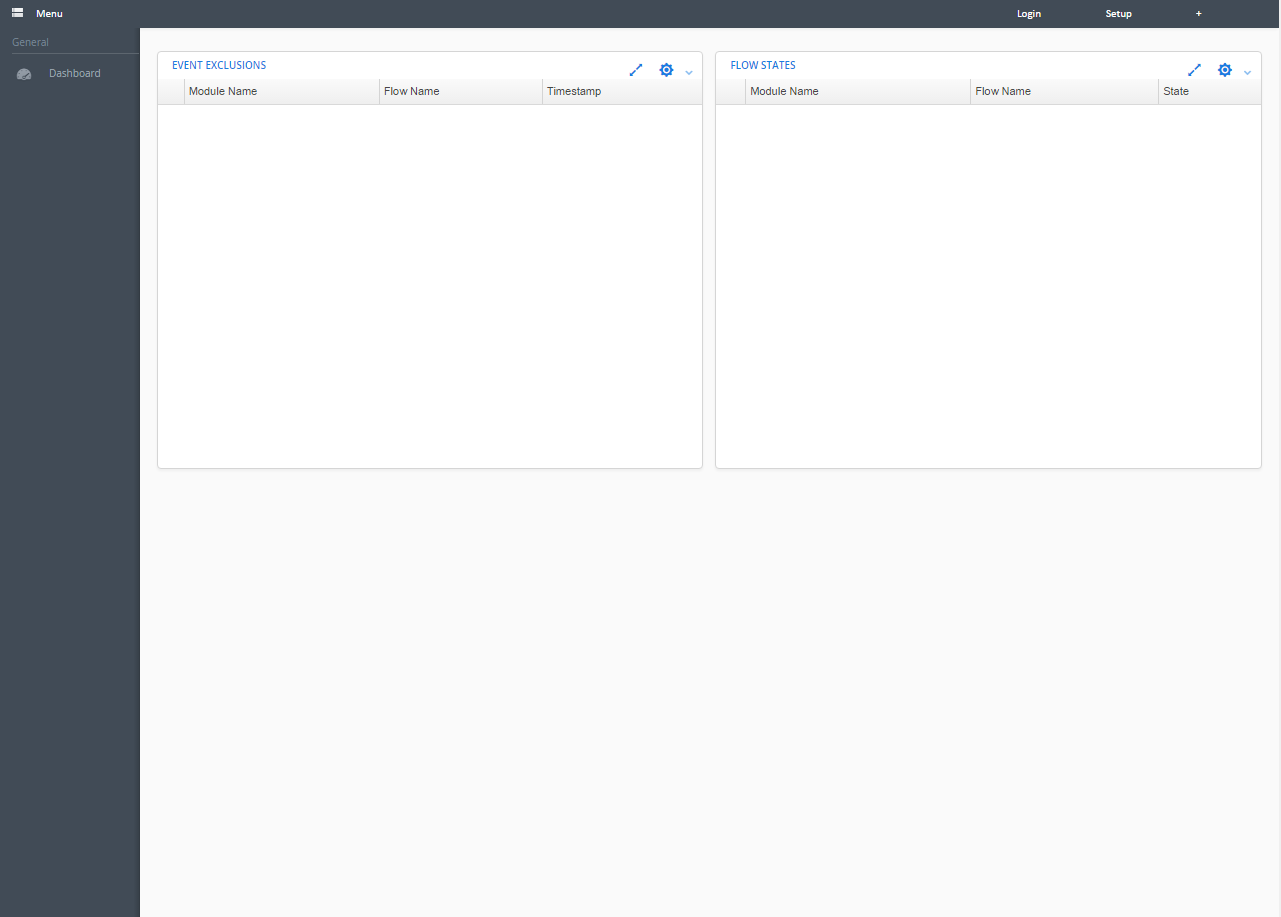
* Event Searching and Tracking
* User Administration and Management
* Ikasan Support and Resources
* Security and access management
* Data mapping
* Error and event exclusion lifecycle
* Business stream control
* Monitoring

# Accessing the Ikasan Dashboard

The Ikasan Dashboard is bound to the root context of “ikasan-dashboard” at runtime. In order to access the Ikasan User Console deployed to server “*foo*” (assuming default port 8080) you would open a web browser specifying the URL:

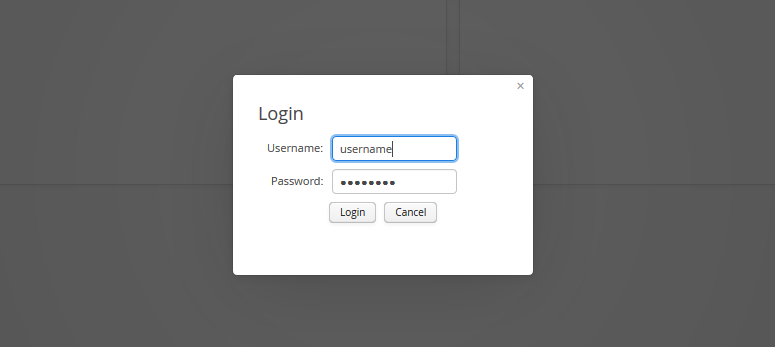
**http://foo:8080/ikasan-dashboard**

This would return the landing page below.

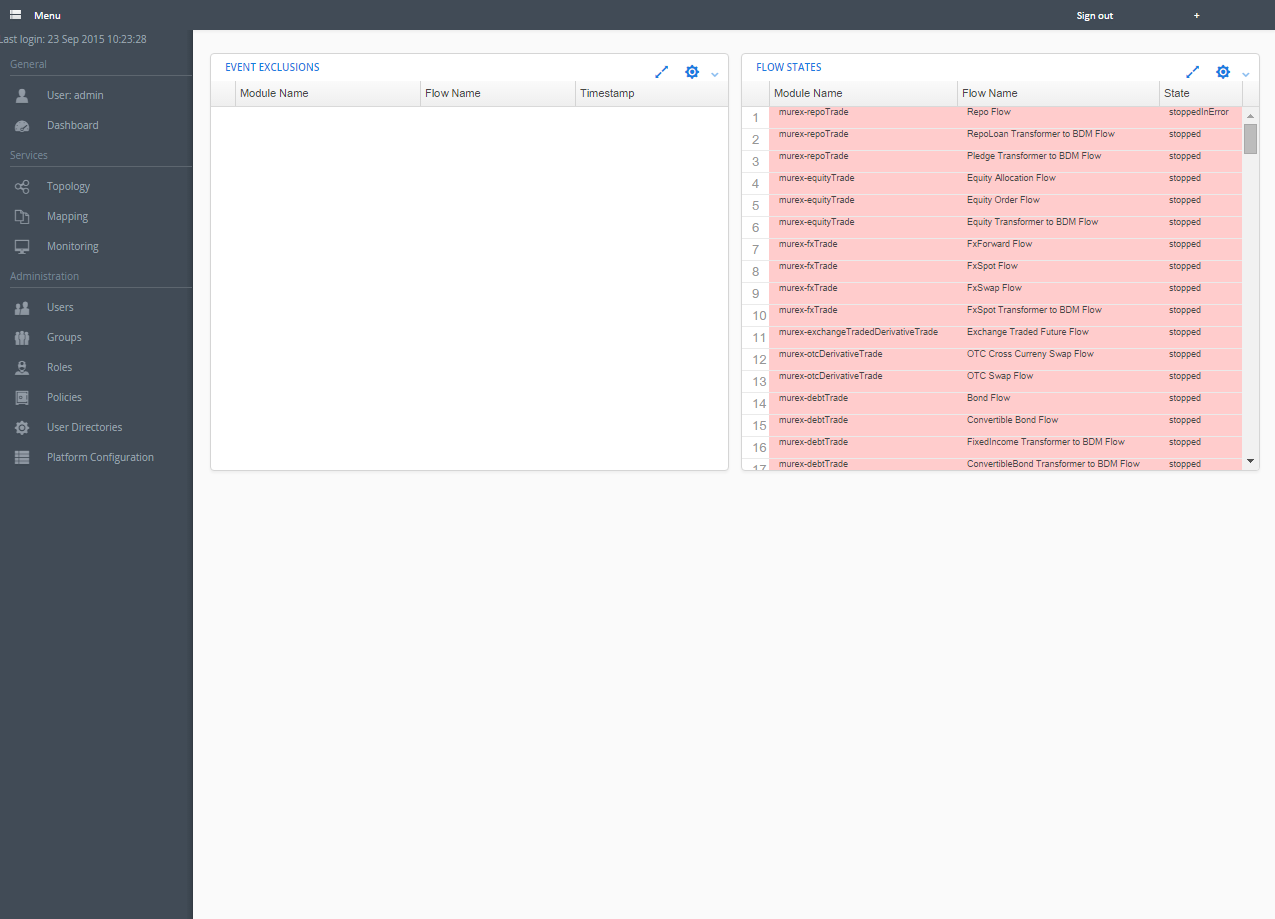


Once you have arrived at the dashboard landing screen you can log in by clicking on the ‘login’ link in the navigation bar at the top of the screen.

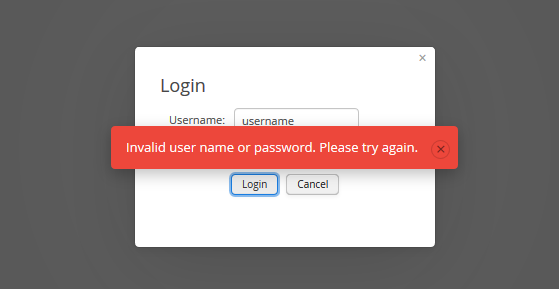
You will then be presented with the login dialog in which the Ikasan dashboard credentials are entered.



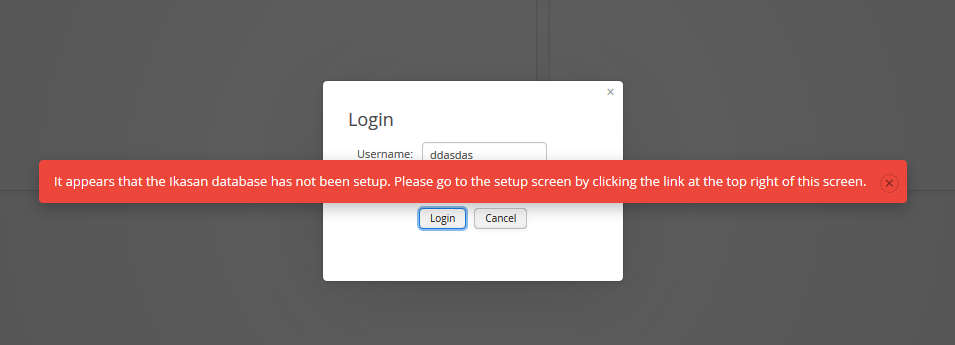
If your credentials are valid you will be presented with a screen similar to below with available functionality appearing in the menu bar on the left of the screen. If you have successfully logged in skip section 3 of this document.



If your credentials are invalid you will be presented with a screen similar to below and you will be required to enter your credentials again.



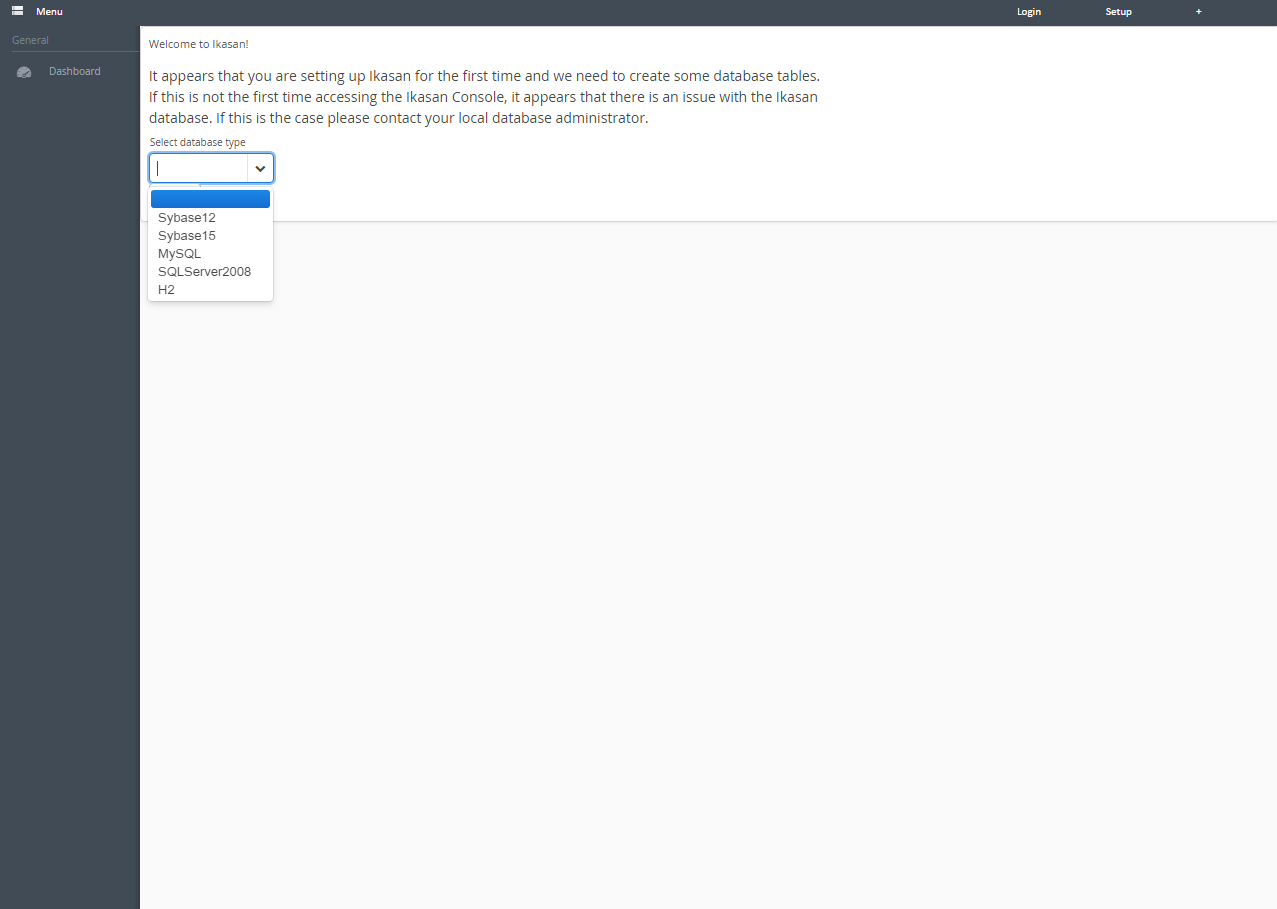
However it is also possible that this is the first time that the dashboard is being accessed in which case you will be required to follow the setup steps outlined in section 3 of this document. If you receive the message below then proceed with the Ikasan setup outlined in section 3.



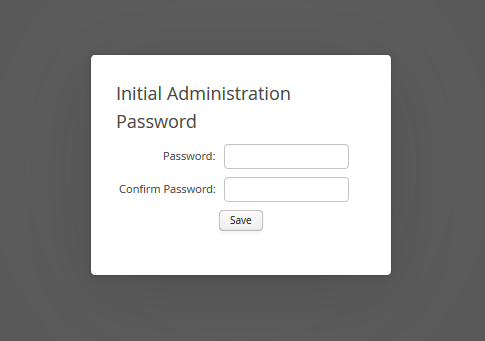
# Platform Setup

If you are setting up Ikasan for the first time, you will be required to go through the platform setup step prior to accessing the dashboard. This screen is accessed by clicking on the setup link on the right hand side of the ‘Navigation Bar’ at the top of the screen.

Upon arriving on the ‘Platform Setup’ screen select the appropriate database that is being used as the Ikasan database and press the create button.



