MISYS | FusionBanking

Misys **Fusion**Banking Payment Manager 5.1.1

Administrator Guide

Version 1.01

Connect
Innovate
Expand™

Copyright

Disclaimer

Misys does not guarantee that any information contained herein is and will remain accurate or that use of the information will ensure correct and faultless operation of the relevant service or equipment. Misys, its agents, and employees shall not be held liable to or through any user for any loss or damage whatsoever resulting from reliance on the information contained herein or related thereto. This document contains information proprietary to Misys. Misys does not undertake mathematical research but only applies mathematical models recognized within the financial industry. Misys does not guarantee the intrinsic theoretical validity of the calculation models used. It is the obligation of the customer to ensure that responsible decisions are taken when using Misys products.

Feedback

Do you have comments about our guides and online help? Please address any comments and questions to your local Misys representative.

Need more information? Read more about our products at http://www.misys.com/software or contact your local Misys office at http://www.misys.com/contact-us.aspx.

Contents

Chapter 1 Technical Requirements 6
Mandatory Components 6
Misys BankFusion Meridian, FusionBanking Message Manager and FusionBanking Payment Manager Run Time Environment 6
IBM System i DB2/400 Minimum Environment 7
Hardware and Software Requirements 7
Development Environment 7
Client Environment 8
Chapter 2 Introduction 9
Chapter 3 Overview of FusionBanking Payment Manager 10
FusionBanking Payment Manager Workflow 10
Payment Alerts 10
Authorising and Verifying Payments 11
Releasing Payments 11
Chapter 4 Configuring FusionBanking Payment Manager 12
Common Screen Layouts 13
BIC/Local Bank Code Query Tools 14
Working with Static Data Tables 15
Setting Authorisation Permissions and Alerts 17
Maintaining Static Data Authorisation 17
Modifying Static Data which Requires Authorisation 18
Authorising Changes to Static Data 19
The Configuration Menu 20
Host Administration 21
Code Tables 27
Repository Actions 38
Report 42
Infrastructure Maintenance 42
The Security Menu 42
Roles, users and permissions 42
Security roles 43
Security Permissions 43
Adding users in LDAP 51
The Security Navigation Pane 51
The System Control Data Menu 62
Payment Data 63
Alert Data 64
Payment Configuration 68
Rule Data 76
STP Criteria 78

Configuring the FileAct Application 79
Configuring the SWIFT Alliance Gateway 79
Configuring SWIFTNet DNs 82
Configuring FileAct over SAG Services 82
Transfer Profiles 83
Scheduling tasks 92
Configuring Batch Files 92
Enabling Batch File Functionality 92
Batch File Profile Details 92
Batch File Information 93
Batch File Formatting and Message Information 94
Batch File Response Handling 97
Batch file scheduler 98
Configuring Message Templates 99
Importing Jasper Reports 102
Configuring iReport 104
Configuring Credit / Debit Mandate Lookup 107
Configuring Clearing Systems 110
Chapter 5 Configuring Compliance Watch List Processing 114
Chapter 6 Configuring Target2 Processing 115
Background 115
Configuring the filter 115
The switchable features 115
Appendix A - Parameters list for security complex permissions builder conditions 117
Appendix B - Payments Netting 120
Overview 120
Netting Message Types 120
FusionBanking Payment Manager Workflow Components 120
Appendix C - Switchable Features 138
Appendix D - Automated Cancellation Processing 141
SWIFT 141
Codeword model 141
ISO15022 model 142
MTn92 model 142
Cancellation prerequisites 143
Appendix E - Multiple Message Processing 144
Overview 144
Enabling the Multiple Message Functionality 144
Identifying Potential Components 145
MT210 Multiple message criteria 145
MT102 Multiple message criteria 146
MT203 Multiple message criteria 146
Generating Multiple Messages 147

Creating multiple messages when the maximum components are available 147
Creating multiple messages when the maximum size is reached 147
Releasing messages at cut off time 147
Message States 148
Individual messages 148
Component messages 148
Multiple messages 148
Configuration Options 149
Currencies Table 149
Multiple Message Service Profile 149
Manual Routing Actions for Potential Multiple Messages 150
Route as Individual 150
Route as Part of a Multiple 150
Multiple Message Display Facilities 150
Glossary 151

Chapter 1 Technical Requirements

Below are the minimum technical requirements for BankFusion Meridian, FusionBanking Message Manager and *FusionBanking Payment Manager version 5.1.1*. It describes the mandatory components, as well as the minimum hardware and software requirements.

The Company reserves the right to modify these hardware, software, and architecture requirements at any time at its sole discretion.
The Client must enter into appropriate license and maintenance service agreements direct with the owners or distributors of required components not provided by the Company. The Company makes no representations and accepts no liability for such products nor any of the services linked to them.
All PCs should have a keyboard, a mouse and a network card.

Mandatory Components

Misys BankFusion Meridian, FusionBanking Message Manager and FusionBanking Payment Manager Run Time Environment

Application Server	IBM WebSphere Application Server version 7.0.x (Base, Network Deployment and Express), see http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27006921
Hardware and Software Platforms	Pre-requisites as listed on the IBM WAS 7.0 web site, see http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27006921
Databases	DB2/400 plus associated JDBC drivers DB2 LUW v10.5 or higher plus associated JDBC drivers Microsoft SQL Server 2008 plus relevang Microsoft JDBC drivers Oracle v11g + thin JDBC drivers A database is required for the BankFusion Meridian 5.0 runtime server. This database may be hosted on a different machine from the BankFusion Meridian server. Where BankFusion Meridian 5.0 is a component of FusionBanking Message Manager or FusionBanking Payment Manager 5.1.1, this will normally be the 5.1.1 database server. A separate database server is recommended for FusionBanking Message Manager or FusionBanking Payment Manager 5.1.1 implementations, with the exception of System i, where the built-in database may be used on the physical server that hosts the application server.
Other	IBM WebSphere MQSeries version 7.0.1

IBM System i DB2/400 Minimum Environment

The minimum environment for the IBM System i DB2/400 is as follows:

- 1-way / 1000 CPW
- i5OS at V5R4 or higher
- 1GB
- 3x 35 GB Disk
- RAID 5 protection
- PC console via Ethernet LAN
- Integrated 10/100/1000 Mbps Ethernet port

Hardware and Software Requirements

The following paragraphs indicate the hardware and software requirements for both development and client environments of *FusionBanking Payment Manager version 5.1.1*.

Development Environment

Hardware	PC Workstation
Processor	x86 architecture -32-bit 2GHz processor (or better)
RAM	4GB
Hard Disk	4GB free
Monitor and Graphics card	Any monitor & card supported by the operating system. Screen resolution of 1024x768 and > 256 colours is required.
SOFTWARE	
Operating System	Windows XP Service Pack 3 / Windows 7 Professional Service Pack 1
Database drivers	Relevant JDBC drivers for Database platform if testing runtime on a PC development workstation
Platform To test runtime on the development workstation it is recommended that WebSphere Application Server and WebSphere MQ be installed.	Java Runtime Environment v1.5 when using BankFusion Meridian Java development environment IBM WebSphere MQ Series version 7.0.1 or above for Windows IBM WebSphere Application Server version 7.0.x or above for Windows Internet Explorer v7 and v8 with latest Service Packs and Security patches are recommended; v6 is still supported. Optional: IBM Client Access - only needed for running System i session on PC

Client Environment

Hardware	PC Workstation
Processor	x86 architecture – 32-bit 2GHz processor (or better)
RAM	4GB
Hard Disk	4GB free
Monitor and Graphics card	Any monitor & card supported by the operating system. Screen resolution of 1024x768 and > 256 colours is required.
Other	Network connection to the server
SOFTWARE	
Operating System	Windows XP Service Pack 3 / Windows 7 Professional Service Pack 1
Other	Internet Explorer v7 and v8 with latest Service Packs and Security patches are recommended; v6 is still supported.

Chapter 2 Introduction

FusionBanking Payment Manager is a J2EE application for processing payments. It translates and delivers payments between systems, regardless of the underlying message standards, and can be used with a variety of host systems and target networks.

This guide describes how to configure the system components within FusionBanking Payment Manager for individual users. The intended audience is system administrators.

The scope of the guide covers all the applications available within FusionBanking Payment Manager. Where your bank has not licensed a particular application, this functionality will not be available to you.

This guide should be read in conjunction with the following documentation:

BankFusion Meridian with Message Manager Installation Guide	This describes how to install BankFusion Meridian with Message Manager. Please note that this can also be used for the FusionBanking Payment Manager.
FusionBanking Payment Manager User Guide	This describes the functions and facilities available in FusionBanking Payment Manager Explorer, the graphical user interface (GUI) to FusionBanking Payment Manager.
BankFusion Meridian 5.0 User Guide	This describes BankFusion Meridian, the middleware product providing base services for FusionBanking Payment Manager.

Chapter 3 Overview of FusionBanking Payment Manager

FusionBanking Payment Manager Explorer provides a number of features which allow you to successfully manage payments. These include:

- A query function and audit viewer that allows users to define their own queries to search for payments and also track a payment's path through the system and view its content at any point in its progress.
- A payment alert system for notification of payment issues
- A payment release system for storing future dated payments and releasing them on time
- Priority for urgent payments
- Manual input and repair of messages
- Custom actions for queues
- Message archival
- System alerts
- Report printing
- An audit trail and checking mechanism to track and monitor data changes

These features are governed by security control which combines user role-based access with privileges to ensure the right payments are seen by the right users.

FusionBanking Payment Manager Workflow

FusionBanking Payment Manager Workflow includes packaged interfaces for processes such as funds checking, Watch List Checking and CSMs such as SEPA, STEP2, TARGET2, SIC, HK-RTGS. These are all based on frameworks which allow banks to use the embedded integration toolkit to utilise existing systems and to connect new channels and CSMs with minimal effort.

Efficient integration to external networks Basing core processing on generic message formats insulates the hub from the complexities of external network formats and rules. This approach significantly reduces the effort of integrating a new payment network because core processing and logic is reusable.

Bespoke development, such as mapping to and from ISO 20022, is handled by dedicated network adaptors, allowing network specific development to be clearly defined and outsourced if appropriate.

Payment Alerts

The payment alerts functionality allows you to receive an alert when a pre-defined condition occurs for a payment, for example when a payment is approaching its settlement cut-off date. Alerts are role-based. If your role has been configured to receive payment alerts, you will be notified of an alert either by e-mail or screen popup, or both.

There are a number of instances in which a payment alert could be triggered, for example a watch list check failure or a payment approaching settlement cut-off date.

The type of alerts you will receive and subsequent action you will need to take depends on your role. You will need to contact your system administrator to determine which alerts you have been set up to receive.

Note that if your supervisor has requested that you should be aware of specific types of alert but not necessarily have access to them, it is possible you may receive alerts for payments you will not be able to view. This could be useful for informing other users, including your administrator, if they have missed an alert.

Authorising and Verifying Payments

FusionBanking Payment Manager supports verification only, up to six eye authorisation, or a combination of both.

The authorisation limit facility allows you to specify a maximum payment amount that a user is allowed to authorise. You can set up a limit for an individual but the facility is also role-based, so that if the user's role has a limit set on it, this will be taken into account too. If a user has an individual limit set, this will be used; if there is no individual user limit, the limit for the user's role will be used. If a user tries to authorise a payment with a value greater than their defined authorisation limit, an error message will be displayed.

There are a number of custom actions a user can be assigned to. For example, a verifier can send a payment that is queued for verification to a repair queue or cancel a payment that is queued for verification. There are also restrictions on the verification and authorisation actions that a single user can perform. For example, a user cannot authorise a payment that they have verified, nor can a verifier repair a payment that they have routed to a repair queue.

For information on how to configure authorisation limits, see Assigning Limits to Roles and Users.

For information on how to configure verification and authorisation actions as custom actions, see Configuring Queue Actions.

Releasing Payments

The payment release process allows you to release outgoing payments with a settlement date of today and in the future, on time and error-free. Outgoing payments entering FusionBanking Payment Manager are subject to a cycle check to identify such payments. Payments with a settlement date in the future are stored in a ‘warehouse’ queue and, subject to validation, are automatically released into the workflow on their release date (and time). Payments received with a settlement date of ‘before' today and payments that have already passed their settlement cut-off can be configured to be routed to a repair queue and an alert will be raised. Payments received with no value in the **Value Date** field are sent without undergoing checks. For urgent or exceptional release requests it is possible to manually release a payment before it reaches its specified release date or release time.

For information on how to configure criteria for releasing payments, see *Payment Release Maintenance*.