You will then be presented with a dialog in which you must enter the ‘admin’ user password that will be used during the initial setup.



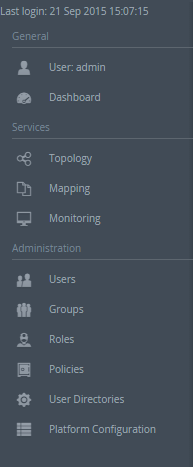
Once you have entered the user password press the save button. This action will then perform the task of creating the required database tables and populating the database with the data required for the dashboard to become operational. Once this is complete you will successfully be able to log into the application as described above. The credentials for the initial login are username ‘admin’ along with the password entered for the administration user in the setup step.

The next logical step in setting up the application in an enterprise context is to setup a user directory (LDAP) and synchronise this application with this directory. The [Managing User Directories](#_Managing_User_Directories) section of this document outlines the steps required to do this in more detail.

# Menu Navigation

Once logged in a menu will appear on the left hand side of the screen. The menu options that are available to a user are dependent upon the role of the user within the application. The image below shows all menu options that are available within the application. The following sections of this document will describe each functional area in more detail. Each can be accessed by clicking on the appropriate link in the menu below.

The last login time for the currently logged in user is displayed at the top of the menu.

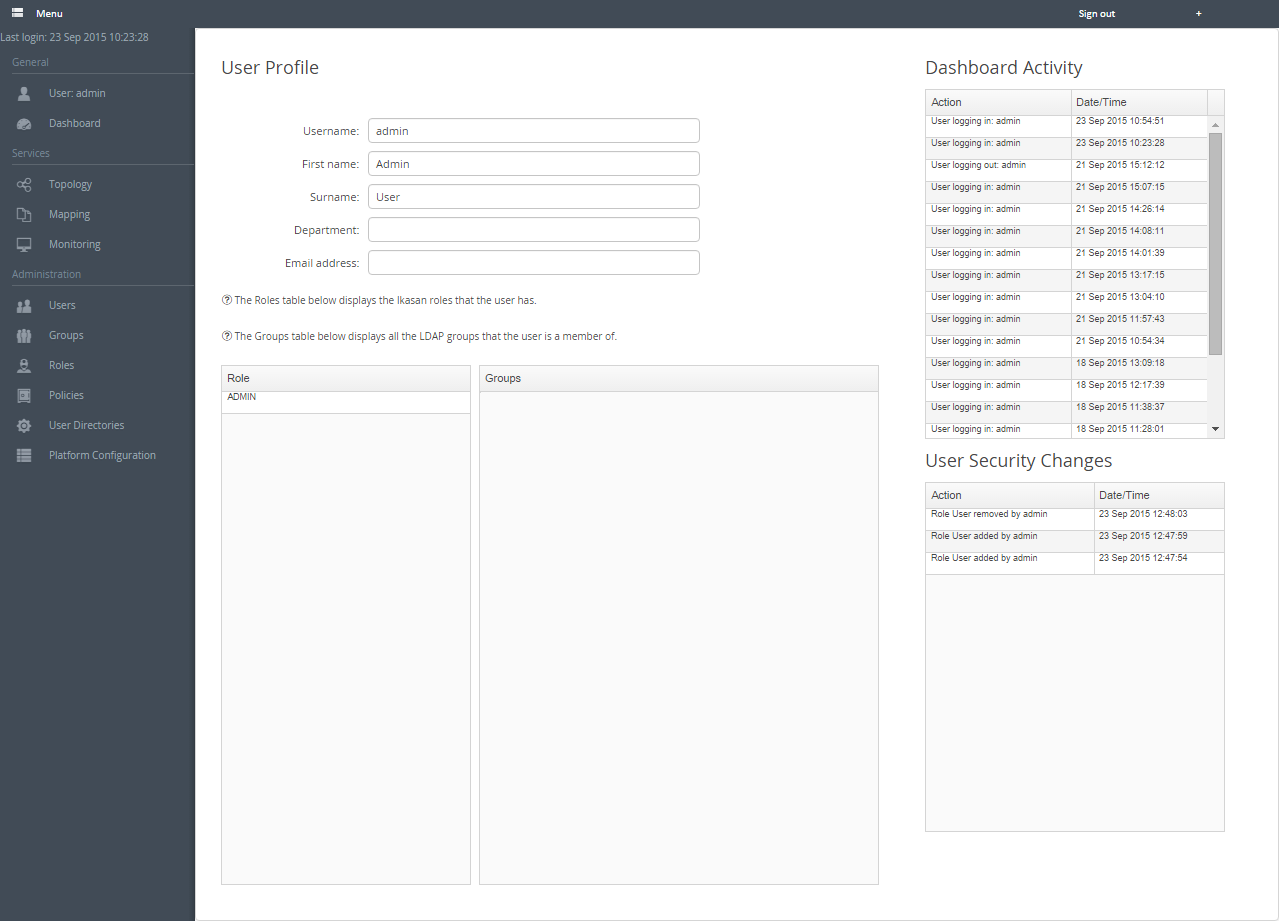


# General

## User Profile

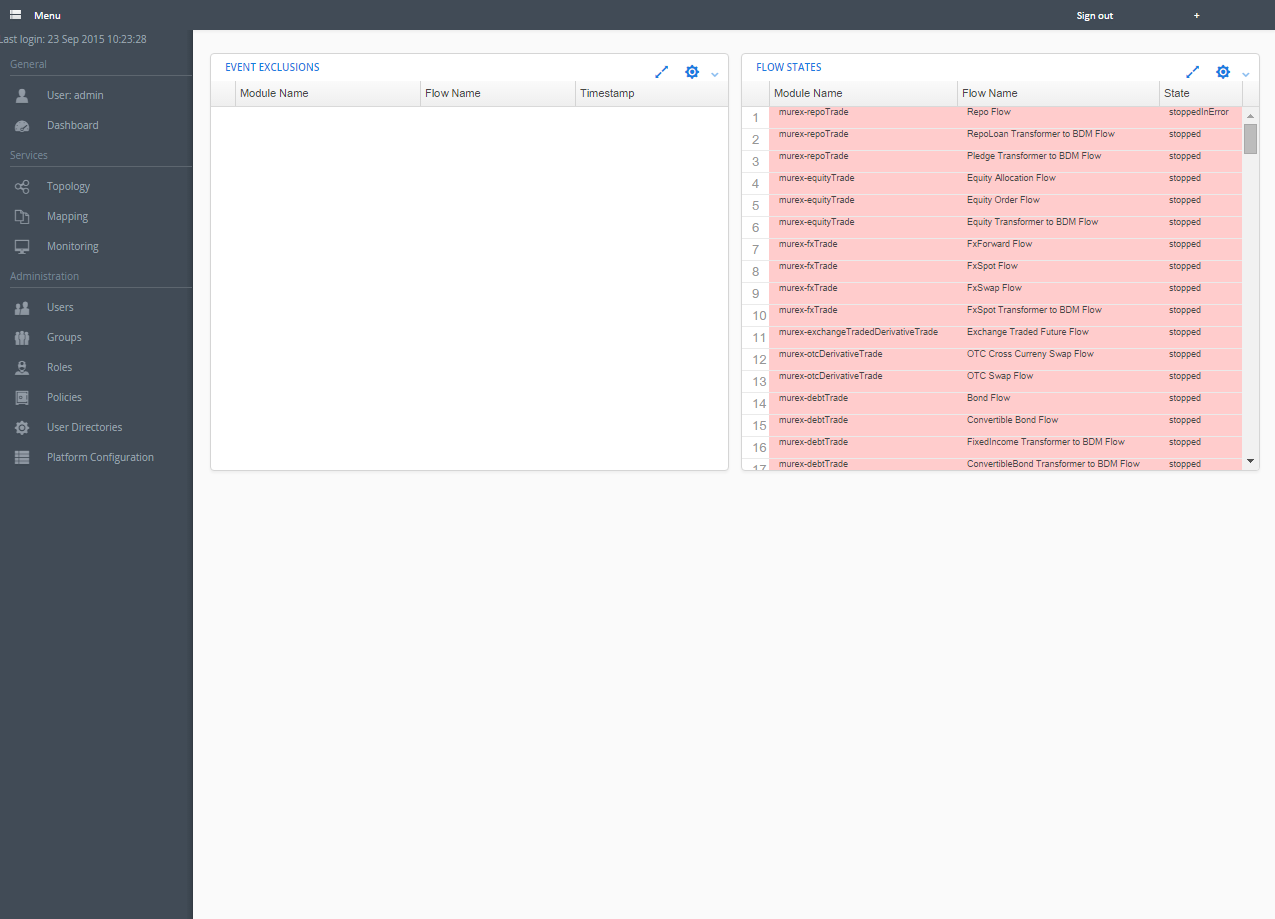
The User Profile screen is purely an informational screen providing details of the currently logged in user. It displays the following information:

* General user in formation such as name department and email address are shown in the form at the top left of the screen.
* The ‘Role’ table displays all roles that the current user has. The roles are managed within the context if the Ikasan dashboard.
* The ‘Groups’ table displays all the groups that this user is a member. These groups are sourced from the LDAP repository and are not managed from within the Ikasan dashboard.
* The ‘Dashboard Activity’ table displays information about the current user’s previous access times for the Ikasan dashboard.
* The ‘User Security Changes’ table provides an audit trail of all changes to this current users security permissions.



## Dashboard

The ‘Dashboard’ screen is a work in progress. The intention is that this screen will provide a relevant view based on the users profile.

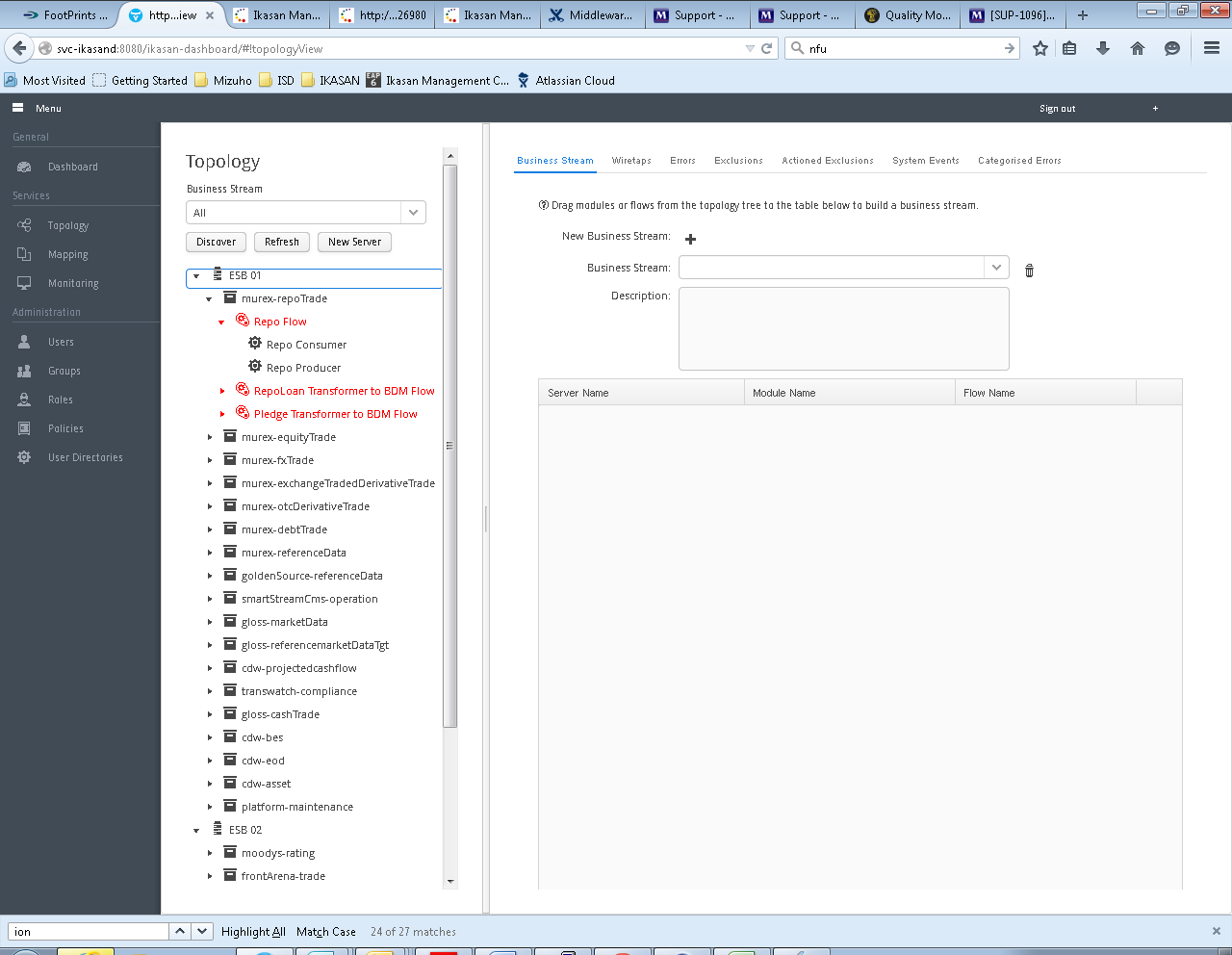


# Services

## Topology View

The ‘Topology View’ exposes a view onto the underlying integration elements that form the Enterprise Service Bus. These users ability to access individual tabs is driven by the roles that the user has. It provides the following functional areas:

* [**Topology Tree**.](#_Topology_Tree) The topology tree provides a hierarchical view on all the servers, integration module, flow, and component elements and provides functionality to allow for the control and administration of these elements.
* [**Business Stream Tab.**](#_Business_Stream_Tab)The business stream tab allows users to create new business streams and association relevant flows with a business stream.
* [**Wiretaps Tab.**](#_Wiretap_Tab)The wiretaps tab allows a user to search for data that has flowed through the ESB, which has been wiretapped at relevant points within a flow. The tab provides the ability to filter the results based on criteria defined by the user. Users can drill down on details on wiretapped events.
* [**Errors Tab.**](#_Errors_Tab)The errors tab exposes errors that have occurred within the ESB. These errors can be filtered based on criteria defined by the user. Users can drill down on details of the error.
* [**Exclusions Tab.**](#_Exclusions_Tab)The exclusions tab provides the user with access to events that have been excluded by the ESB. Exclusions typically occur when a business exception has occurred, for example due to missing reference data. Business exceptions are distinctly separate to technical exceptions which are normally transient. For technical exceptions, the ESB will attempt to self-recover and as such events do not need to be excluded because once the underlying issue is resolved, the data will flow as normal. Whereas business exceptions are excluded which allows for the root cause to be remediated, for example reference data fixed, and the data subsequently resubmitted into the ESB to flow to its intended destination. This tab allows the user to drill down into details of the excluded data, the error that caused it and provides functionality to allow them to action the exclusion.
* [**Actioned Exclusions Tab.**](#_Actioned_Exclusions_Tab) The actioned exclusion tab provides an audit view of exclusions that have been actioned.
* [**System Event Tab.**](#_Systems_Events_Tab) The system event tab provides a view on system level events that have occurred within the ESB. These events include flow startup control events, mapping changes, dashboard and module access, and user security permission changes to name a few.
* [**Categorised Errors Tab.**](#_Categorised_Errors_Tab)The categorised errors tab provides a view on all errors that have been deemed categorised errors. The user can drill down on details and action if applicable.



### Topology Tree

The topology tree provides a hierarchical view on all the servers, integration module, flow, and component elements and provides functionality to allow for the control and administration of these elements. The following functionality is available within the tree (dependant on the permissions you have within the application):

ESB wide functionality:

* [Add a new server.](#_Adding_a_New)
* Discover new modules.

At the server level:

* The ability to view details of the server. (Not currently implemented)
* [The ability to categorise an error.](#_Categorised_Errors)

At the module level:

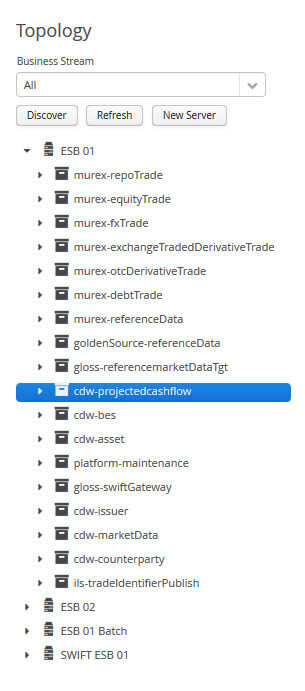
* The ability to view details of the module. (Not currently implemented)
* The ability to view the module diagram. (Not currently implemented)
* [The ability to categorise an error.](#_Categorised_Errors)

At the flow level:

* The ability to control the flow (Start, Stop, Pause, Resume).
* [The ability to configure the start-up type.](#_Start_up_Control)
* [The ability to categorise an error.](#_Categorised_Errors)

At the component level:

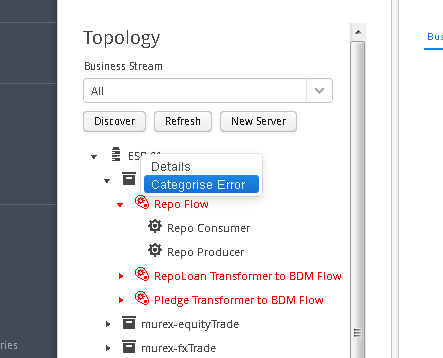
* [The ability to configure a component.](#_Component_Configuration)
* [The ability to add a wiretap to a component](#_Wiretap_Configuration).
* [The ability to categorise an error.](#_Categorised_Errors)



#### Categorised Errors

A categorised error is a decoration of an underlying ESB error occurrence. It allows the user to provide a criticality as well as a user friendly error message for errors of a certain type, which caused a certain action at a certain location within the ESB. These errors will then be displayed on the ‘[Categorised Errors Tab’](#_Categorised_Errors_Tab) where they can be filtered based on relevant criteria.

In order to create a categorised error, select the location within the ESB where you want to categorise an error by expanding the dashboard topology tree. Right click on the node in the tree and select ‘Categorised Error’ from the menu that appears as seen in the image below.



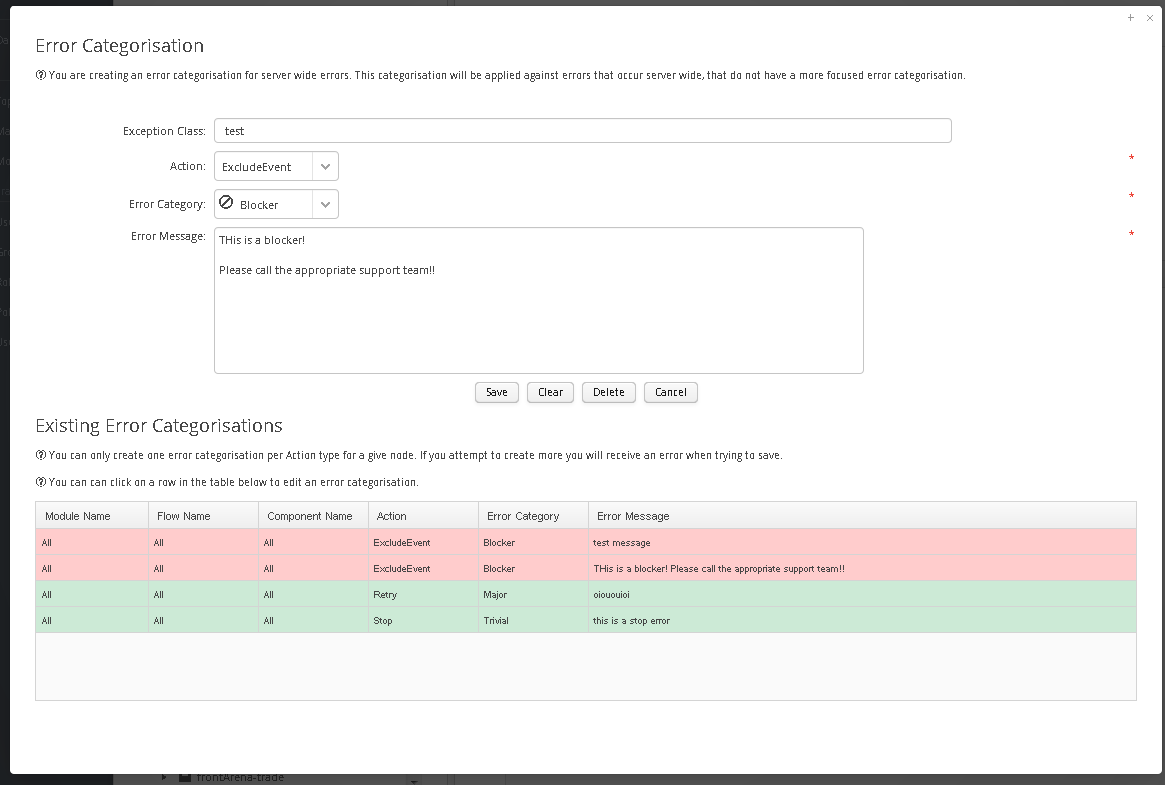
Once you have selected the ‘Categorise Error’ menu item, a window will appear. This window allows you to create, modify or delete categorised errors associated with the node. There are some basic rules for the creation of a ‘Categorised Error’.

1. For a given node (ESB Element) within the topology tree, the ‘Action’ / ‘Exception Class’ combination must be unique.
2. ‘Categorised Errors’ are applied to the underlying error occurrence in a cascading manner from the most relevant to the least relevant configured ‘Categorised Error’. For example, of you have a ‘Categorised Error’ configured at the component level that is a direct match for the ‘Exception Class / Action’ combination, then this is the ‘Categorised Error’ that will be displayed in the ‘Categorised Error’ tab when searched. However, if there is no direct match at the component level, but there are ‘Categorised Errors’ configured at the flow, module or server level that match on the ‘Exception Class / Action’ combination, then this will be cause this error to be included in the results on the Categorised Error tab.

The use of the ‘Error Categorisation’ window is straight forward. The form at the top allows the following to be added:

* **Exception Class** – free form text containing the fully qualified java exception class to match on.
* **Action** – the action taken by Ikasan when the exception occurs.
* **Error Category** – how this particular error should be categorised.
* **Error message** - the user friendly error message that will be displayed with the categorised error.

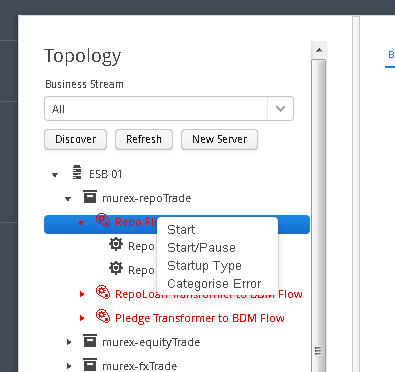
Once the ‘Categorised Error’ is saved it will appear in the table of ‘Categorised Errors’ at the bottom of the window. Any of these can be selected and modified or deleted from this table.



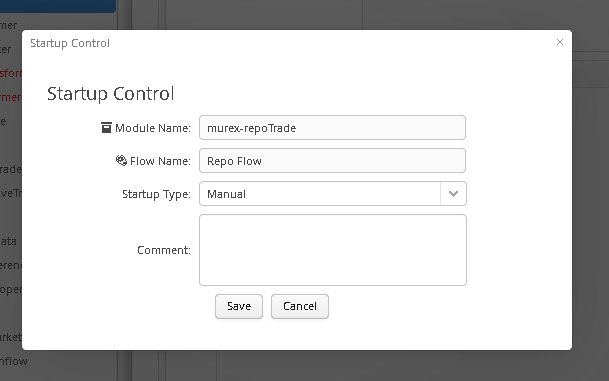
#### Start up Control

The start-up control functionality is available at the flow level within the ‘Topology Tree’. It can be accessed by right clicking on the relevant flow node in the topology tree that you want to set the start-up control for. There are 3 settings for start-up control:

1. Manual – when a server restarts, it relies on the user to manually restart the flow.
2. Automatic – when a server restarts, the flow will be automatically restarted.
3. Disabled – the flow is disabled and cannot be restarted.

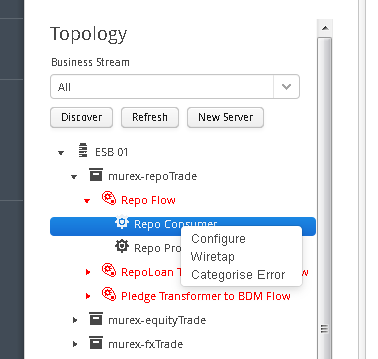


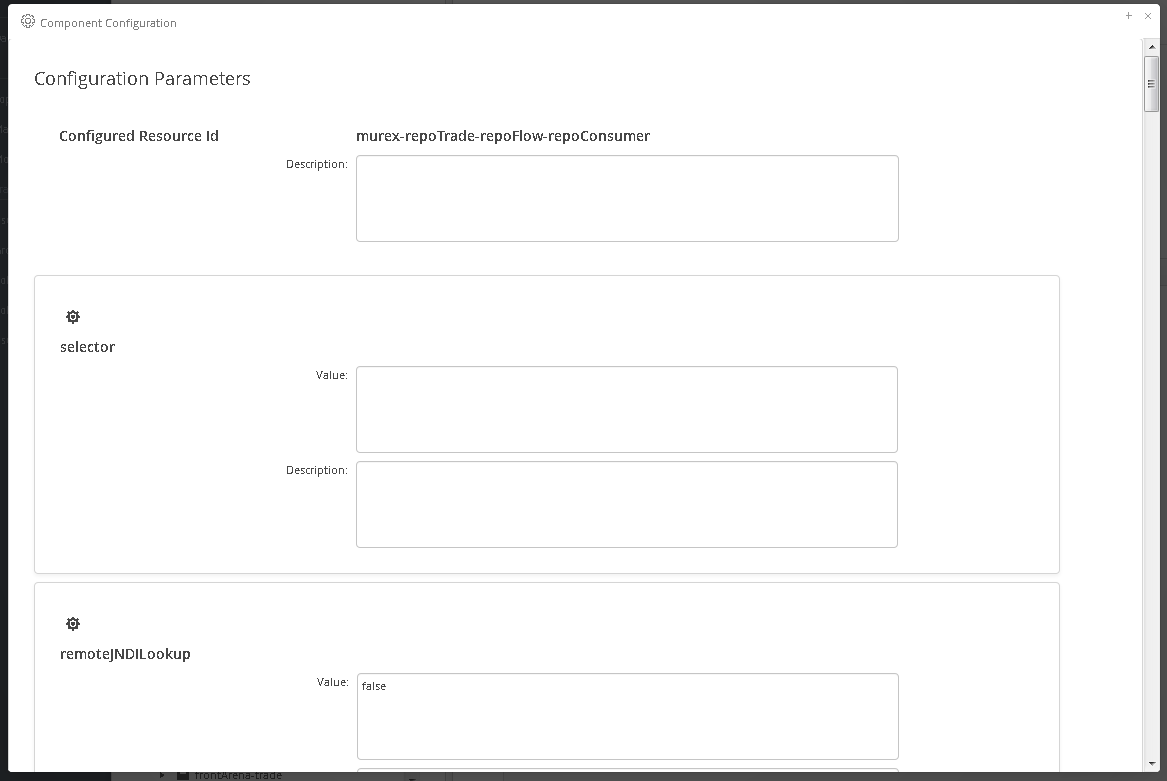
Once selected the ‘Startup Control’ window will be displayed. The user can then select the appropriate startup type. A comment is mandatory when setting the startup type to ‘Disabled’.



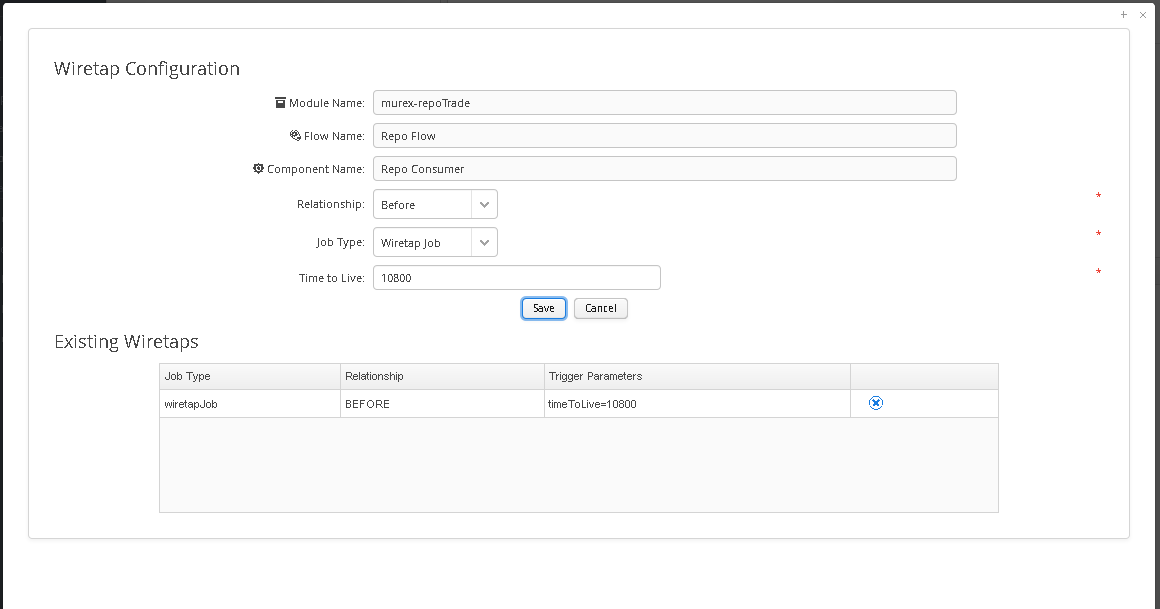
#### Component Configuration

The component configuration functionality is available at the flow level within the ‘Topology Tree’. It can be accessed by right clicking on the relevant component node in the topology tree that you want to create or modify the configuration for.