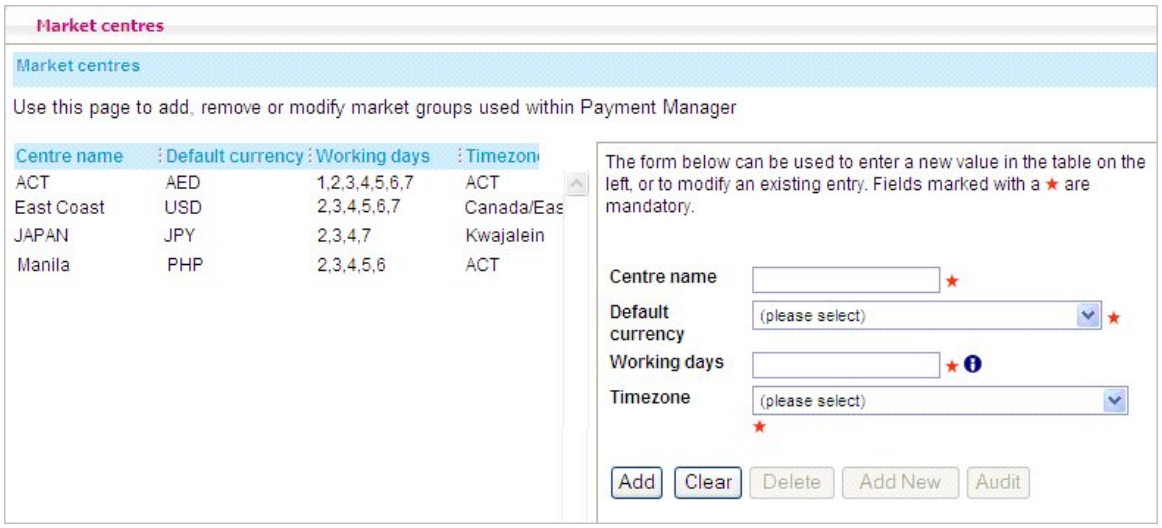
Chapter 4 Configuring FusionBanking Payment Manager

A number of configuration options are available within the FusionBanking Payment Manager Explorer. They are accessed from the Administration menu at the top of the main screen.

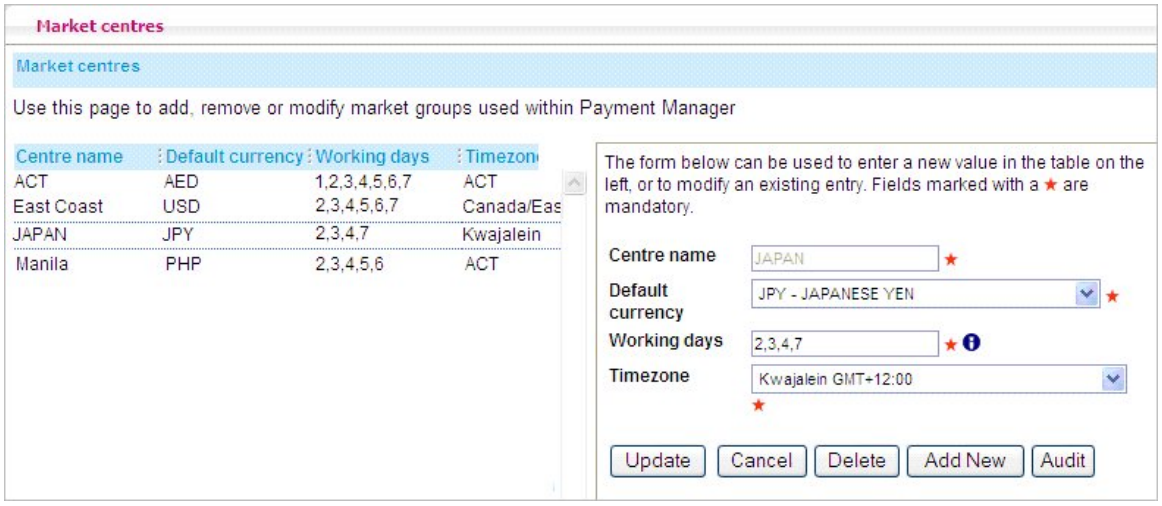
Option	Function
User Preferences	Allows you to choose your preferred display settings for the FusionBanking Payment Manager Explorer user interface.
Configuration	Allows you to configure host functionality, code tables and user custom actions such as payment authorisation and release.
Security	Allows you to set up users, roles and permissions. Role-based functions include payment authorisation and payment alert notification.
System Control Data	Allows you to set up static data used for straight-through processing and change the system base currency. You can also access a number of payment configuration functions such as payment release and payment priority.
Message Locks	Displays all the locks currently held in the system.
File Act Configuration	Describes how to configure the FileAct application which allows you to transfer files via SWIFTNet FileAct.
Batch File Configuration	Describes how to handle batch files.
Ad Hoc File Transfer	Allows you to manually upload files to the FileAct application.
Raise Alerts	Allows you to send messages to other users.
Template Editor	This is described in the FusionBanking Payment Manager User Guide.
Admin Reports	Allows you to run query definition and security audit reports.
Reports	Allows you to run payment reports.

Common Screen Layouts

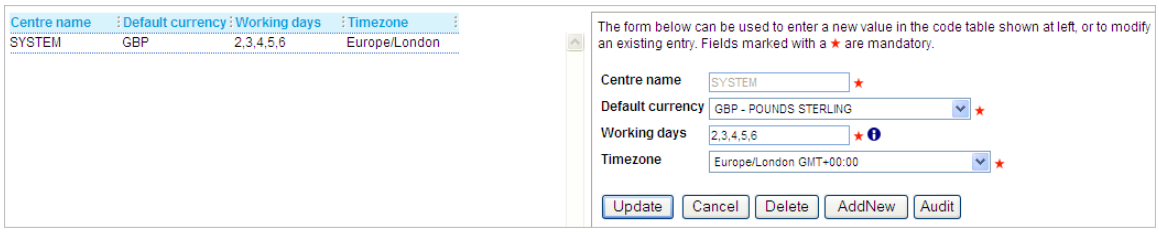
A number of input screens have a common layout, an example of which is given below.



To add a new entry, enter the new details in the fields on the right hand side of the screen and click **Add** to save the details or **Clear** to remove them.

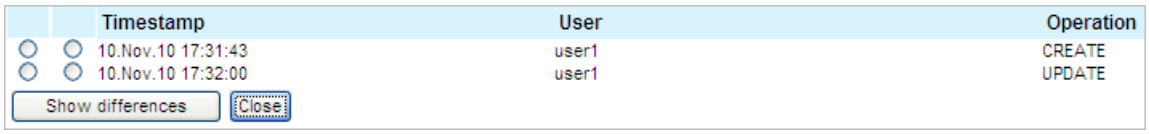


To modify an entry, select the entry from those displayed at the left hand side of the screen and modify the details.

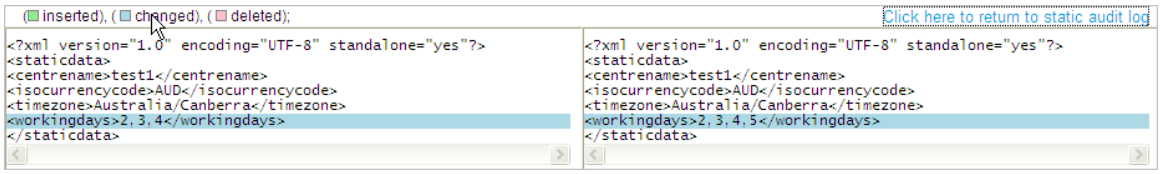


Click **Update** to save the new details or **Cancel** to remove them. You can delete the entry by clicking **Delete** or add a new entry by clicking **AddNew**.

Clicking **Audit** allows you to see any changes made to static data, as well as pending changes.

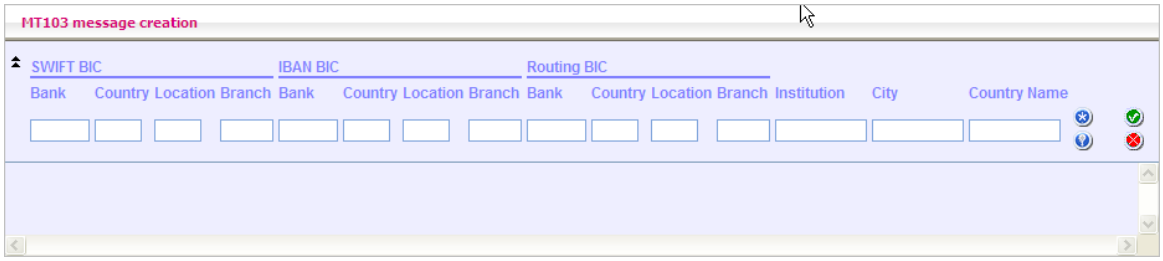


The dialog displayed shows the type of operation carried out, the user who carried out the operation and the date and time of the operation. To see the differences between two entries, select the appropriate radio buttons, one from each column as shown above. In the example shown below it can be seen that in the column on the right hand side, the number of working days has been changed.



BIC/Local Bank Code Query Tools

The Customer/BIC directory query tool provides a means of searching for valid BICs from the SWIFTRef Bank directory.



Wild-card entries such as * can be used to represent one or more characters. For example, the entry *BD* in one of the Bank fields would return all BICs containing the letters BD. Also, you can search on more than one field.

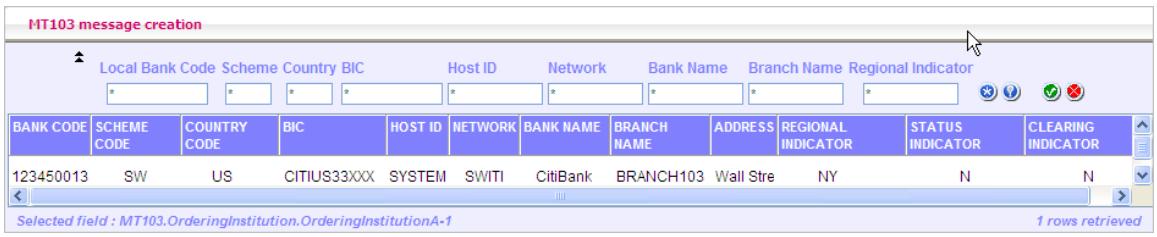
 - **Reset** clears the search fields

 - **Search** activates the search process

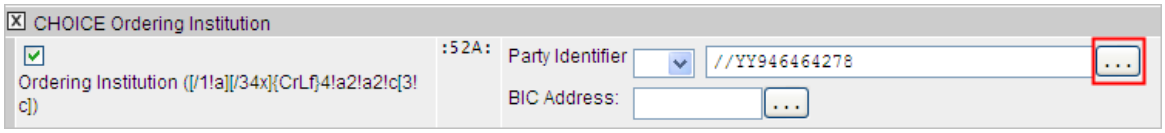
 - **Select** returns the selected BIC from the results grid to the fields the query tool was activated from

 - **Cancel** removes the query tool from view

The local bank code query tool provides a means of searching for local bank codes. The same wild card facilities and search buttons as above apply to this feature also.



This facility is present on fields 52A, 52C, 52D, 56A, 56C, 56D, 57A, 57C, 57D, 58A and 58D of message types MT101, MT202, MT210, MT103 and MT102.



Working with Static Data Tables

FusionBanking Payment Manager is shipped with a number of static data tables, shown below.

Static Data Table	Description
Allowed currencies	Defines allowed currencies for a correspondent
Assign queue actions	Assigns the actions that can be performed against a specific queue
Base currency	Assigns the default system currency
BIC features	Assigns a switchable feature against a specific BIC code
Business entities	Available business entities / lines of business
Character conversions	Translation of characters not supported by the SWIFT FIN network
Correspondent maintenance	Contains correspondent bank details
Country maintenance	Contains a range of data about countries defined in the system
Create/modify custom action filters	Assigns filter to custom actions.
Create/modify custom actions	Custom project queue actions
Create/modify queue actions	Contains data used to define custom and default actions
CSMs	Contains details about supported clearing and settlement mechanisms
Currencies	The ISO currencies available for use within the system
Custom BICS	Contains custom BIC codes that can be used within the system
Electronic Broker	Electronic broker details
Error Codes	Codes and text description for the SMS / e-mail alerts that can be generated
Host features	Details of the switchable features in use by a specific host system
Host groups	Contains details of defined host groups (aggregated host systems)
Host system routing	Allows a given BIC to be associated with a specific host system
Hosts	Contains details of host systems in use
IBAN format	Defines the IBAN structure of a country for IBAN validation purposes

Static Data Table	Description
Local bank code	Identifies an institution and/or a branch at a domestic level
Market centre holidays	Defines holidays / non-working days for specific market centres
Market centres	Contains date and time details for market centres
Nostro table	Nostro agent data
Parties	Party and counterparty data used for SSI creation during netting
Payment limit amounts	Assigns amount limits per host, business entity and currency
Payment queue priority	Data used to assign priority to queued payments
Payment release maintenance	Data used to assign payment release times and settlement cut-off times
Report groups	Definition of the Report Groups that Jasper reports can be associated with
Routing criteria	Defines the criteria of the rule for routing messages
Routing outcome	Defines the possible outcome of the rule and criteria for routing messages
Routing rule	Defines the rule for routing messages
SMTP (mail) Server Maintenance	Defines the SMTP server details used to forward alerts by e-mail
Standard settlement instructions	Details of Standard Settlement Instructions (SSIs) used in payments netting
STP correspondents	STP Correspondent data
Template	Data used in the definition of message templates
Third Party Payment Exceptions	Identifies valid beneficiaries for a given customer

A facility is available for authorising changes to data held within these tables.