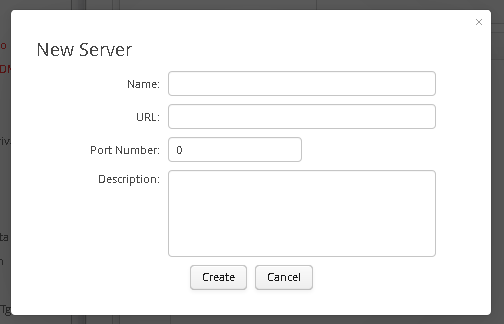




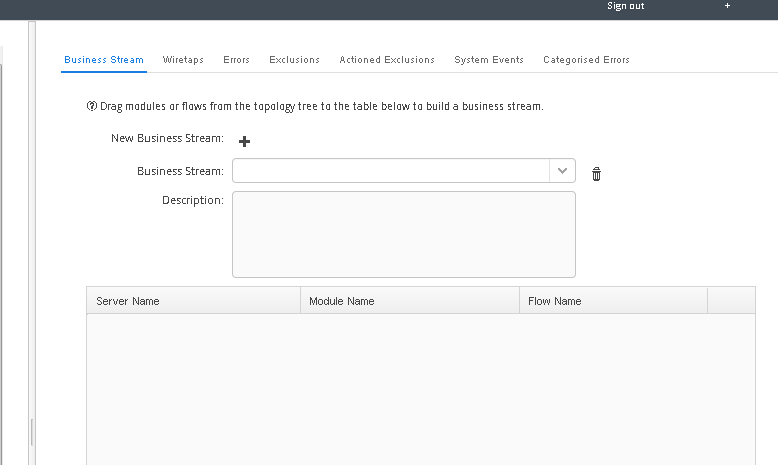
#### Wiretap Configuration

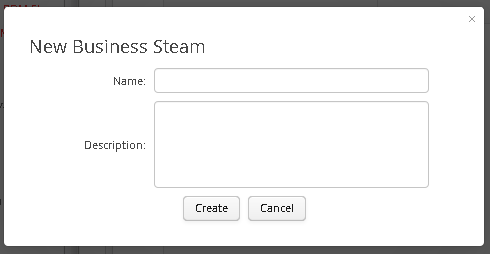


#### Adding a New Server

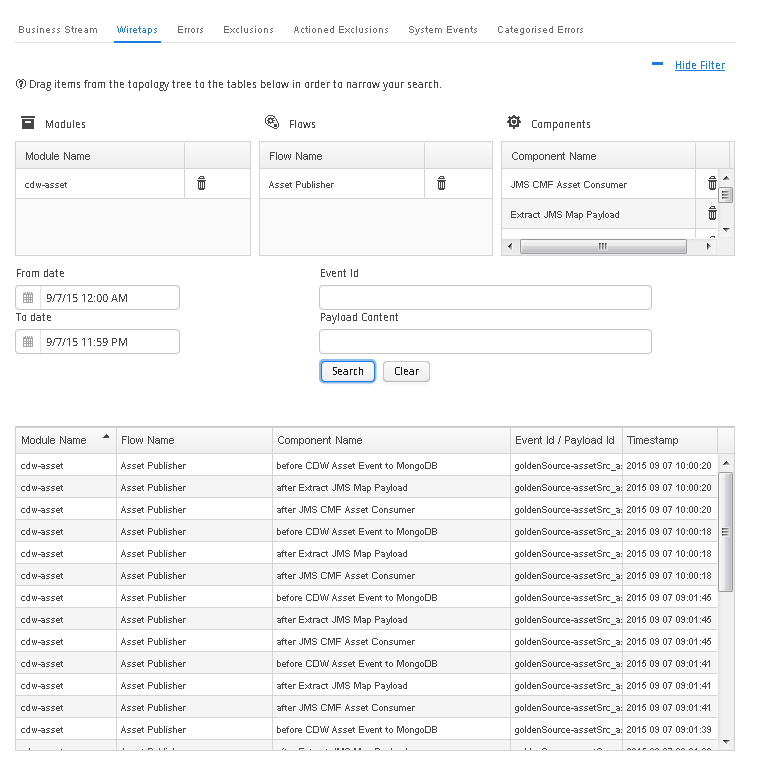


### Business Stream Tab

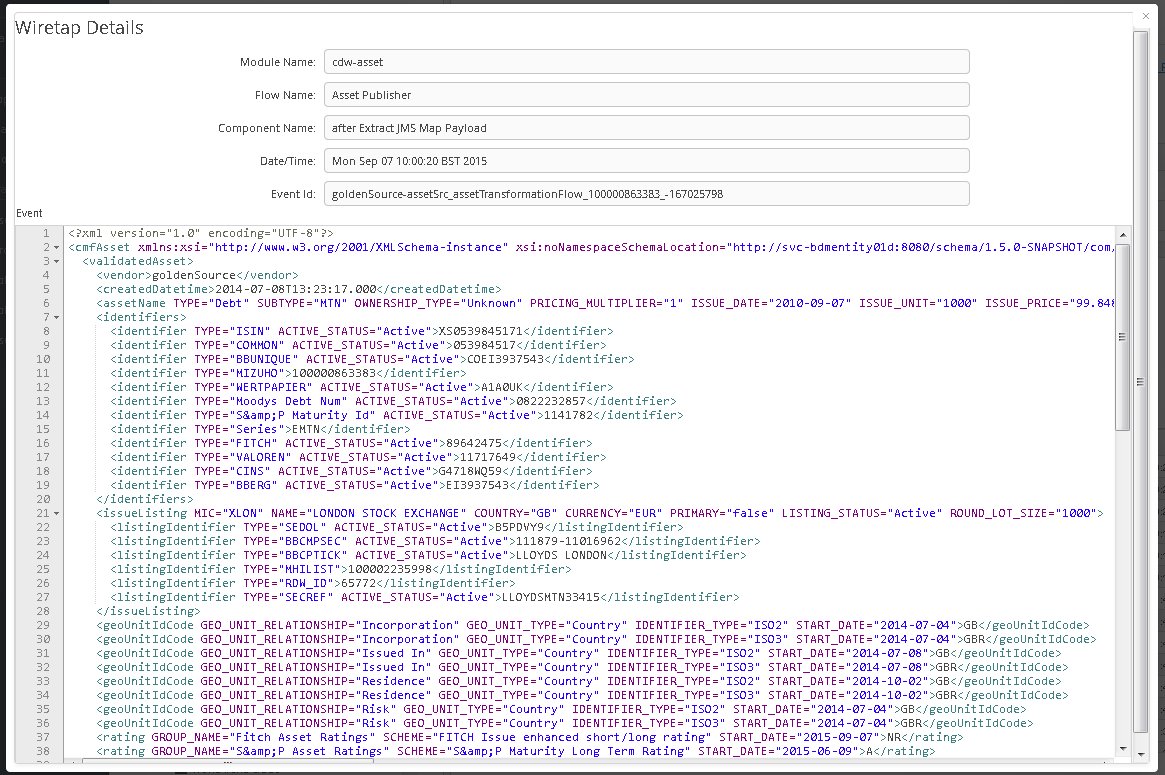




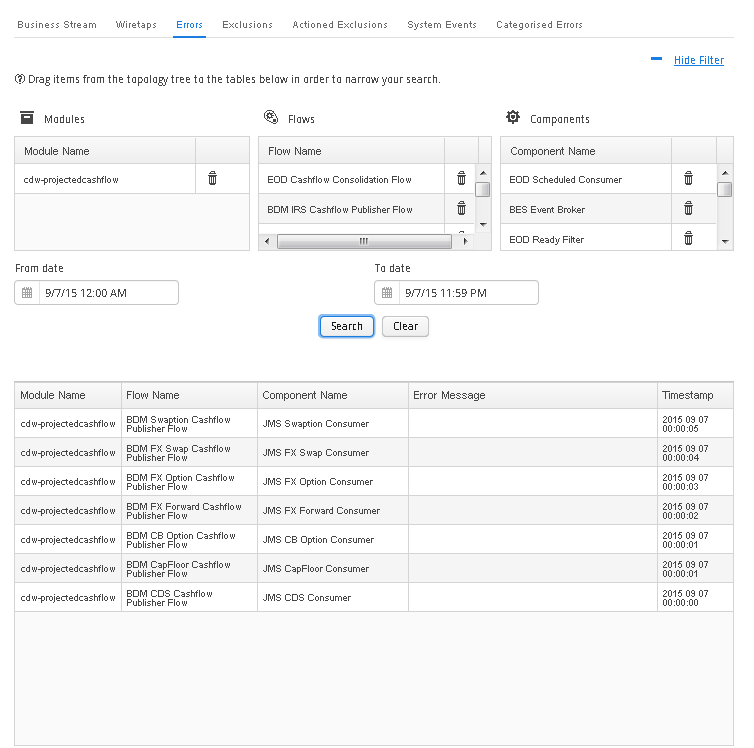
### Wiretap Tab



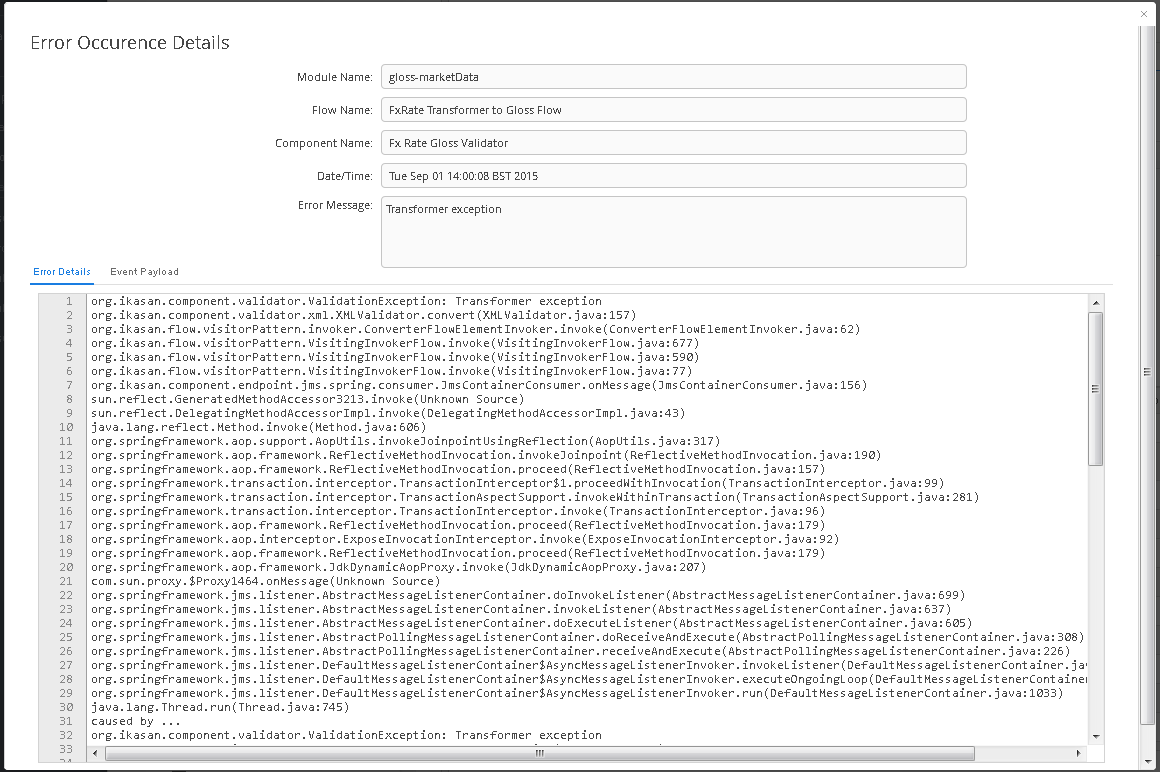
#### Wiretap Details Window

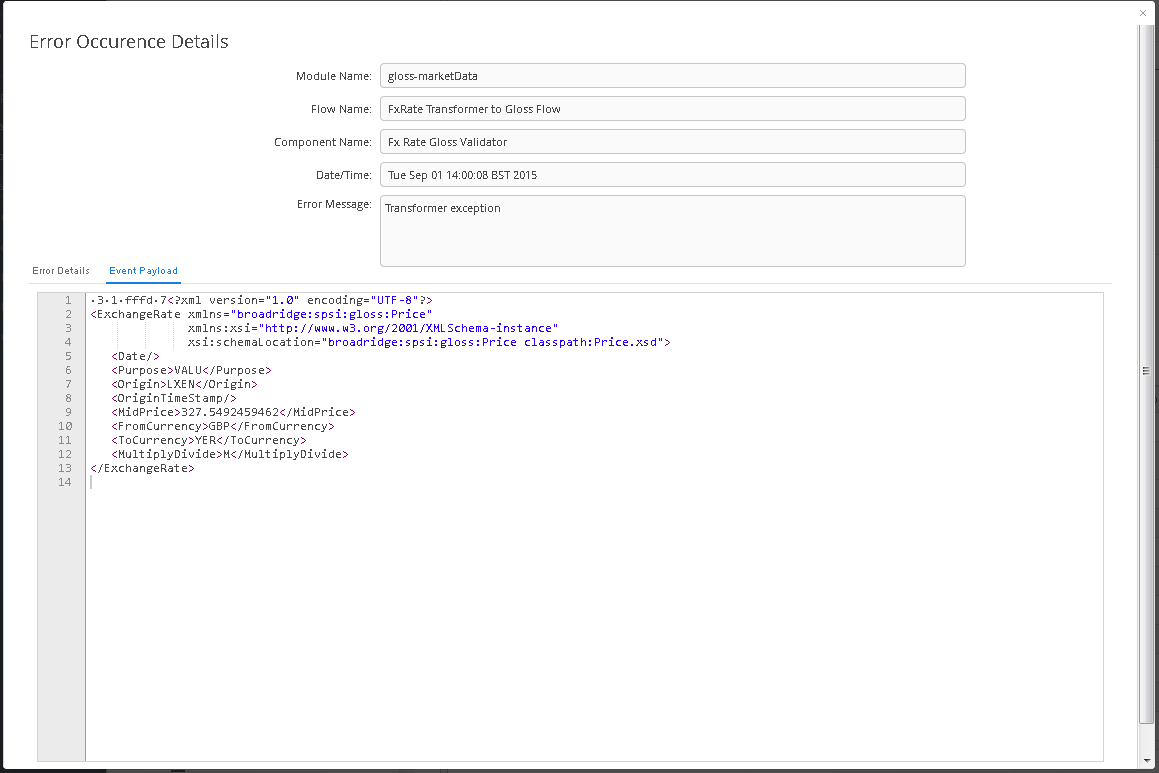


### Errors Tab

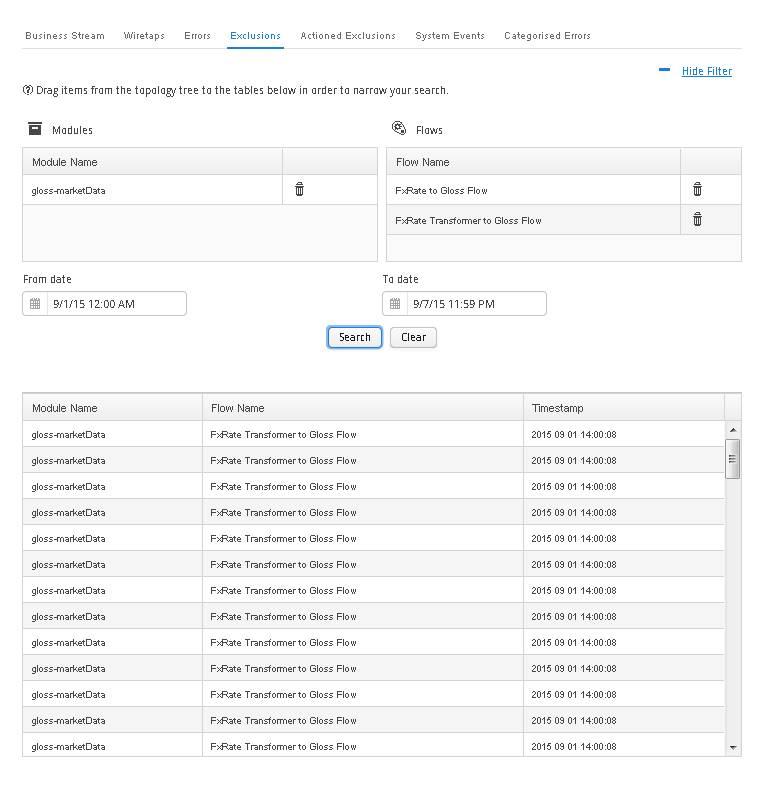


#### Error Occurrence Details Window

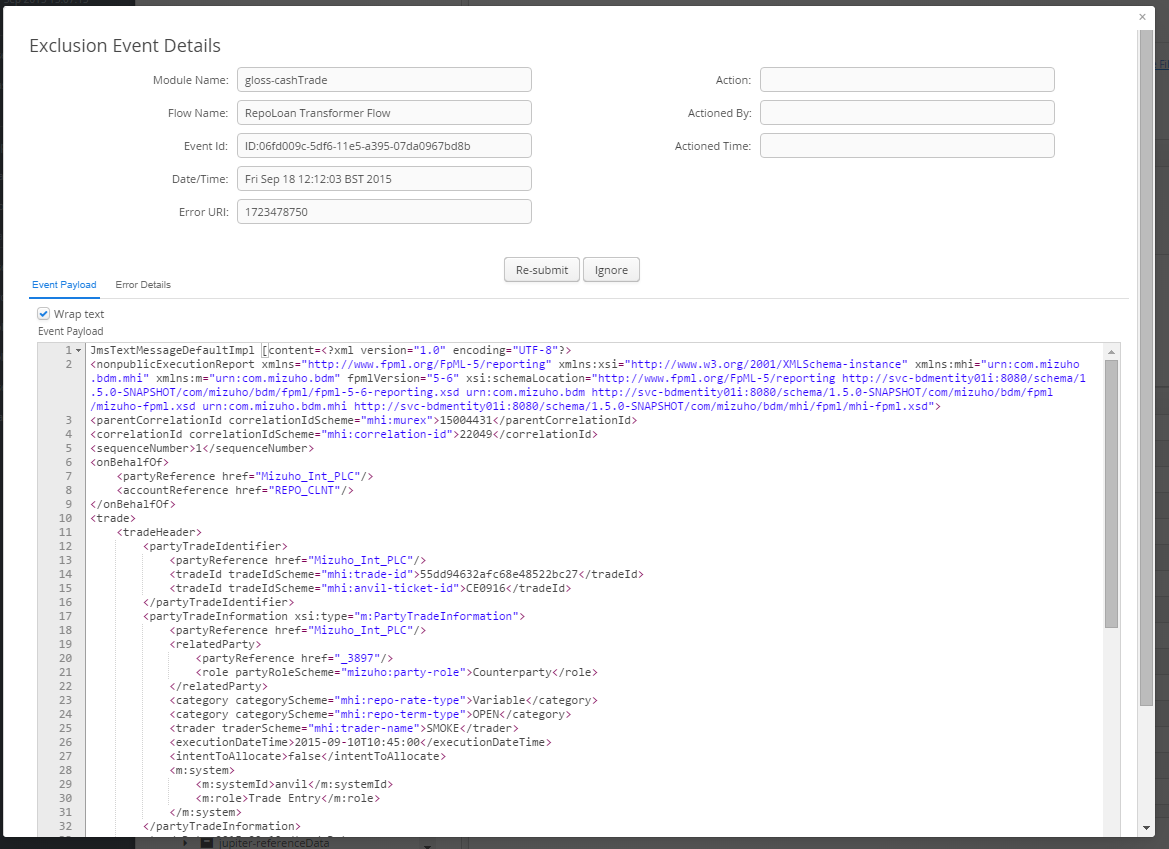




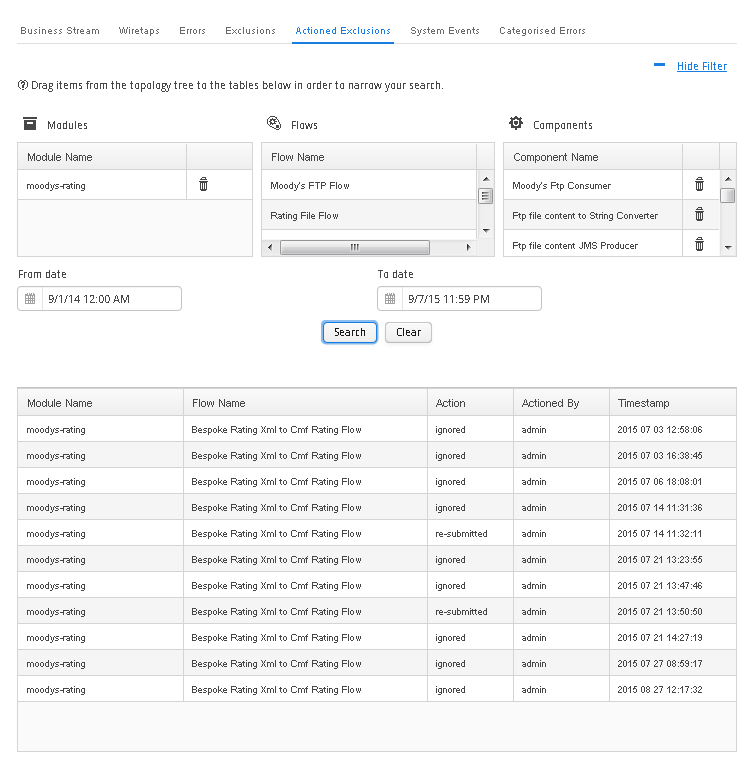
### Exclusions Tab



#### Exclusion Event Details Window

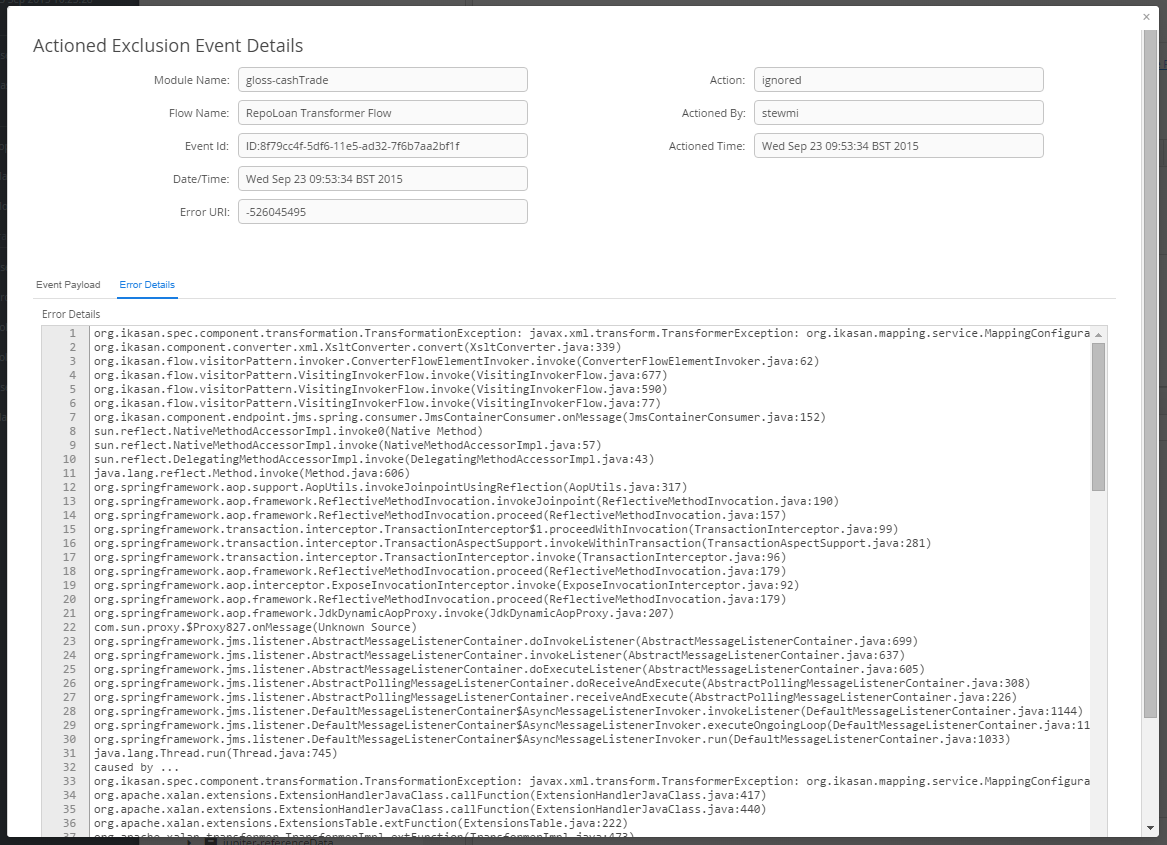


### Actioned Exclusions Tab

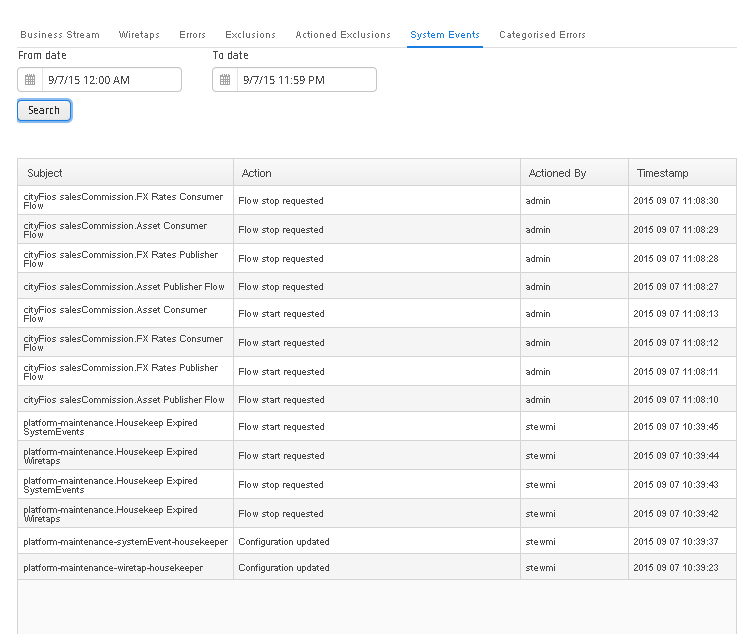


#### Actioned Exclusion Event Details Window

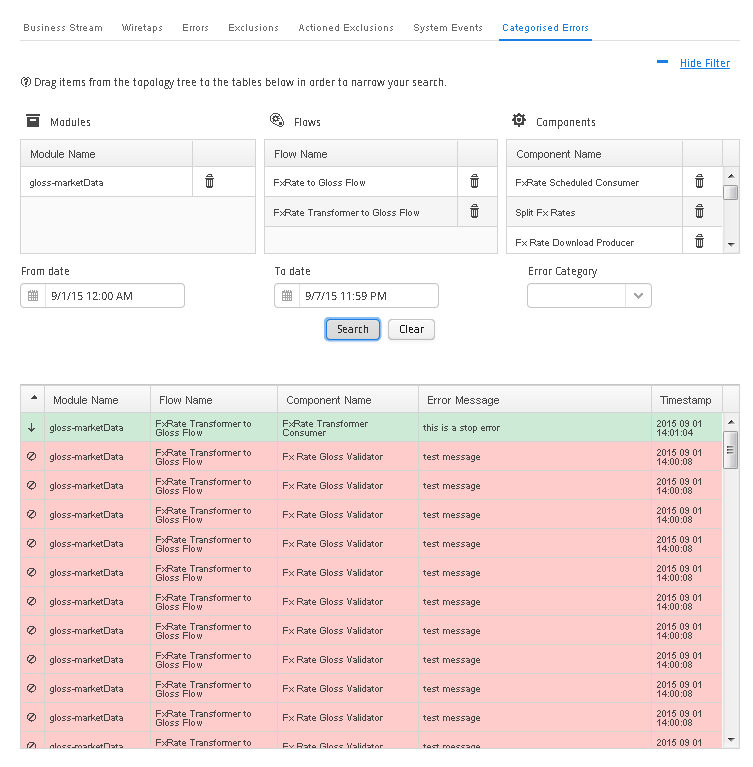




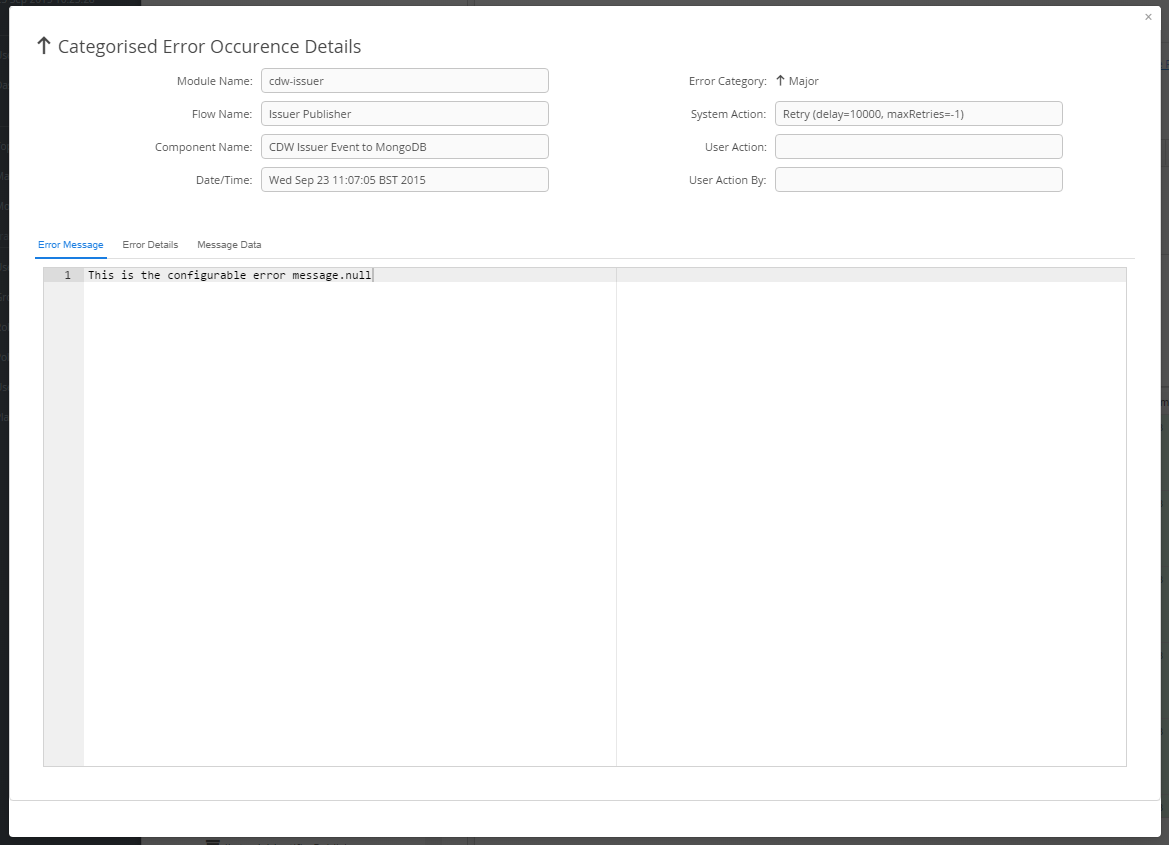
### Systems Events Tab

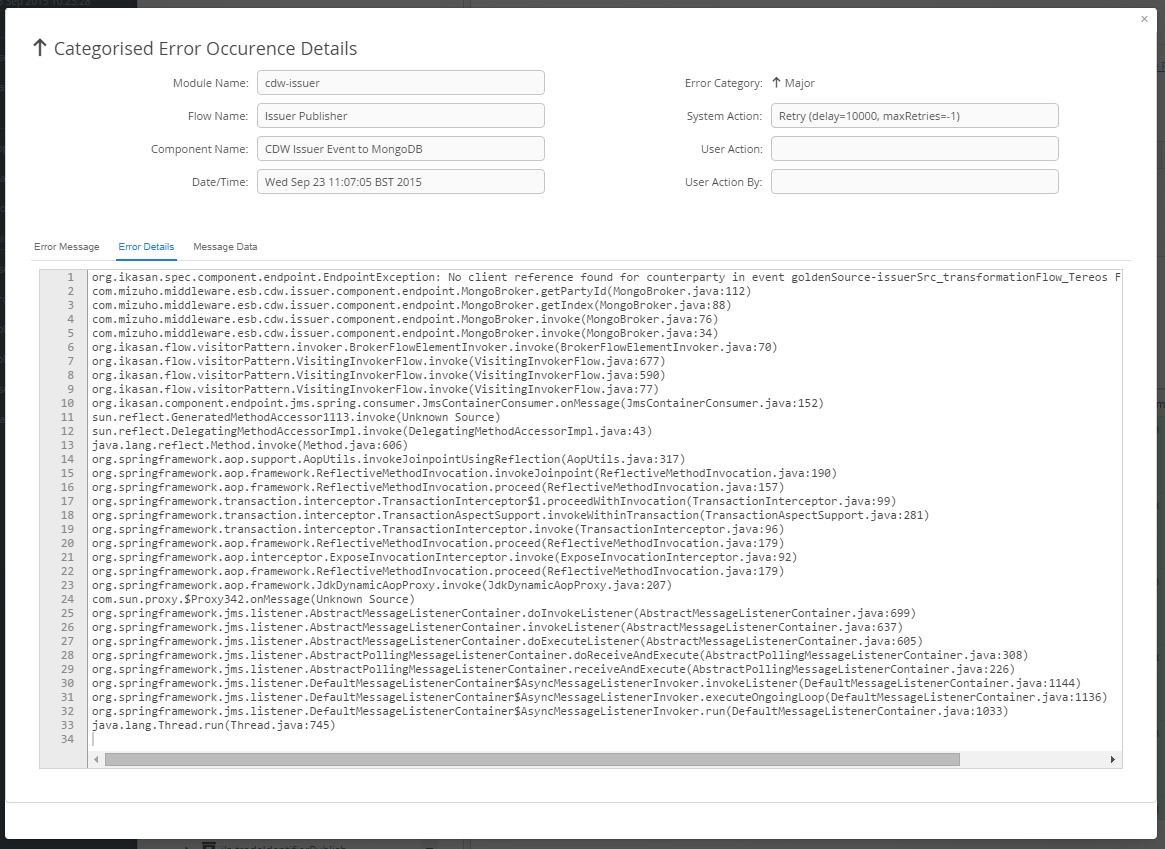


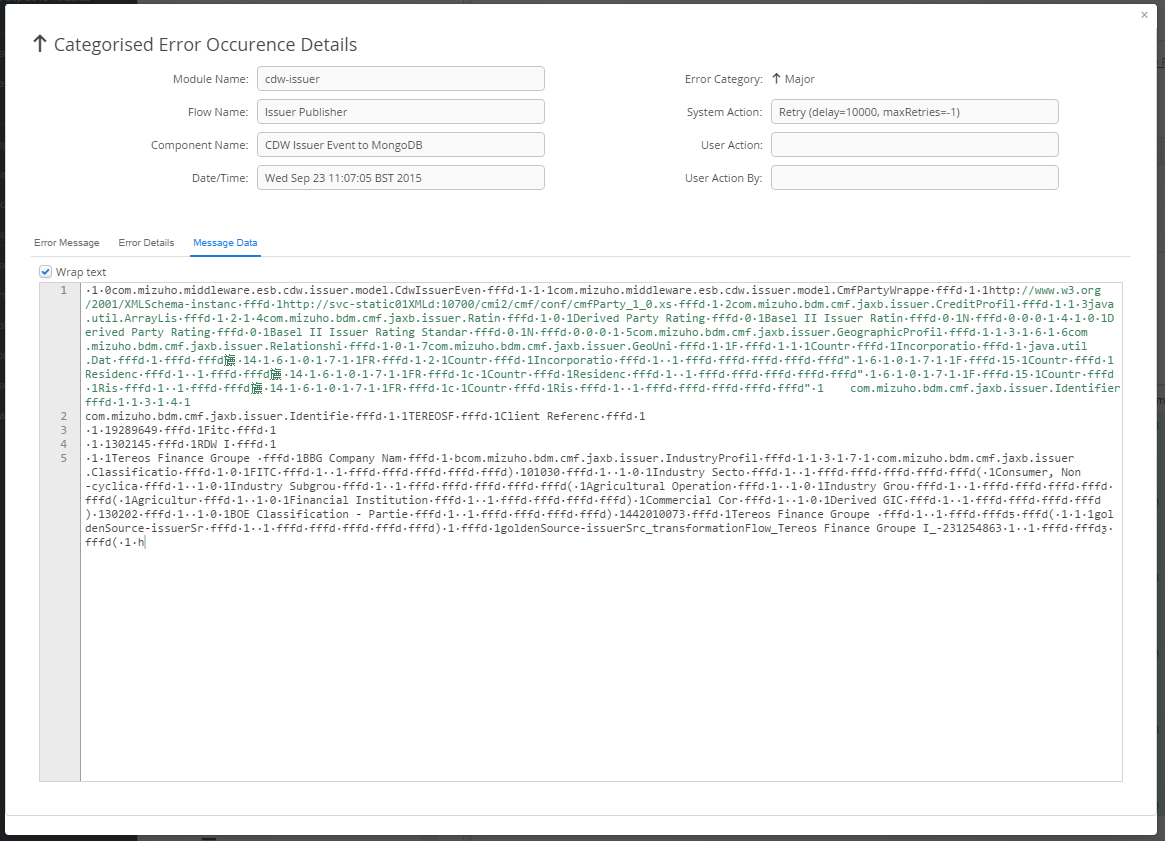