The following static data tables do not support authorisation of changes:

- SWIFTRef Upload
- RMA Upload
- FileAct static data tables
- Batch File static data tables

Setting Authorisation Permissions and Alerts

To set up authorisation capabilities, you can assign any of the following permissions to users in the Authorise Static Data Role:

Static Data Table	Description
Define static data tables as requiring authorisation after amendment	Define authorisable static data
View static data held in system tables (Menu selection **Administration > Configuration > Code Tables**)	View system tables
Edit static data held in system tables (Menu selection **Administration > Configuration > Code Tables**)	Configure system tables
Authorise static data held in system tables (Menu selection **Administration > Configuration > Code Tables**)	Authorise system tables
View system control static data (Menu selection **Administration > System Control Data**)	View system control data
Edit system control static data (Menu selection **Administration > System Control Data**)	Configure system control data
Authorise system control static data (Menu selection **Administration > System Control Data**)	Authorise system control data
View static data in message templates (Menu selection **Administration > Message Template**)	View message templates
Edit static data in message templates (Menu selection **Administration > Message Template**)	Configure message templates
Authorise static data in message templates (Menu selection **Administration > Message Template**)	Authorise message templates

These are complex permissions, allowing you to select the static data tables to be associated with the permission.

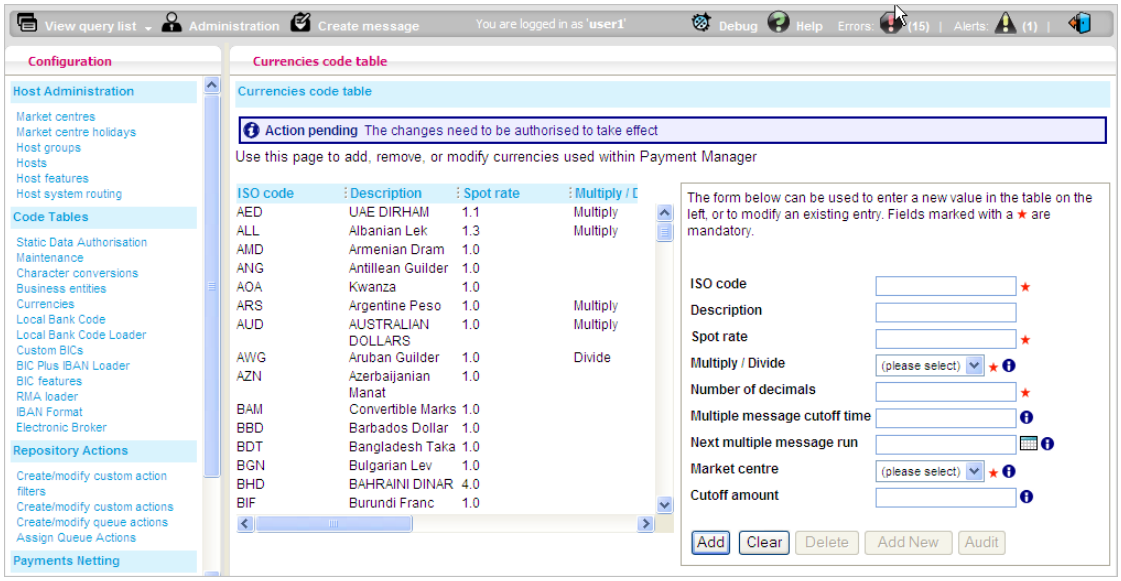
You can set users up to receive an alert, such as an email or screen popup (or both), when authorisation is required for an amendment to a static data table. In order to receive an authorisation alert, the user must have the Authorise permission for the particular table and have been configured to receive authorisation alerts.

Maintaining Static Data Authorisation

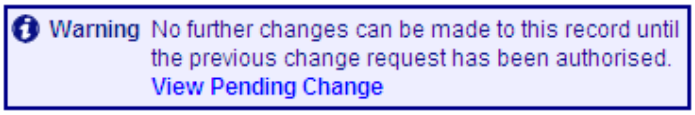
The facility to set authorisation on or off for static data tables can be accessed from the menu selection **Administration > Configuration > Static Data Authorisation Maintenance**. For more details on this function, see Static Data Authorisation Maintenance.

Modifying Static Data which Requires Authorisation

Where static data tables have been set up so that any modifications made to them will require authorisation, an information message will be displayed, as below, when any record in such a table is amended.



An alert will be sent to the supervisor responsible for authorising changes and no further changes can be made to this record until the authorisation has been carried out. If an attempt is made to modify data with changes pending, a warning message will be displayed and the pending changes can be viewed.

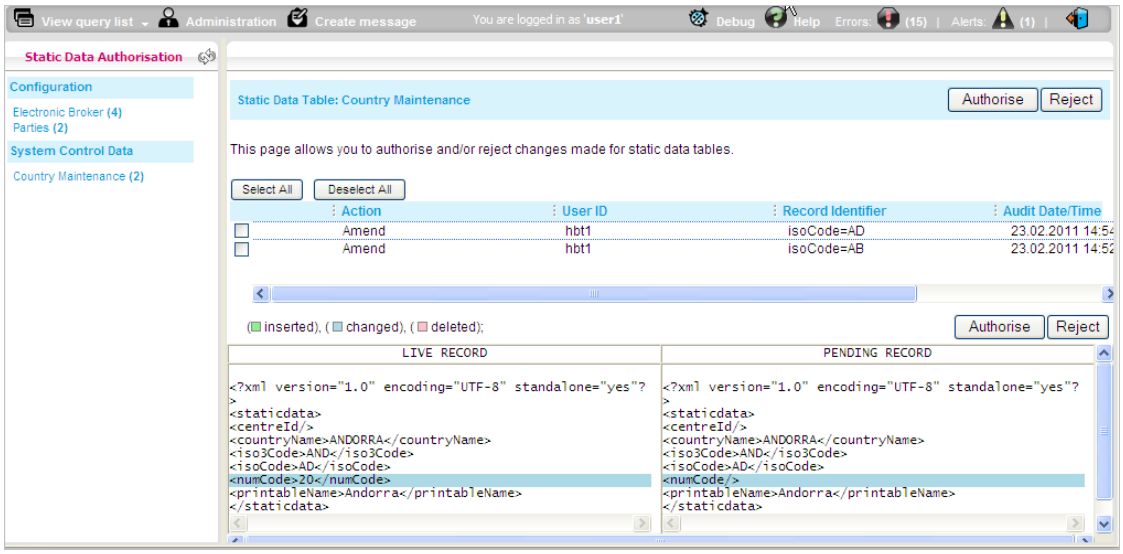


Authorising Changes to Static Data

To authorise changes to static data, select **Static Data Authorisation** from the Administration menu. A list of static data tables is displayed at the left of the screen. The number in parentheses indicates the number of records requiring authorisation for a particular table.

Select a table from the list. The records requiring authorisation will be displayed. Records can be easily identified from the **Record Identifier** (or key) column entries. Some records may have more than one identifier and an entry of "" indicates that the particular field is empty.

To view the details of the change to a particular record, click the entry to select it. The details will be displayed in the bottom panel of the window. The live record shows the unchanged record which is available for use; the pending record shows those changes requiring authorisation.



To authorise or reject any of the changes in the top panel, check the box(es) next to the change(s) and click **Authorise** or **Reject** in the top panel. A warning message will be displayed asking if you want to perform authorise/reject on rows with ticked checkboxes. Clicking **OK** will authorise/reject the selected change(s).

If you have the bottom panel displayed, you can also authorise or reject an individual change displayed therein by clicking **Authorise** or **Reject** in the **bottom** panel. A warning message will be displayed asking if you want to perform authorise/reject on the selected row. Clicking **OK** will authorise/reject the selected change(s).

If you do not have the required permissions to authorise or reject a change(s), a message will be displayed stating that another user must authorise/reject the change(s).

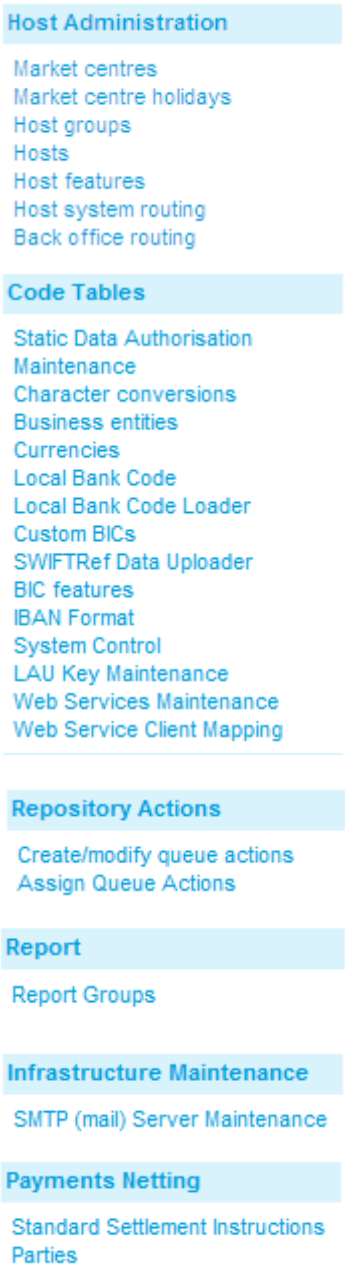
Once changes have been authorised or rejected, a message to that effect will be displayed.

To refresh the display of static data tables, click  .

You can also view pending changes via the Audit facility Common Screen Layouts.

The Configuration Menu

Configuration functions are subdivided into five groups, as described below.



Host Administration allows you to define Host Groups and to allocate Market Centres and Host Systems to Host Groups. It also defines the archiving processing requirements.

Code Tables allows you to view and maintain all system data used by the system such as currency codes, BIC, business entities and character conversions. In addition, the Static Data Authorisation Maintenance option allows static data tables to be flagged as requiring authorisation for changes.

Repository Actions allows you to set up custom actions and assign these actions to queues.

Report allows you to set up reports.

Infrastructure Maintenance allows you to set up a user's SMTP (mail) server to allow them to receive email payment alerts.

Payments Netting allows you to combine a number of payment and receive messages with similar settlement instructions to be netted together.

The static data tables above can be set up so that any modifications made to them will require authorisation (see Code Tables above).

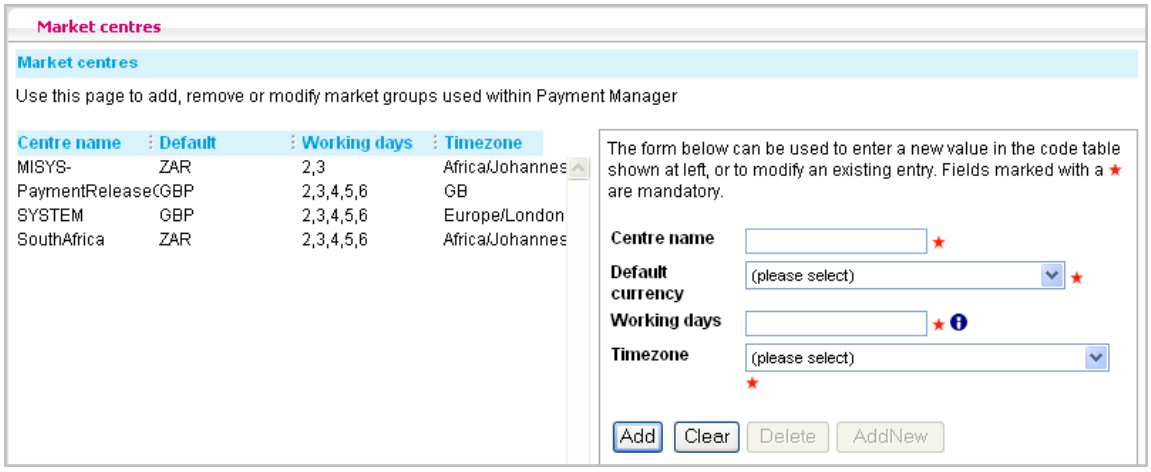
Host Administration

Market Centres

Market Centres allow time zone, default currency, working day and holiday information to be captured, which is then used to adjust dates and times according to the location of the user.