### Categorised Errors Tab



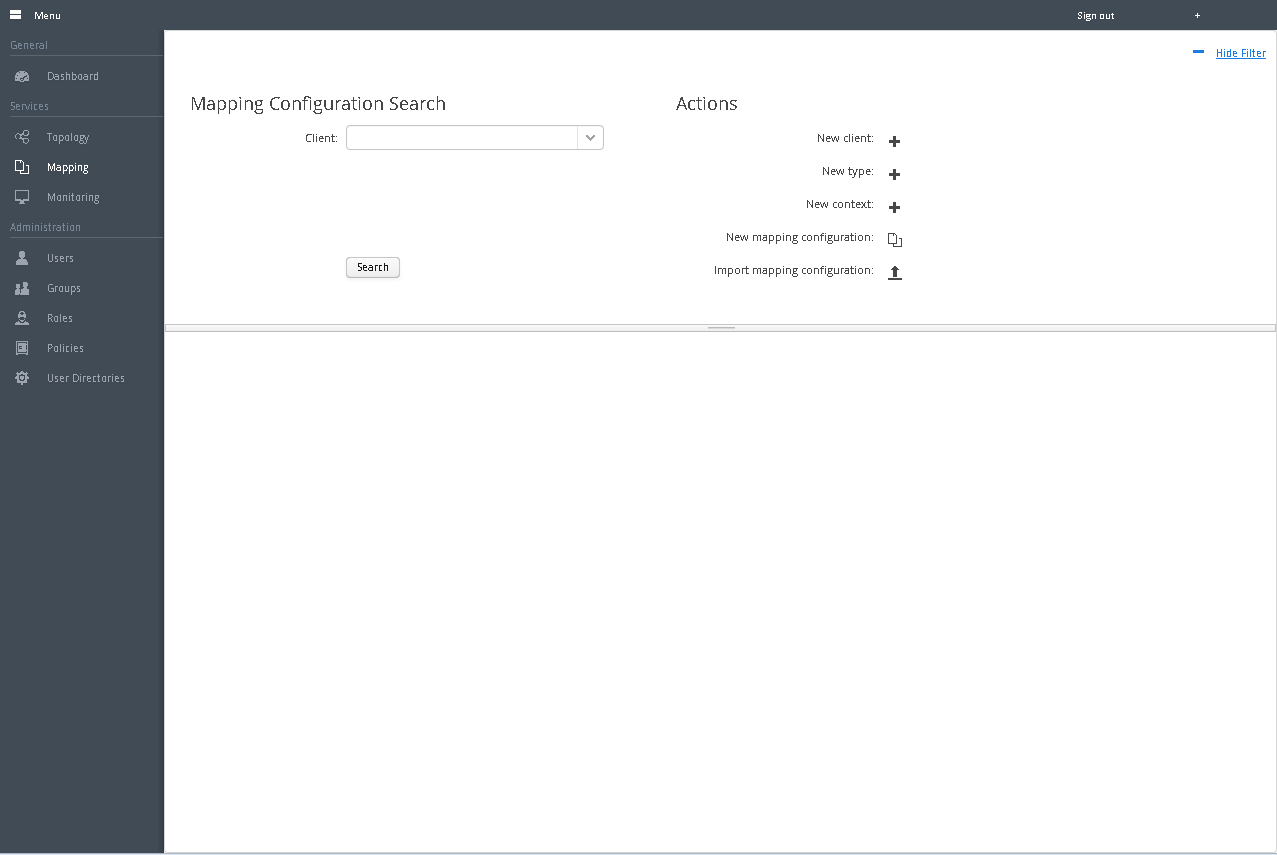
#### Categorised Error Occurrence Details Window



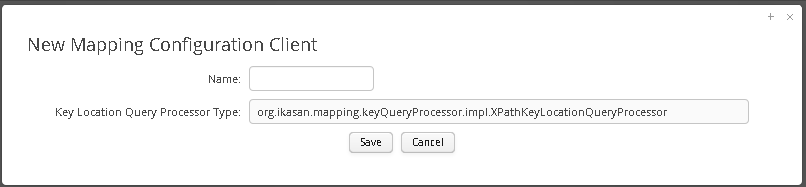




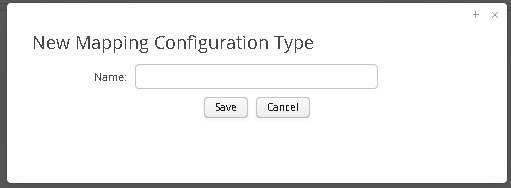
## Mapping View



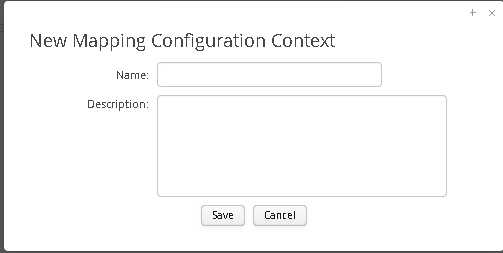
### Creating a New Mapping Configuration Client



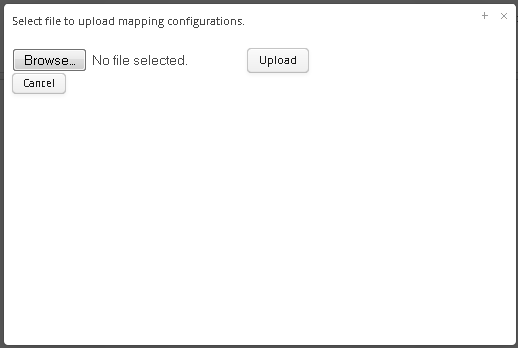
### Creating a New Mapping Configuration Type



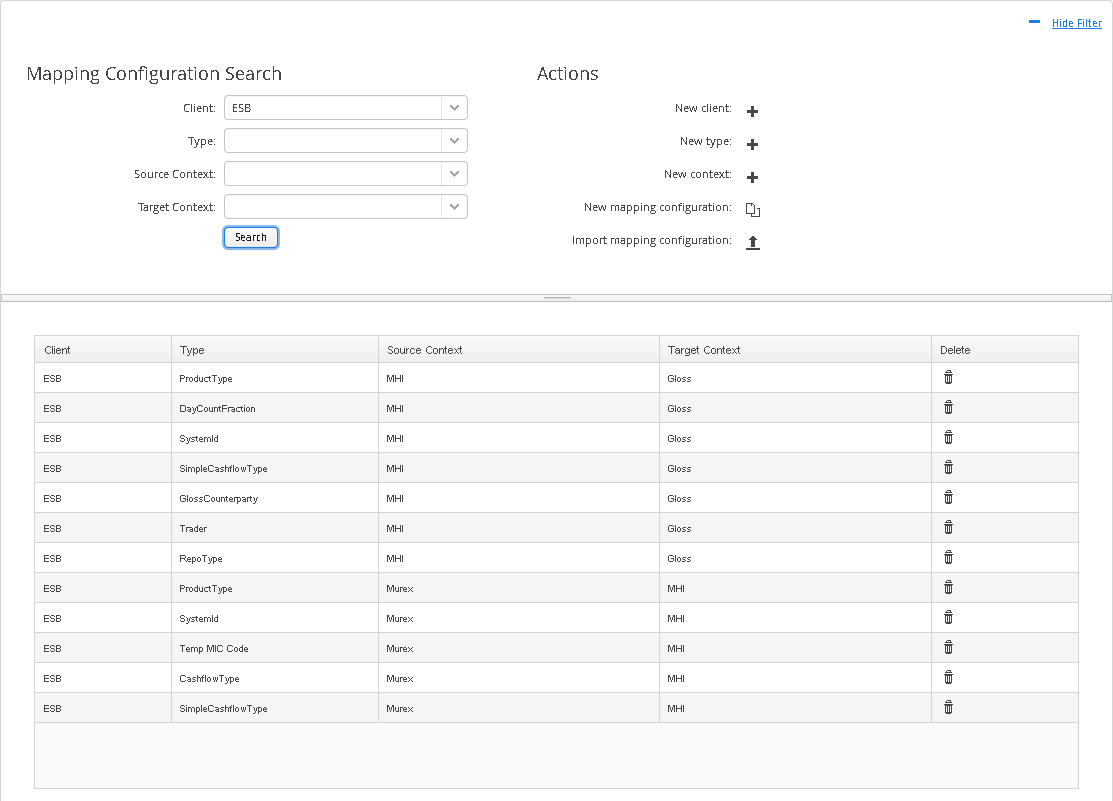
### Creating a New Mapping Configuraiton Context



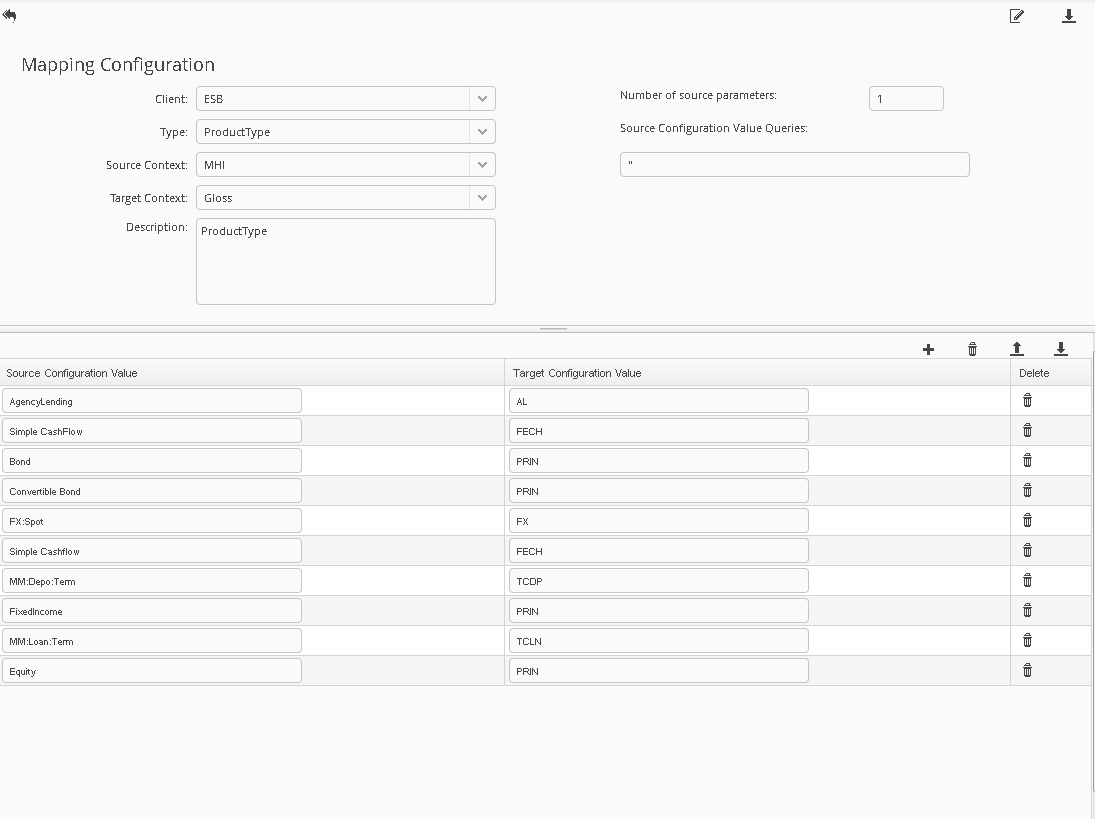
### Uploading a Mapping Configuration



### Mapping Configuration Search

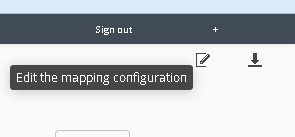


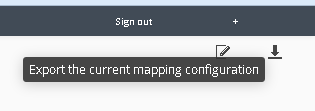
### Managing a Mapping Configuration



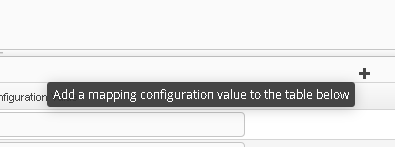
#### Mapping Configuration Controls

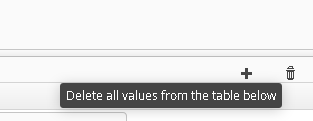


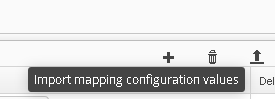


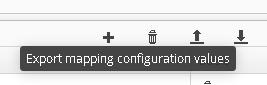




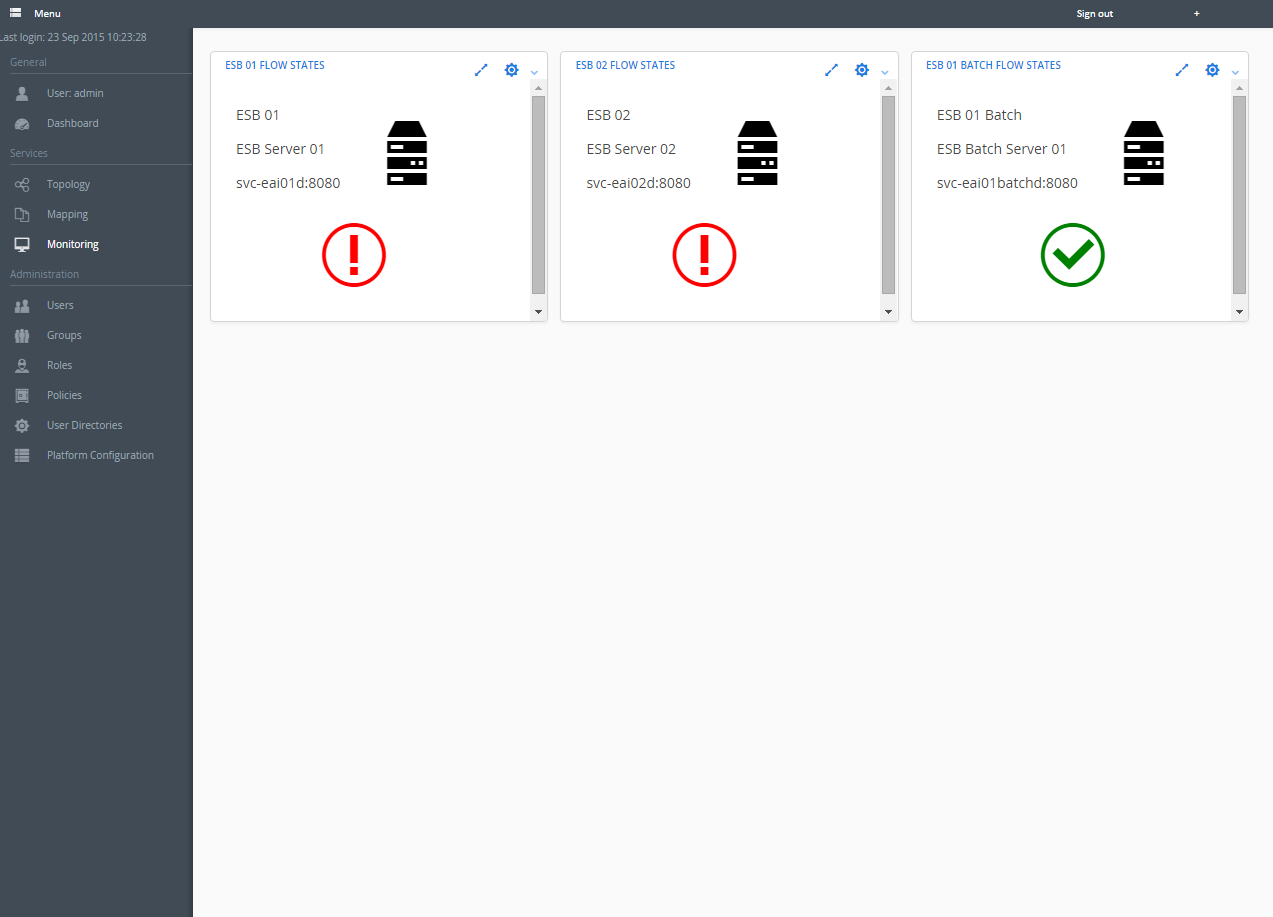