The following default market centre is supplied:

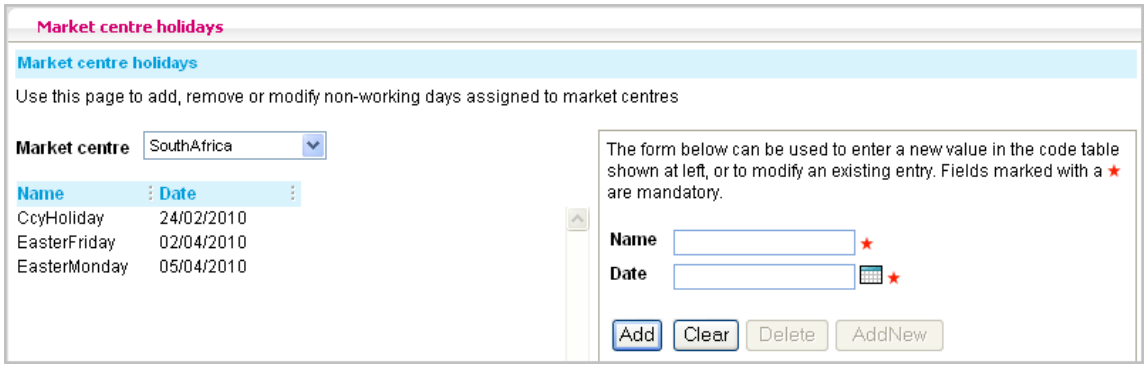
- Centre name - System
- Default currency - GBP
- Working days - 2,3,4,5,6
- Timezone - Europe/London



Field	Description
Centre Name	Enter a meaningful name for the market centre.
Default Currency	Select the currency associated with the market centre. A dropdown of ISO currencies is provided to select the appropriate currency.
Working Days	This denotes the working days in the market centre. Entry should be a comma-separated list of numbers representing the days of the week in this list: 1=Sunday, 2= Monday, 3=Tuesday, 4=Wednesday, 5=Thursday, 6=Friday, 7=Saturday. For example, to set Monday to Friday as working days, entry should be "2,3,4,5,6".
Time Zone	This is the time zone associated with the market centre. Select the appropriate time zone. This is used to help calculate the current run date for the market centre. This offset is used to calculate local time for a host when performing user queries or message processing functions.

Market Centre Holidays

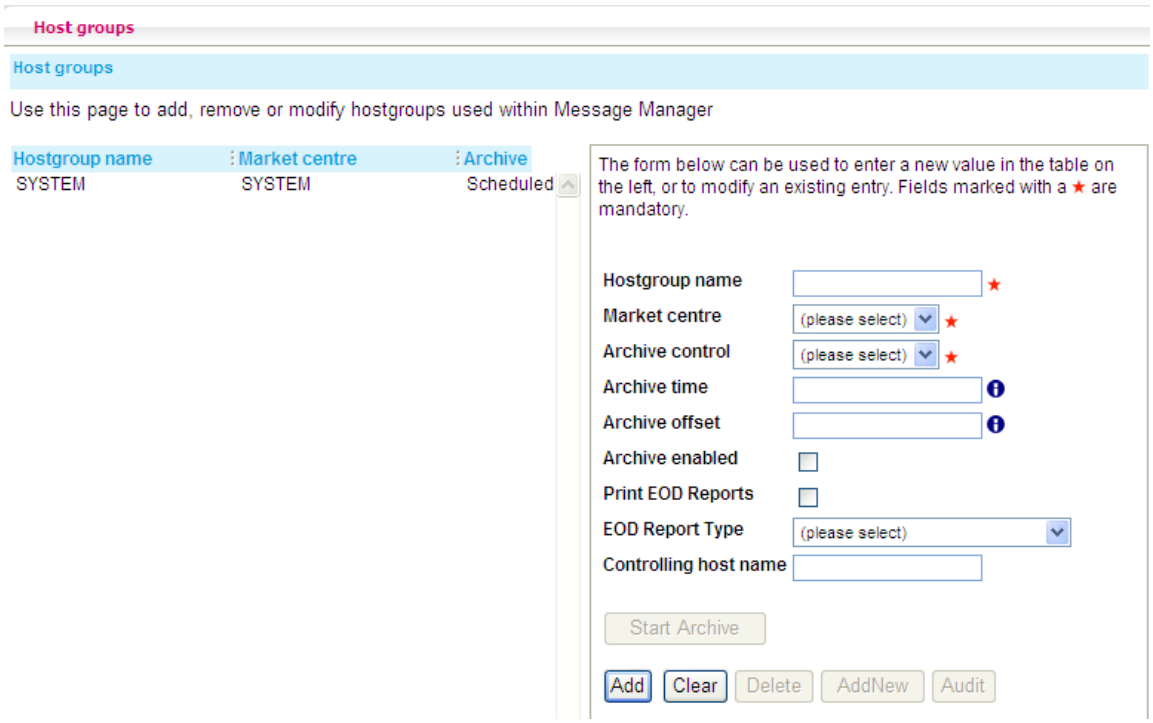
This table defines the public holidays in a particular market centre location. Together with the working days set in the Market Centres table, this is used to determine the run date and next working date for the market centre.



Field	Description
Name	The descriptive name of the holiday, e.g., New Year's Day.
Date	The date of the holiday. Select the date from the calendar picker or enter it manually using the date data-entry format specified in User Preferences (see Setting User Preferences).

Host Groups

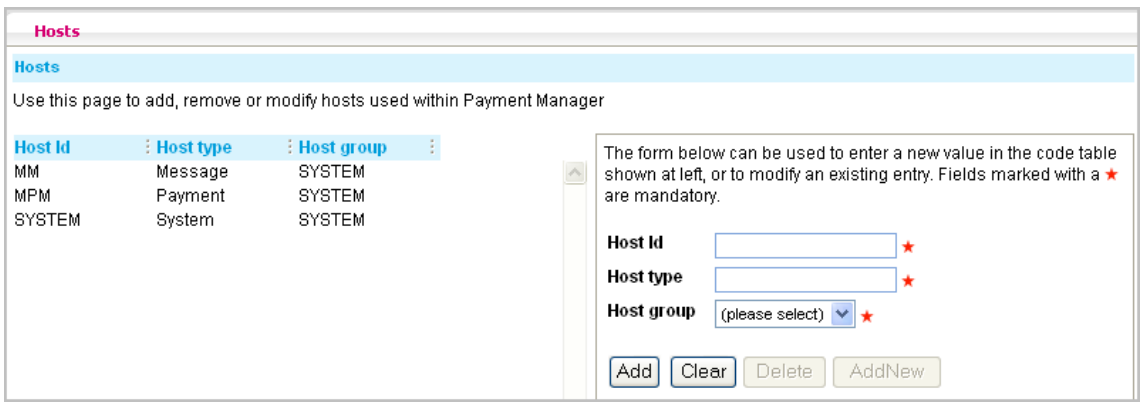
Many work-groups within a financial institution may use multiple host systems to book and account for transactions. FusionBanking Payment Manager's data design allows host systems to be aggregated as Host Groups. A typical host group operates on the same time zone and so is assigned a market centre which controls the run date within the host group. Archiving details are also set up at this level to enable dropping of historic messages from the live database and copied onto the archive database where they can be queried separately.



Field	Description
Host Group Name	Enter a meaningful name to identify the host group.
Market Centre	This is the market centre where the host group exists. A drop down of all market centres available in the system is provided.
Archive Control	Defines how the archiving process for the host group is initiated: Host triggered - a fully integrated host (such as Misys Midas Plus) sends a message to the server to trigger the archiving process. Scheduled – a schedule is configured for working days (non-working days of the week and public holidays are specified for the market centre attached to the host group). The archiving runs every working day at a scheduled time. Manual – a user initiates the archiving process.
Archive Time	The time when archiving should take place. Entry must be in 24-hour format. Entry to this field is optional. If entered, this will override the time specified at the customer level.
Archive Offset	Number of days after System Arrival Time (for other message types) that a message is retained on the database before being dropped.
Archive Enabled	Tick this box to activate the archiving process.
Print EOD Reports	**Print End-of-Day Reports:** if checked, End-of-Day queries are printed to the server automatically at End-of-Day; **Print Security Audits:** if checked, Security Audits are printed automatically at End-of-Day.
EOD Report Type	Report format can be any of the following: • Network dependent format report • Tabulated report • Detailed message report
Controlling Host name	This is the host that will determine when the archiving process will run and is used only for Host Triggered archiving. If this option is ticked, the host system elected will trigger the archive run for all that host group when FusionBanking Message Manager receives an appropriate rundate message.

Hosts

A host system represents a back-office system that feeds messages into or receives messages from Payment Manager. A number of host systems can be specified in FusionBanking Payment Manager.

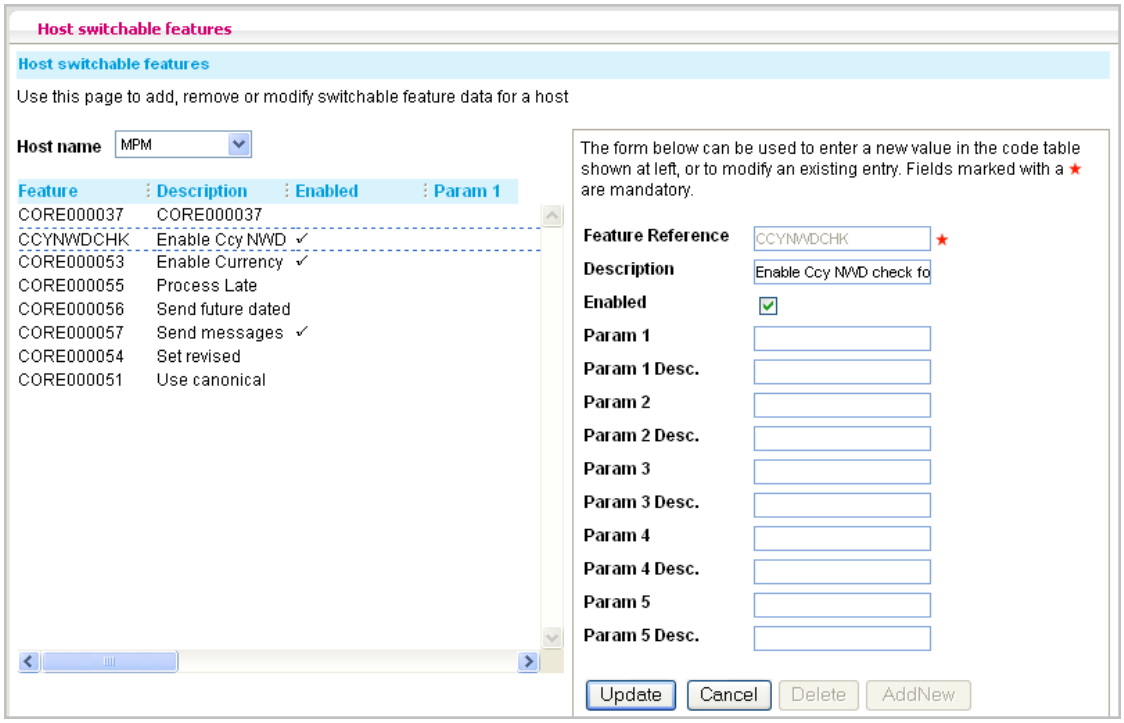


Field	Description
Host Id	A unique ID for the host system
Host Type	Narrative describing the type of host system (e.g. Equation, Midas, etc.).
Host Group	The host group to which this host is allocated.

Host Features

Switchable features allow FusionBanking Payment Manager processing functions to be enabled and disabled on a host by host basis without the need to change any underlying code. They can be toggled (on or off) within the user interface.

Switchable features can be defined on a per-host basis. Up to five optional parameters can be defined per switchable feature, per host. See Switchable Features Appendix C - Switchable Features for a list of switchable features supplied.

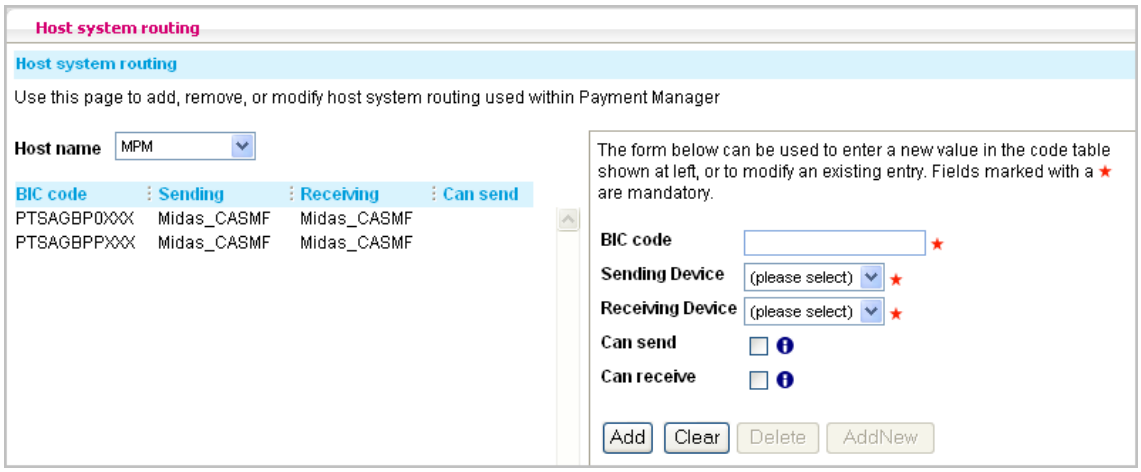


Host System Routing

Hosts and SWIFT devices are linked indirectly by Bank Identifier Codes (BIC). Multiple BIC codes can be associated with each host. For instance, multiple branches of an institution may connect to a single host. Each BIC associated with a host can be linked to up to two SWIFT devices, one for sending and one for receiving messages.

To link a host to a device, select **Administration > Configuration > Host system routing** from the main menu. Select the host name to which the SWIFT device is to be allocated from the dropdown.

The following screen is displayed.



The fields are as described in the table below:

Field	Description
Host name	A dropdown of all available host IDs is provided. Select host name to which the SWIFT device is to be allocated.
BIC code	Specify the BIC code that is assigned to the host. More than one BIC may be assigned per host.
Sending Device	When the BIC is used as a sender of a message, this field specifies the SWIFT device associated with it. A selection of pre-defined SWIFT devices is provided.
Receiving Device	When the BIC is the receiver of an incoming message, this field specifies the SWIFT device associated with it. A selection of pre-defined SWIFT devices is provided.
Can send checkbox	Check this box if this host can send internal messages.
Can receive checkbox	Check this box if this host can receive internal messages.

When routing messages internally, it is necessary that the BICs contained in the message fields, **SenderAddress** and **DestinationAddress** have the **Can send** and **Can receive** options checked respectively.

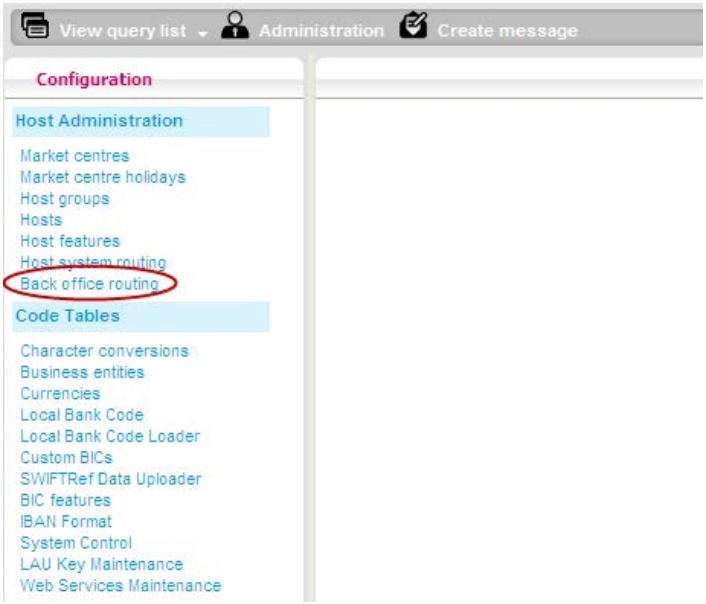
When sending messages from a host, the message's SenderAddress and DestinationAddress are looked up in the Host System Routing table. If the message is to be routed internally (**Can Send** is checked for the **Sender Address** and **Can Receive** is checked for the **DestinationAddress**), the outgoing message is copied to represent the incoming message and forwarded to the appropriate node in the receipt workflow. The original message is then moved to the appropriate node in the outward workflow.

If the message is not to be routed internally it is sent out to SWIFT via the device specified in **Sending Device**.

Each available endpoint is examined in a cyclic fashion until it identifies an available message. This message can then be brought into the database. A Customer ID, Group ID, Host ID and Business Entity are assigned to the message according to the destination address.

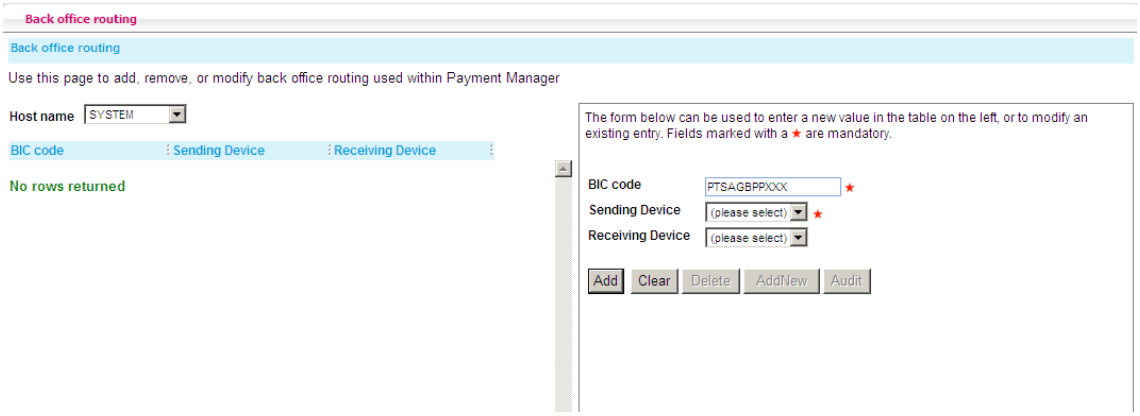
Back Office Routing

Back office routing allows routing to and from different back office adaptors. The code table for Back office routing can be accessed in the **Configuration** menu under **Administration**.



To link a Back Office to a device, select **Administration > Configuration > Back office routing** from the main menu. Select the host name to which the device is to be allocated from the dropdown.

The following screen is displayed.



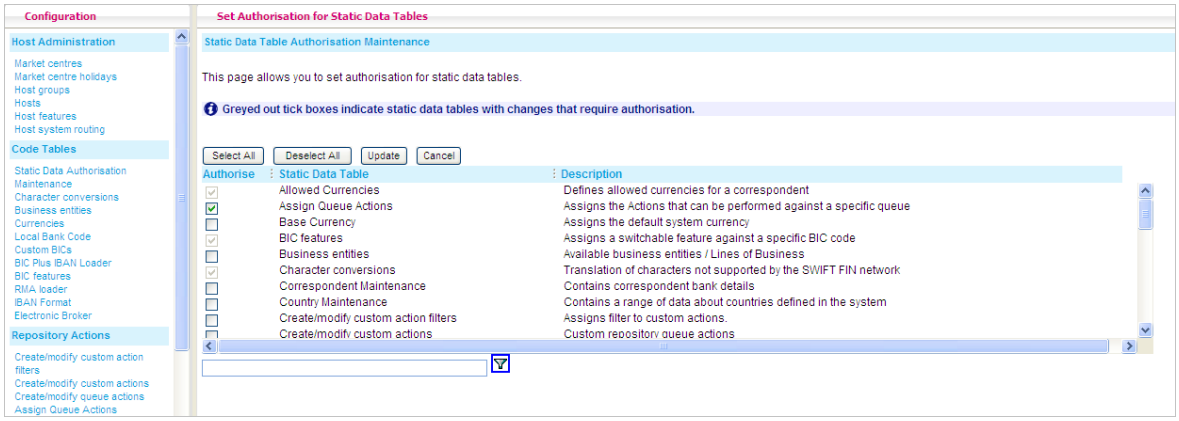
The fields are as described in the table below:

Field	Description
Host name	A dropdown of all available Host IDs is provided. Select back office to which the device is to be allocated.
BIC code	Specify the BIC code that is assigned to the host. More than one BIC may be assigned per host.
Sending Device	When the BIC is used as a sender of a message, this field specifies the device associated with it. A selection of pre-defined devices is provided.
Receiving Device	When the BIC is the receiver of an incoming message, this field specifies the device associated with it. A selection of pre-defined devices is provided. This field is not mandatory.

Code Tables

Static Data Authorisation Maintenance

This screen allows you to specify which static data tables require supervisor authorisation before modifications made by users can take effect. You must have the Define Authorisable Static Data permission assigned.



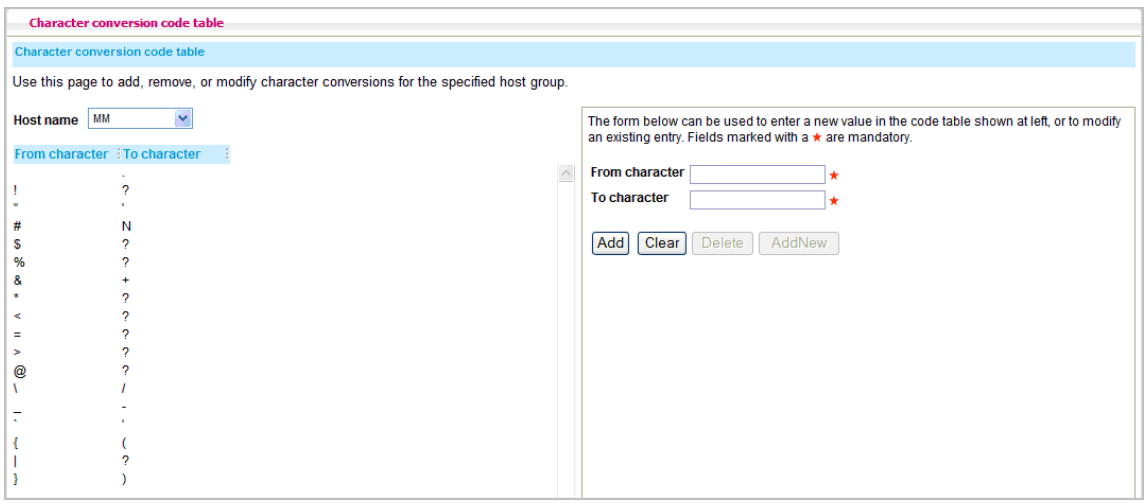
A scrollable list of static data tables is displayed. To turn authorisation on for all tables, click **Select All**. To turn authorisation on for individual tables, check the relevant box in the **Authorise** column. If a box is greyed out, this indicates that there are pending changes requiring authorisation for this table. These changes must be authorised before any further actions can be undertaken on the table.

Click **Update** to save your changes, or **Cancel** to reject them.

You can use the filter feature to find a specific table. The filter box is displayed next to the filter icon  . Enter the details in the box, for example 'curr' to find currency tables, and click the filter icon. Note that if you want to return to the display of all tables after using the filter, click **Update** to save any changes, followed by **Cancel**.

Character Conversion

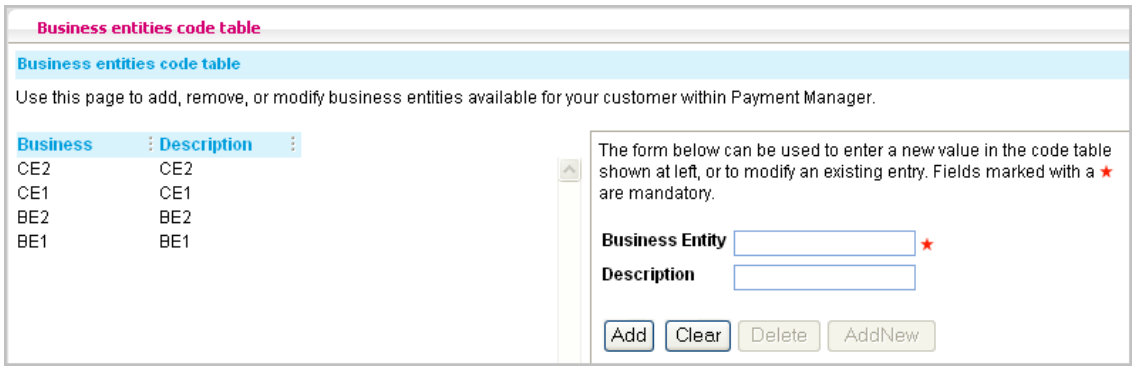
This table provides a translation from characters disallowed by the SWIFT FIN network to allowed characters. For example, '&' is not currently allowed, whereas '+' is. The conversion table can change '&' to '+'.



Field	Description
Host group	Specify the host group to add, remove or modify character conversions.
From character	Enter the invalid character.
To character	Enter the replacing character.

Business Entities

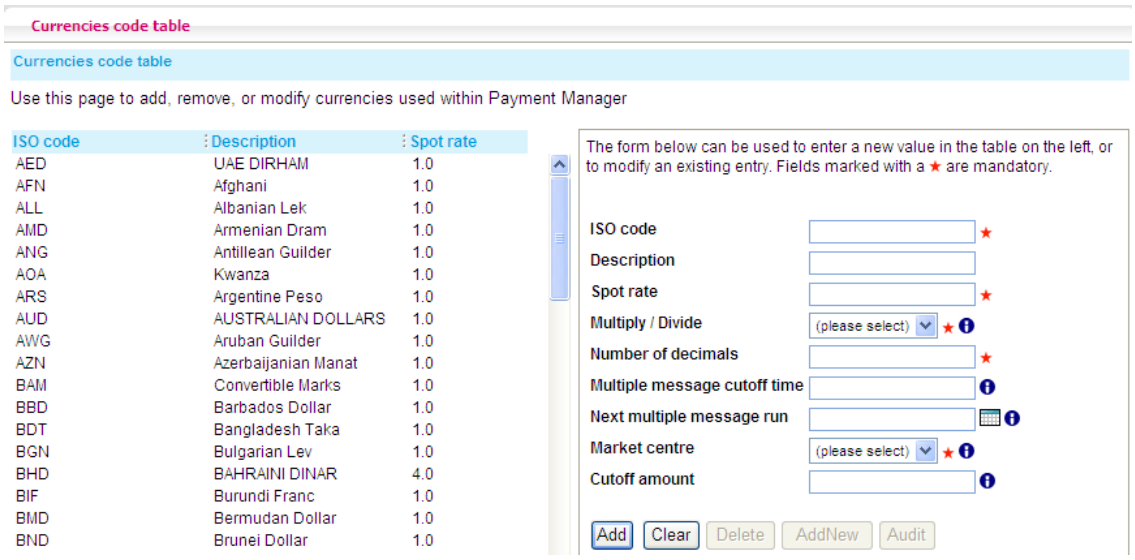
This table defines the business entities available within FusionBanking Payment Manager and is used to group messages into lines of business.



Field	Description
Business Entity	This is the unique, meaningful name for the business entity.
Description	Narrative describing the business entity.

Currencies

This table defines the currencies available within FusionBanking Payment Manager. It comes pre-loaded with ISO currencies.



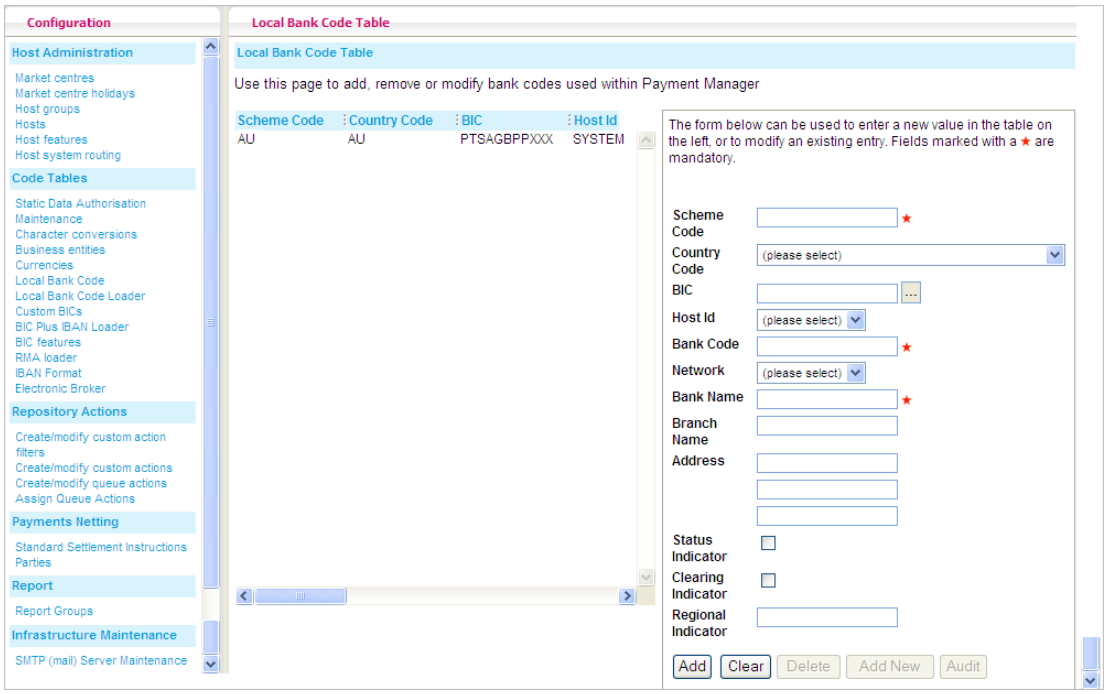
Field	Description
ISO code	The ISO code for the currency.
Description	Enter a meaningful name for the currency.
Spot Rate	The current conversion rate between the base currency and this currency. (To change the base currency, see The System Control Data Menu.
Multiply/Divide	Indicates whether the currency will be multiplied or divided by the spot rate to convert it to the base currency.
Number of Decimals	The number of decimal places used with the currency when an amount is formatted for screen display, e.g., US Dollars - 2 places, so 2 is entered.
Multiple Message Cut off Time	For multiple message processing, the time when all qualified payment and receive messages will be pooled into multiples regardless of whether the maximum limits (i.e., no of components or size) are reached. The time entered must be in the 24-hour format (hh:mm). This is a mandatory field.
Next Multiple Message Run	Enter the date at which the cut off time processing for pooling multiple messages will be made effective.
Market Centre	Enter the market centre for which the timezone of the cut off time will be expressed in. This is to qualify the cut off time against the server time when all payment and receive messages will be sent. Entry is mandatory and is used in conjunction with the FusionBanking Payment Manager multiple message processing.
Cut Off Amount	This is used by the multiple message processing to limit the messages that can be pooled into a multiple message by accepting only those with amounts less than entered here. If no value is specified, then no amount checking is performed. This is an optional field.

Local Bank Code

This table allows you to add, remove or modify bank codes used within FusionBanking Payment Manager. These are specific codes for financial institutions within a country or institutions that are members of a local clearing scheme. These codes are searchable wherever the local bank code picker is displayed on a screen. See BIC/Local Bank Code Query Tools.

Switchable feature CORE000069 is provided to:

- Check that a local bank code received in a payment message is correct and currently valid for incoming and outgoing messages (or both)
- Identify a local bank code from a received SWIFT BIC
- Check that a received SWIFT BIC/local bank code pair matches correctly



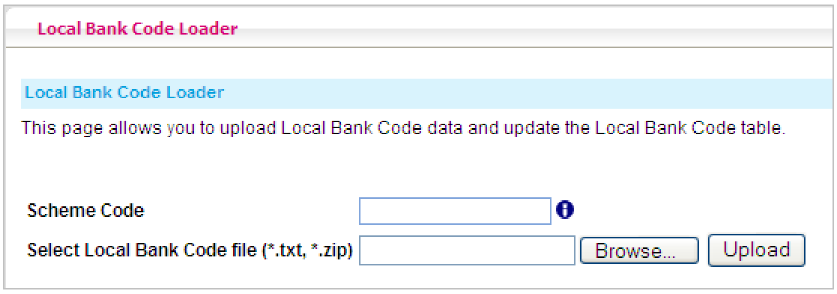
Field	Description
Scheme code	Enter the code for the specific local clearing or local network e.g. 'SC' to indicate the UK Domestic Sort Code.
Country code	Select the ISO country code for the particular country.
BIC	Select the SWIFT BIC code that corresponds to the local bank code.
Host ID	Select the host system.
Bank code	Enter a local bank code. Note that more than one local bank code can be stored for a country but you will need to add these as separate records.
Network	Select the payment network (or clearing and settlement mechanism).
Bank name	Enter the full name of the bank.
Address line 1	Enter the full address of the bank.
Status indicator	Check this box if you want to indicate in the local bank code picker whether a code has been blocked or not. (This will be displayed as Y or N).
Clearing indicator	Check this box if you want to indicate in the local bank code picker whether the bank is a clearing bank or not. (This will be displayed as Y or N).
Regional indicator	Where there are significant regional differences within a jurisdiction (e.g. USA), enter a regional code to identify the difference e.g. NY for New York.

Local Bank Code Loader

This screen allows you to upload a text file for the purpose of updating the local bank code table. The file must have the extention .txt but can be zipped (.zip). It should be comma or tab delimited. An example is shown below.

```
SCHEMECODE(2)   countryCode(2)  bic(11) hostId(10)      bankCode(11)     network(50)     bankName(50)
address1(50)    address2(50)    address3(50)    statusIndicator(1)       clearingIndicator(1)
regionalIndicator(20)
USUSCITIUS33XXXHost100    946464278  FedWire                                               CitiBank New York
                      Wall Street; New
Yorkaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
                    YNY
USUSCITIUS33XXXHost99     946464278  FedWire                                               CitiBank New York
                      Wall Street; New York
                                                      YNY
USUSCITIUS33XXXHost98     946464278  FedWire                                               CitiBank New York
                      Wall Street; New York
                                                      YNY
USUSCITIUS33XXXHost97     946464278  FedWire                                               CitiBank New York
                      Wall Street; New York
                                                      YNY
USUSCITIUS33XXXHost96     946464278  FedWire                                               CitiBank New York
                      Wall Street; New York
                                                      YNY
USUSCITIUS33XXXHost95     946464278  FedWire                                               CitiBank New York
                      Wall Street; New York
                                                      YNY
```

If mandatory fields are not present in the file, an error message will be displayed.

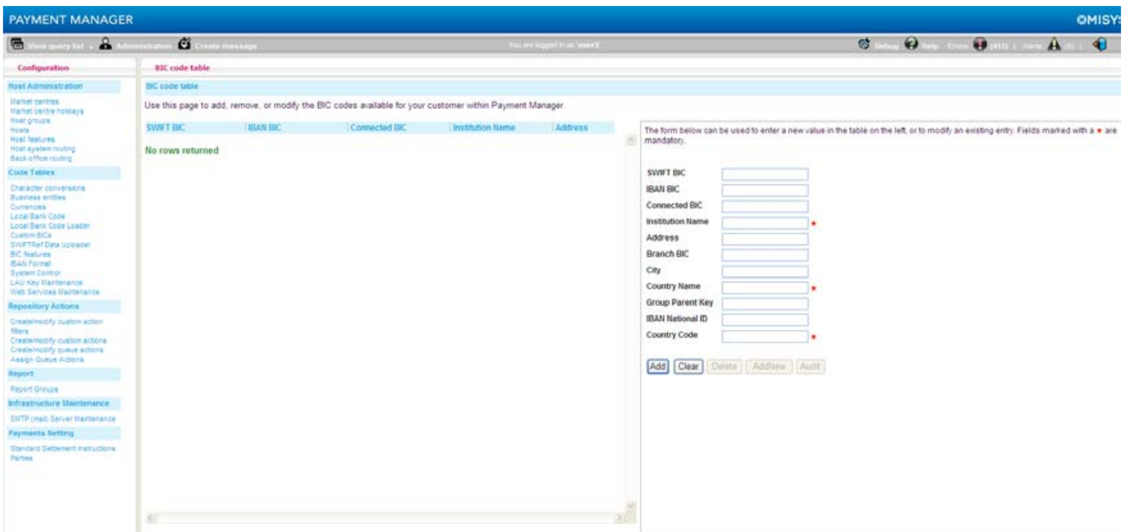


Field	Description
Scheme code	This field allows you to enter the code for the specific local clearing scheme or local network. You do not need to enter a value here if the .txt file contains the scheme code. If you enter a value here, any existing entry with the same value will be overridden.
Select local bank code file	Enter the path for the code file or search for it using the **Browse** button.

Click **Upload** to load the file. If the upload is successful, a message will be displayed.

Custom BICs

This table defines the additional custom BIC codes that can be used within FusionBanking Payment Manager. The SWIFTRef files can be uploaded via the SWIFTRef Data Uploader.



Enter the information in the fields, where applicable. For more information, refer to the relevant *SWIFT documentation*.

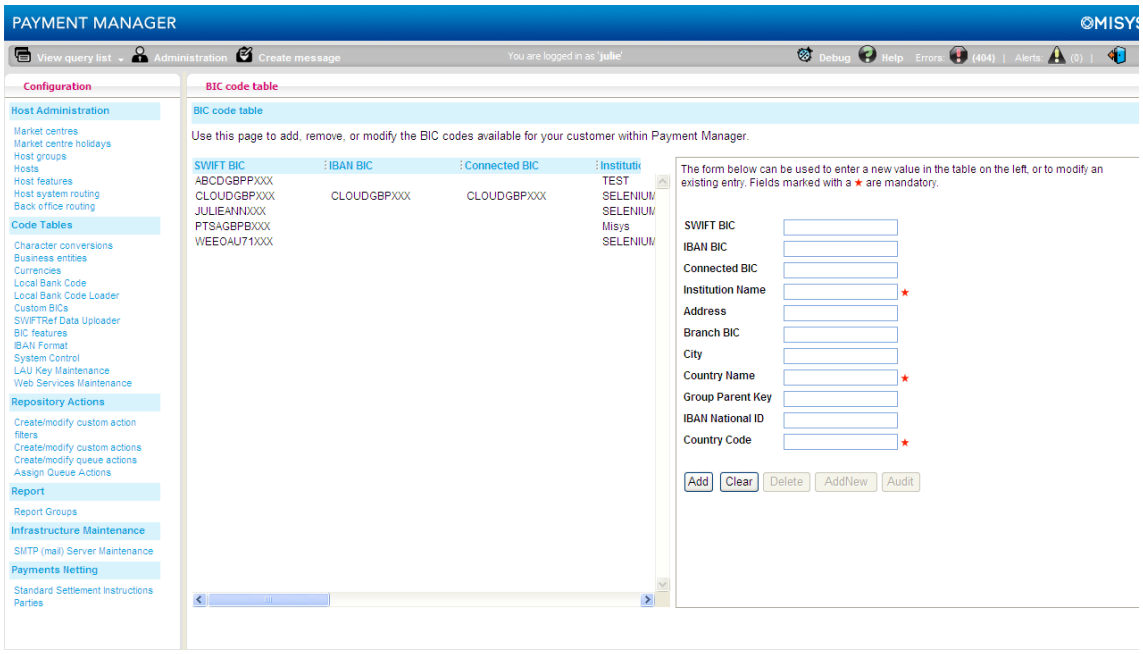
Field	Description
SWIFT BIC	Enter the full SWIFT BIC code
IBAN BIC	Enter the full SWIFT IBAN code
Connected BIC	Enter the Connected BIC
Institution Name	Enter the Institution Name
Address	Enter the address of the institution
Branch BIC	Enter the Branch BIC
City	Enter the city where the institution is located
Country Name	Enter the country where the institution is located
Group Parent Key	Enter the Group Parent Key
IBAN National ID	Enter the IBAN National ID
Country Code	Enter the Country Code

Only those BIC codes entered manually by the customer through this interface will be visible here. Any addresses added will be flagged as such and will be displayed in the left hand pane.

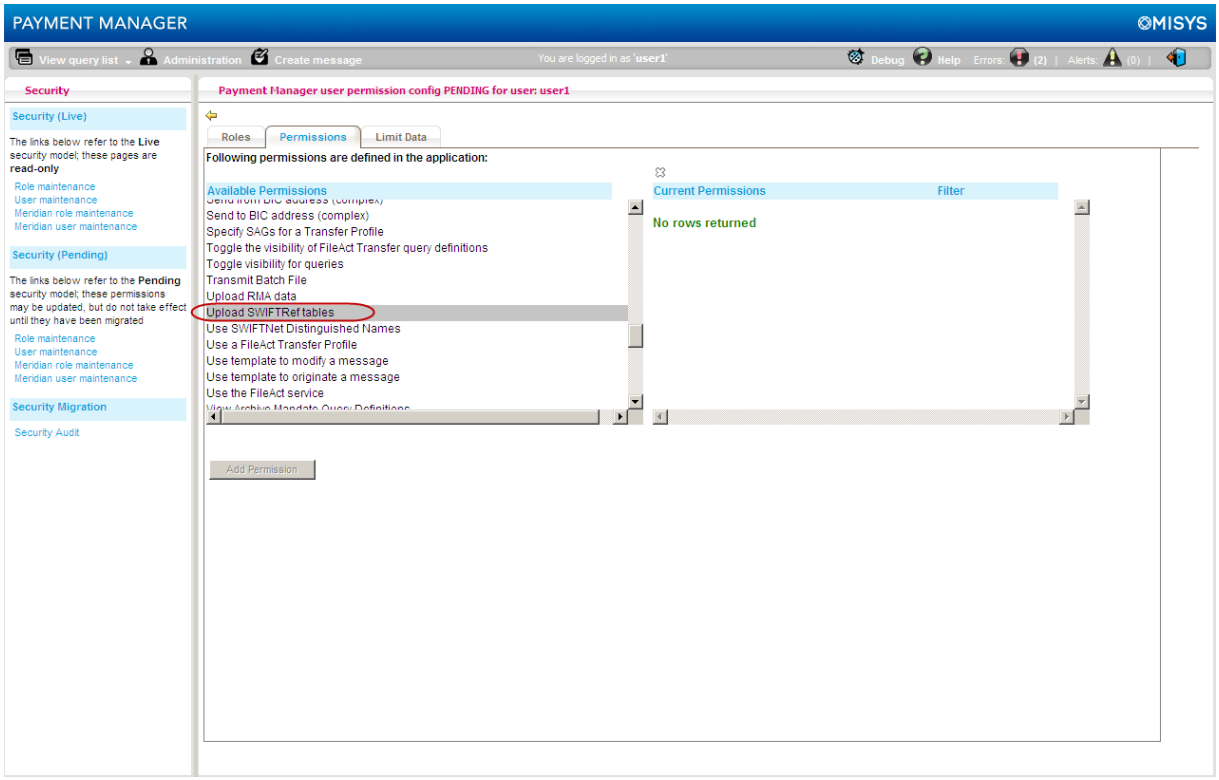
To search for and locate BICs across the whole SWIFTRef database, refer to the *FusionBanking Payment Manager User Guide*.

SWIFTRef Data Uploader

The SWIFTRef Data Uploader replaced the former BICPlusIBAN loader; it enables the FusionBanking Payment Manager to support the new Bank Directory Plus, IBAN Plus and IBANSTRUCTURE files. New mandatory fields are introduced that includes Institution Name, Country Name and Country Code.



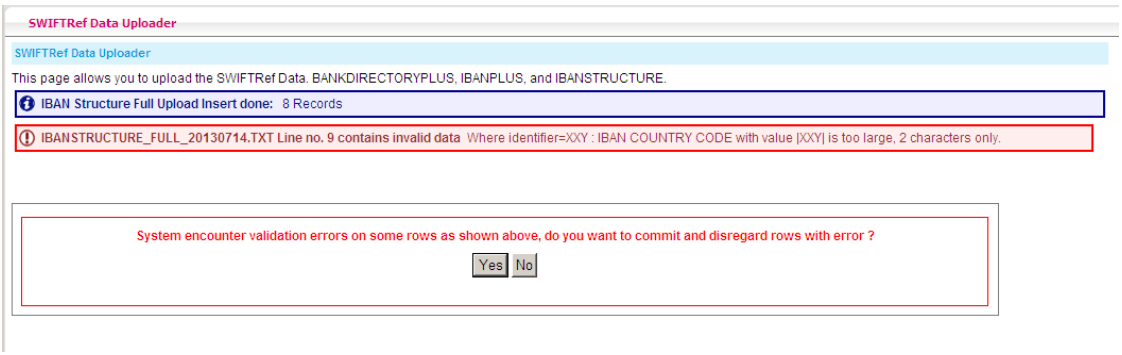
In **Administration > Security > Security (Pending) > User Maintenance**, the user must add the below **Upload SWIFTRef tables** permission and must be authorised, before being allowed to proceed to the upload screen.



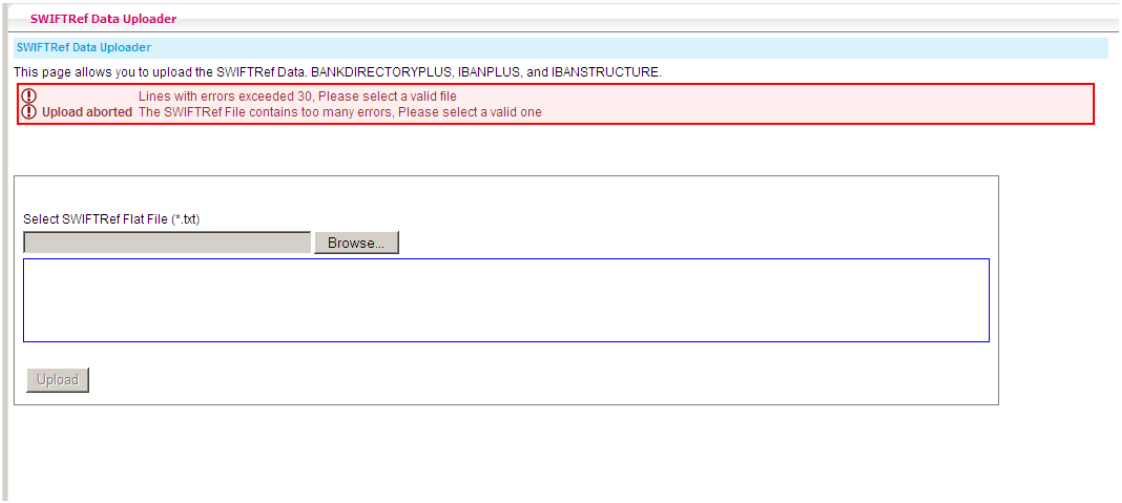
The Upload SWIFTRef permission can also be configured via Administration > Security > Security (Pending) > Role Maintenance.

To use this:

1. Click on **Browse** and select the location and name of the Bank Directory Plus/IBAN Plus/IBANSTRUCTURE files from the Choose File dialog box.
2. Click **Upload** to begin the loading process.
3. Before uploading, the system validates the data in the SWIFTRef file and indicates the line numbers of the records with errors.



However, if the number of error records exceeded 30 lines, the system will prompt an invalid file error and the SWIFTRef file will no longer be uploaded.



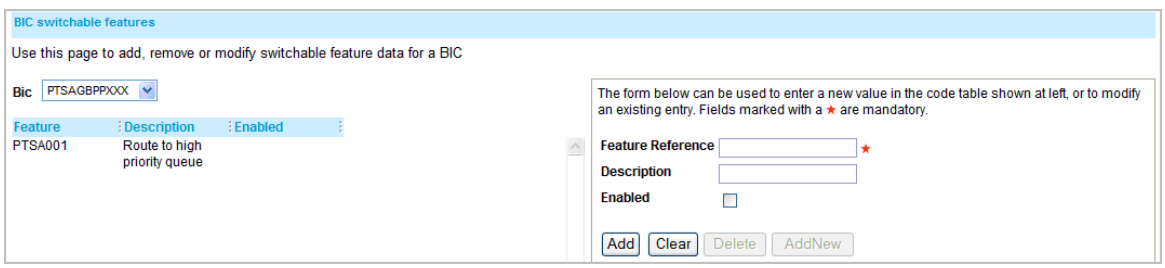
When a valid SWIFTRef file is selected, Upload button will be enabled and no error will be displayed. An error message will appear when an invalid file has been selected. There is an option to abort the process when there is an error. Examples of invalid files include:

- Older date
- Future Date (> 1 Month), (Type: DELTA)
- Invalid Filename

4. When loading the SWIFTRef tables, the following tasks will be performed:
   - New BICs, (those with modification flag 'A' in the SWIFTRef database) will be added to the existing BIC tables.
   - Updated BICs (those with modification flag 'M' in the SWIFTRef database) will be overwritten to the existing BIC table (including those that have been added manually from the Custom BIC option.
   - Deleted BICs (those with modification flag 'D' in the SWIFTRef database) are removed from the FusionBanking Payment Manager BIC table.
   - Unchanged BICs (those with modification flag 'U' in the SWIFTRef database) will be overwritten to the existing BIC table. Although the record is not changed, FusionBanking Payment Manager will update the corresponding record to ensure the latest information is loaded in case previous updates were not loaded.
   - Manually inserted BICs which do not have a corresponding record in the SWIFT version will remain untouched.

BIC Features

BIC Features are switchable features that are defined against BIC codes. This allows FusionBanking Payment Manager processing functions to be enabled and disabled on a BIC by BIC basis. An example of this is a switchable feature that controls the production of certain message types depending on whether the Sender BIC and the Receiver BIC are members of a certain message user groups.

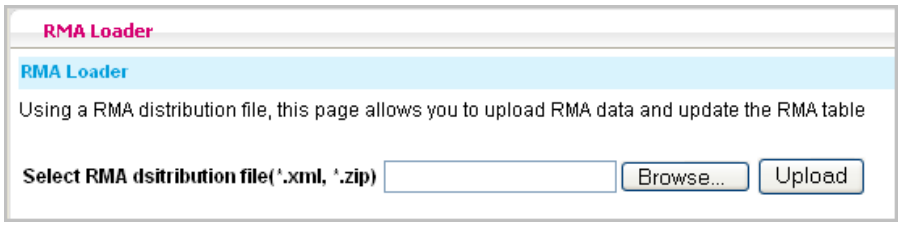


Field	Description
Feature Reference	A user defined reference code that is assigned to a BIC feature.
Description	A short description about the feature.
Enabled	Tick this box to enable the switchable BIC feature.

RMA Loader

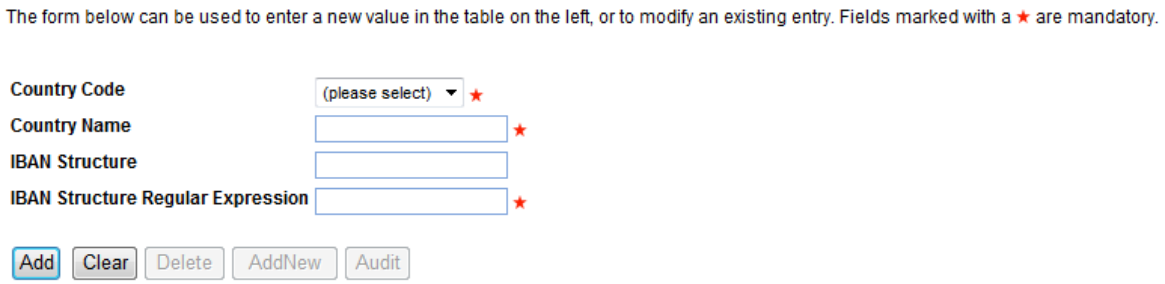
The Relationship Management Application (RMA) allows SWIFT users to manage their business relationships with their correspondents. This option allows you to upload RMA data which can be used in the FusionBanking Payment Manager database to validate messages against authorisations present in the database.

Select the file to upload by searching for it in the browser and click **Upload** to upload it.



IBAN Format

Enter the IBAN structure details in the fields provided.



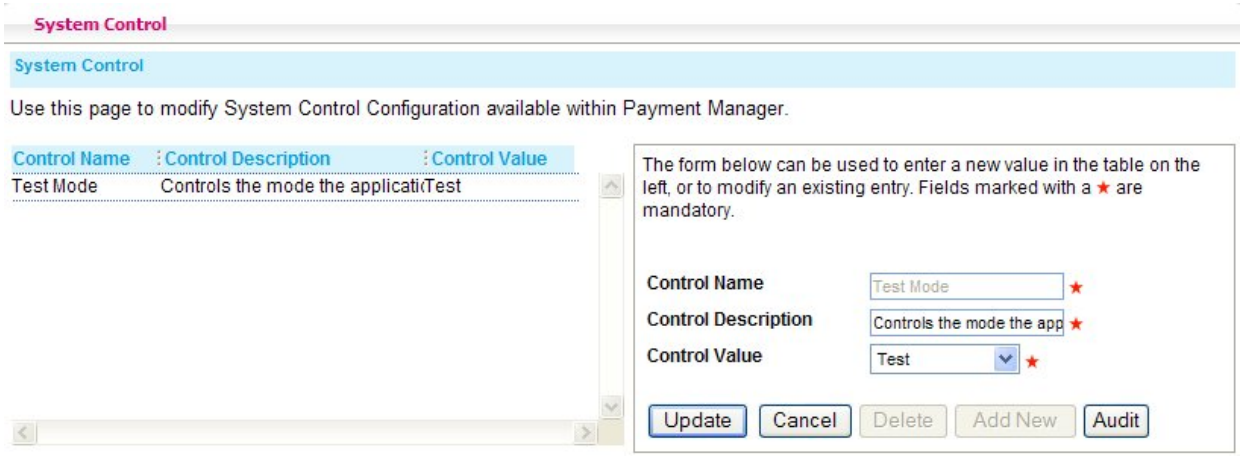
System Control

The System Control feature allows you to choose between two running modes of the application.

You can choose to run FusionBanking Payment Manager in either Production Mode, or in Test Mode. The Test Mode may prove very useful if you want to run tests for example, or for any other actions you want to perform on a different database in order not to alter the production one.

Note that the FusionBanking Payment Manager features available are the same in both modes.

To access the **System Control** feature, under **Administration**, choose **Configuration**, then in the left-hand pane, under **Code Tables**, select **System Control**.



In the screen above, you can modify the existing control to specify Test or Production mode, as described below:

Field	Description
Control Name	The name of the selected control.
Control Description	Enter a short description.
Control Value	Choose between Test or Production in the drop-down list.

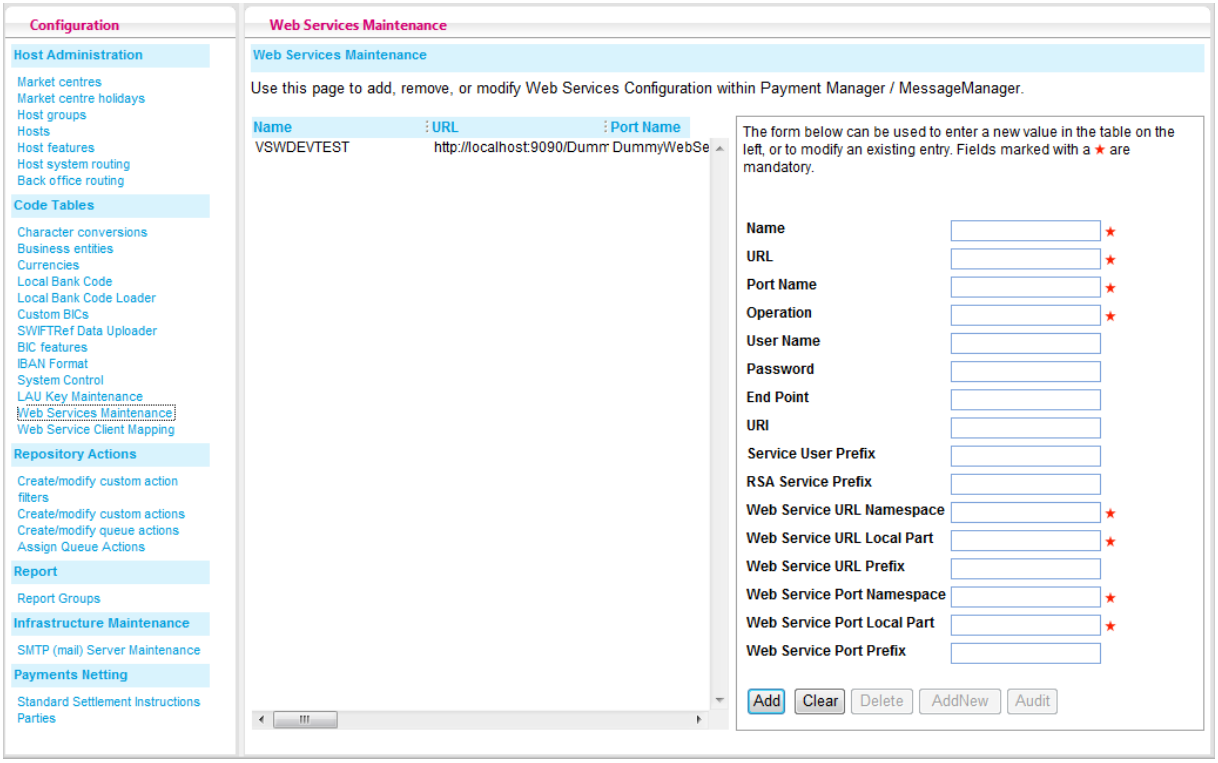
Click on **Update** to validate or on **Cancel** to ignore the changes.

After selecting one or the other mode, log out from the application, then log in again into the application. When in Test Mode, the Login screen and the main screen both display "TEST MODE".

If Test Mode is enabled, alerts will be raised with TEST MODE. Also, If a user or role has been set to "al" or email, the user will receive alerts through an email that will include "Test Mode" as part of the subject.

Web Services Maintenance

This is used to setup the web services that will be used for the credit mandate and debtor mandate data lookup.

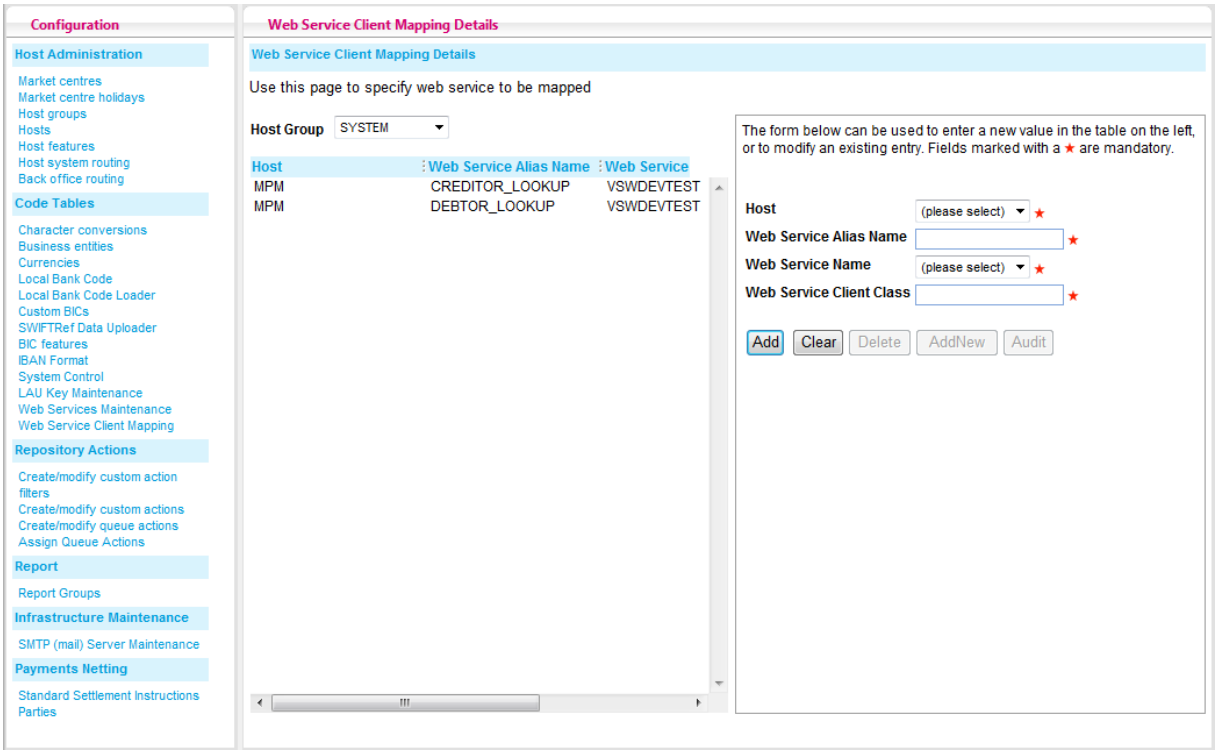


Field	Description
Name	The name of the Web Service
URL	The URL of the Web Service
Port Number	Each operation in a Web Service is normally bound to a port name
Operation	An operation that the Web Service does. (I.e. Validate RSA Passcode, etc.)
User Name	The user allowed to use the service
Password	Password for the service user
End Point	SOAP address provided by the Web Service
URI	Resource Identifier
Service User Prefix	Normally not needed, but due to the Web Service configuration by BF Midas, this was included.
RSA Service Prefix	Same as Service User Prefix
Web Service URL Namespace	URL namespace of the Web Service
Web Service URL Local Part	URL local part of the Web Service
Web Service URL Prefix	URL prefix of the Web Service
Web Service Port Namespace	Port namespace of the Web Service

Field	Description
Web Service Port Local Part	Port local part of the Web Service
Web Service Port Prefix	Port prefix of the Web Service

Web Service Client Mapping

The Web Service Client Mapping allows the users to add web services.



Field	Description
Host	Host Id
Web Service Alias Name	User-defined alias for the web service to be used by the system.
Web Service Name	The name of the Web Service to be used that is configured in Web Services Maintenance
Web Service Client Class	Implementing class of the Web Service.

Repository Actions

The **Repository Actions** menu contains options which allow you to set up custom actions for users.

FusionBanking Payment Manager supplies the following default custom actions which are assigned to the relevant queues:

- **Authorise** - for authorising payments

- **Create** - for creating messages via the Input / Repair module
- **Delete** - for deleting messages (routing messages to the Deleted node)
- **Force Post - for force posting**
- **Move to Repair** - for moving messages to the Repair node
- **NotDuplicate**
- **Release** - for releasing messages into the payment network
- **Repair** - for repairing messages via the Input / Repair module
- **Resubmit** - for resubmitting
- **Retry** - for retrying failed payments
- **Route** - for routing payments to a new node
- **Verify** - for verifying payments

Payment Release

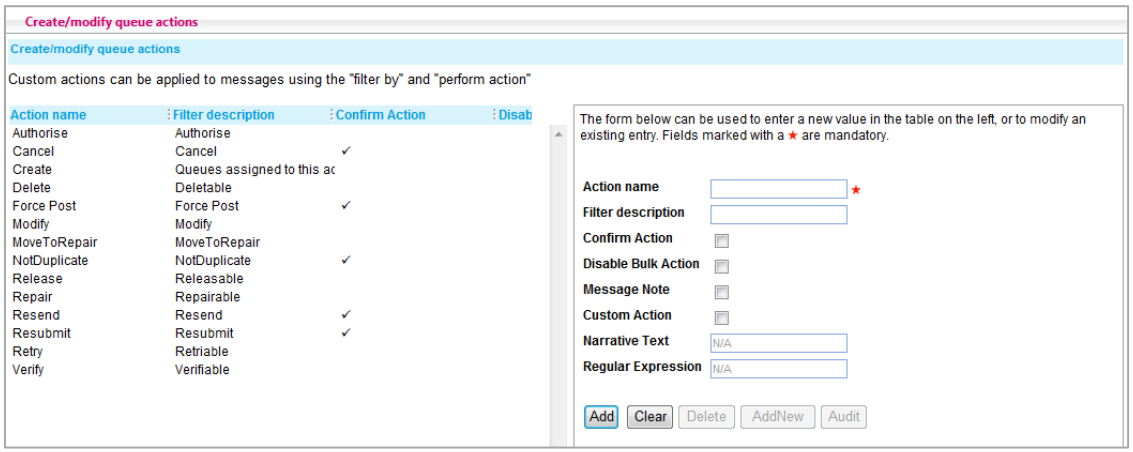
See Payment Release