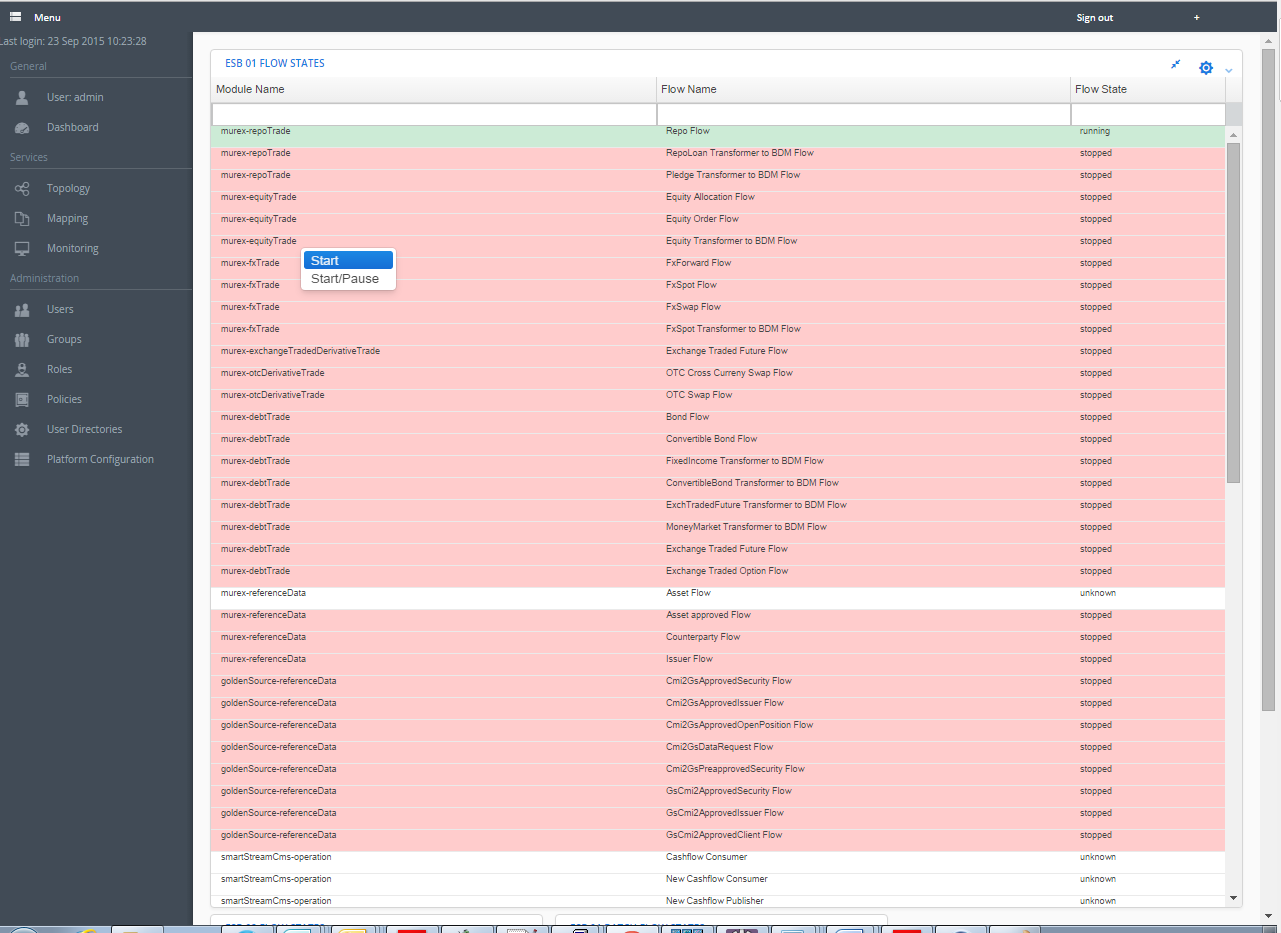






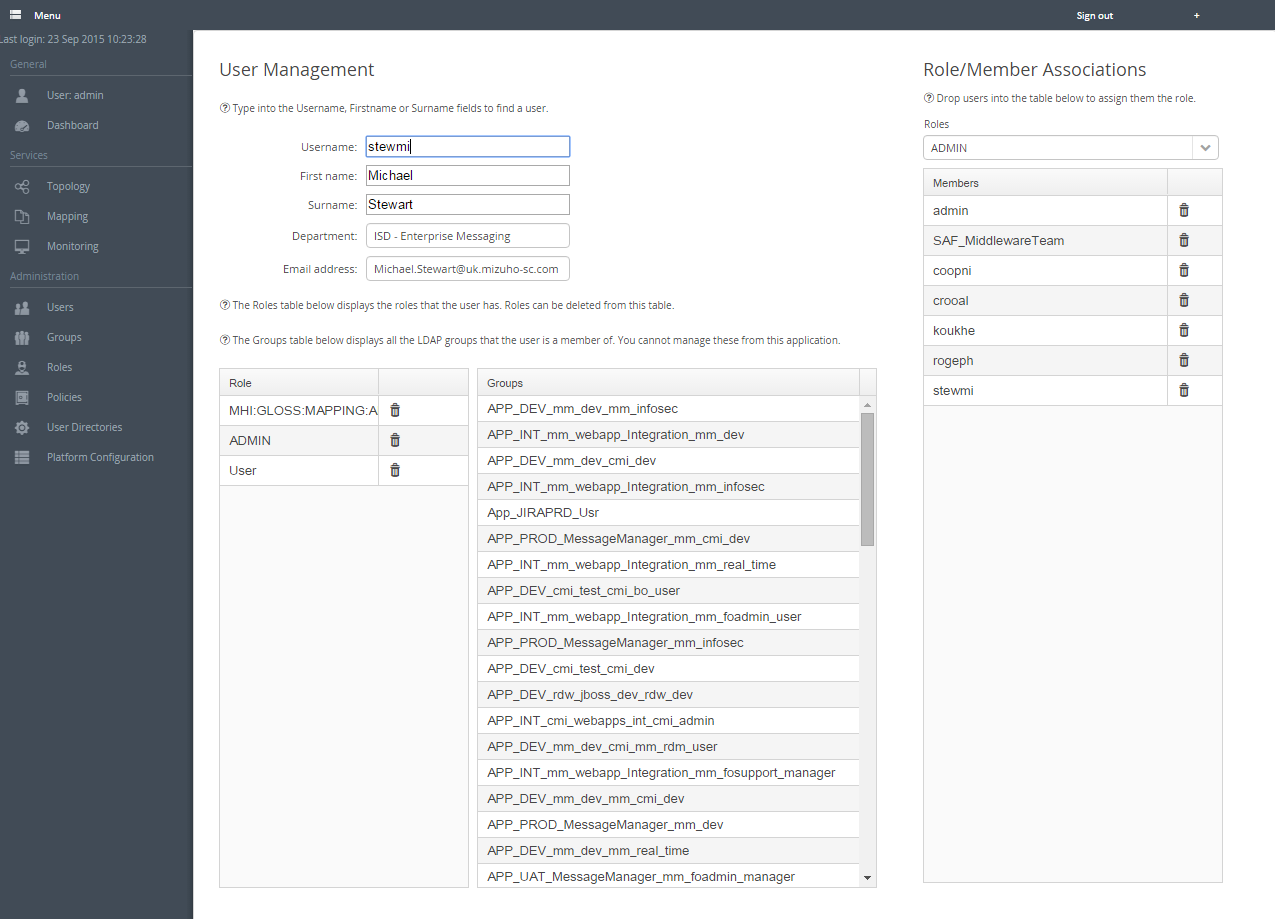
## Monitoring View



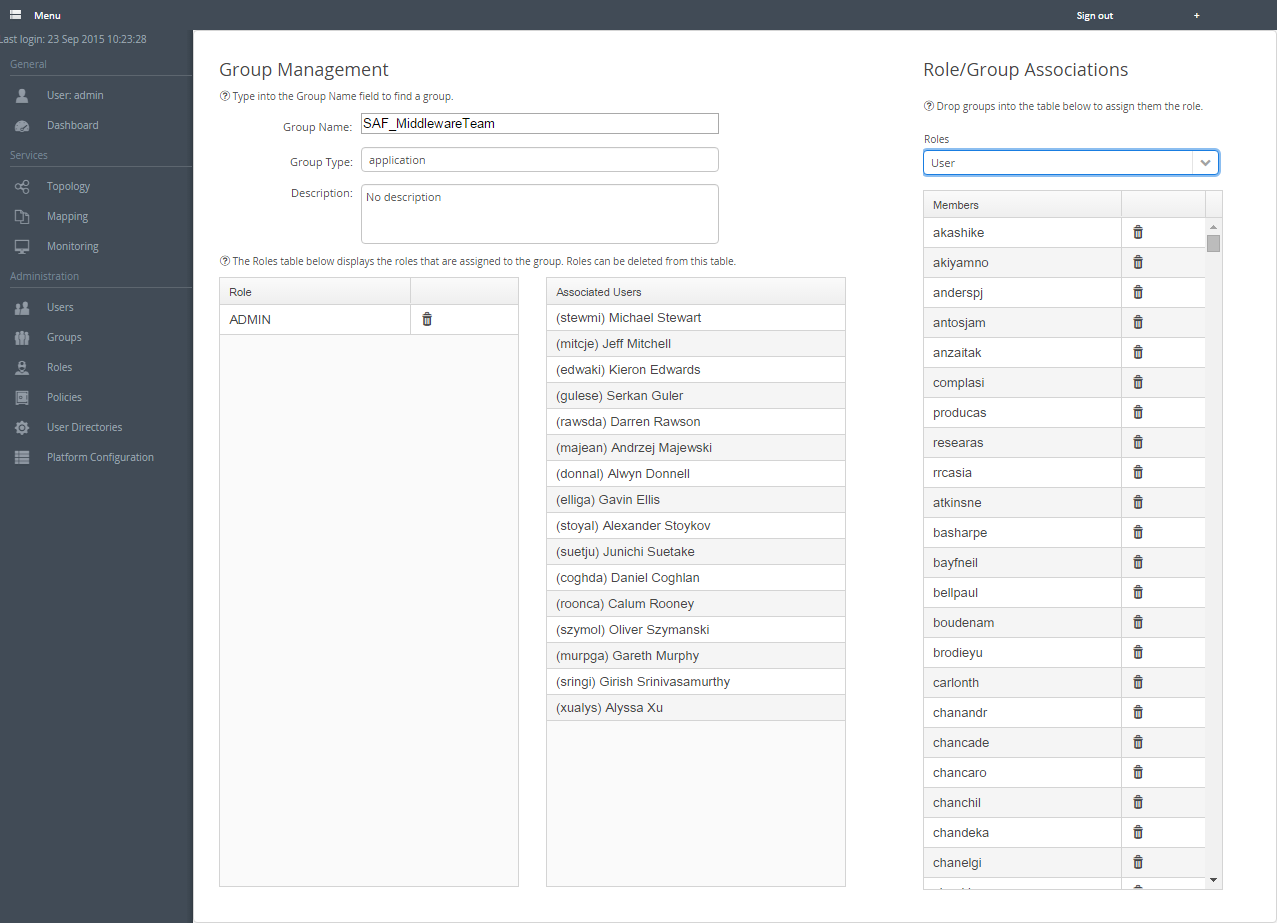


# Administration

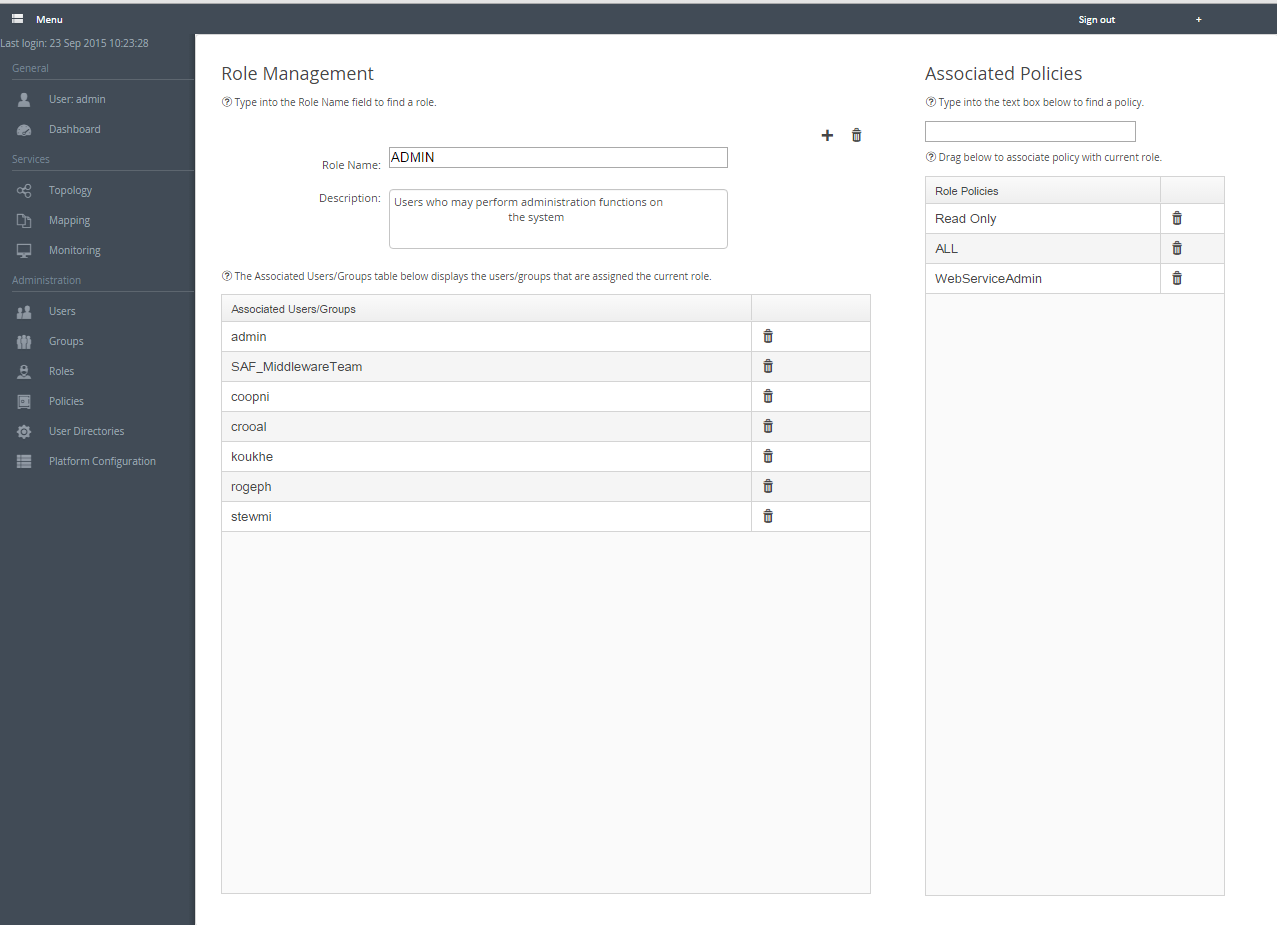
## User Administration



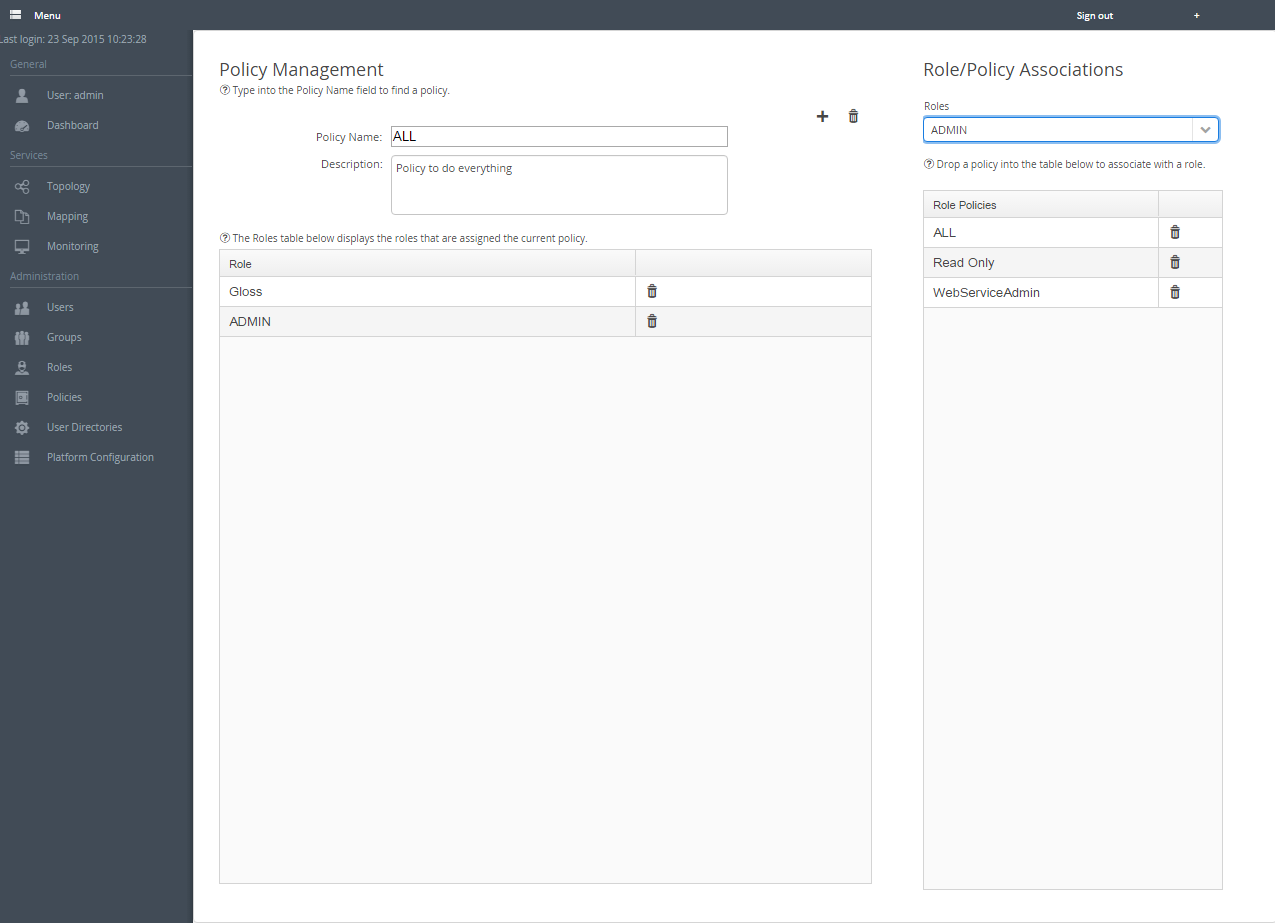
## Group Administration



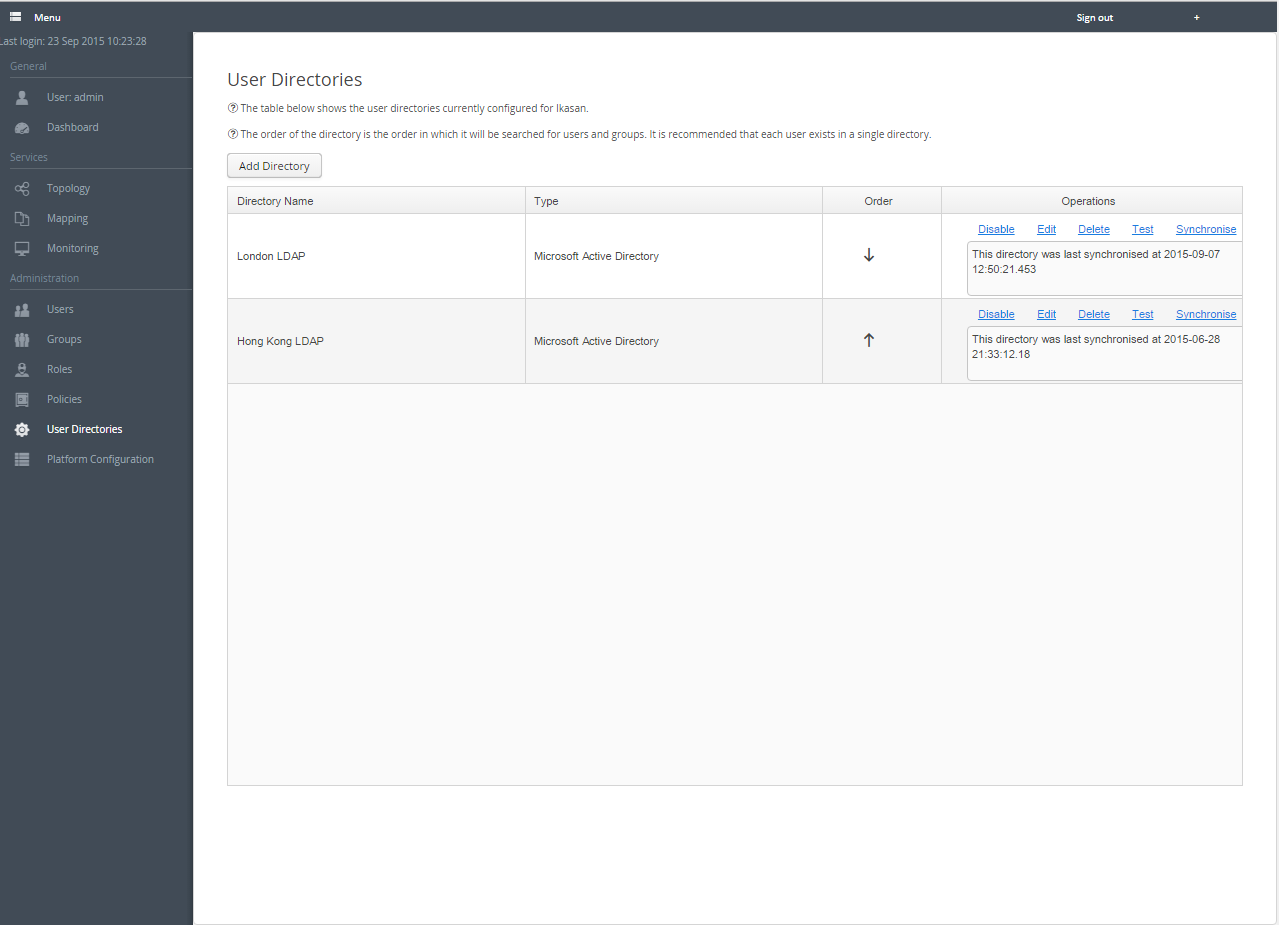
## Role Administration

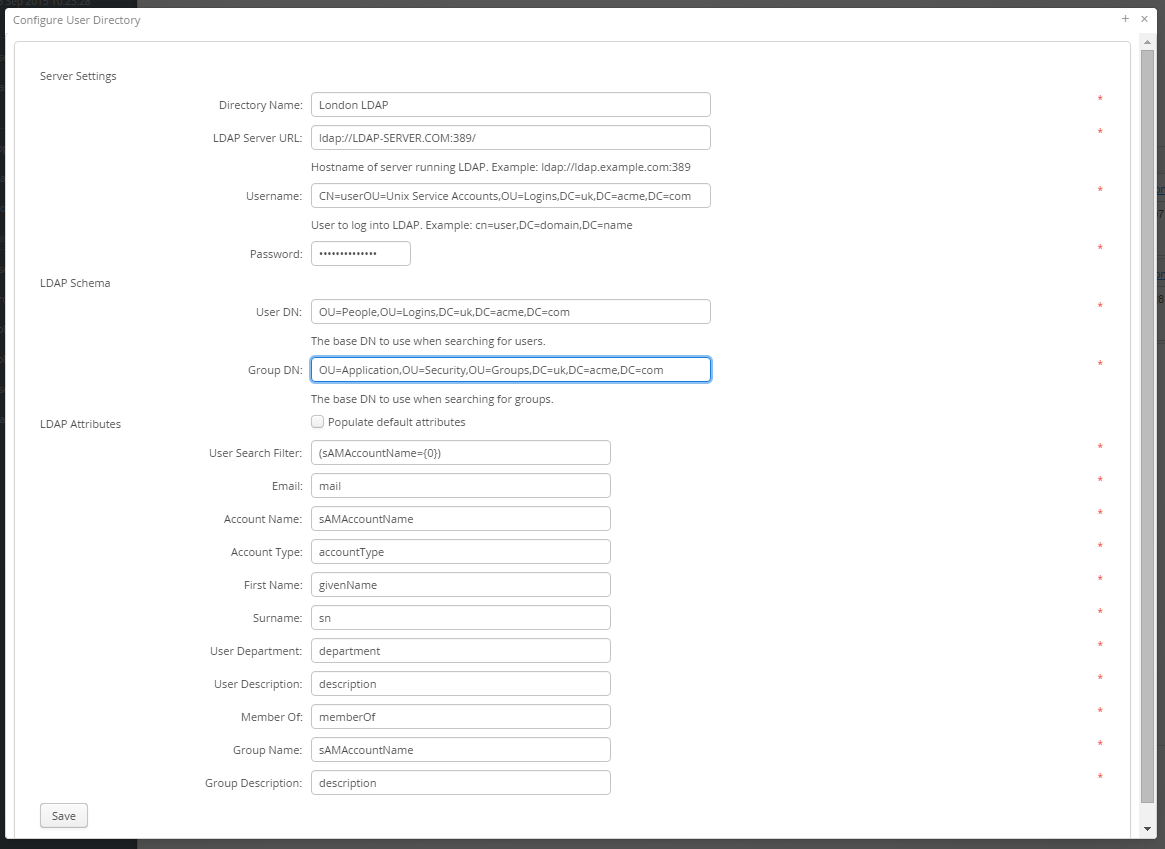


## Policy Administration



## Managing User Directories





## Platform Configuration

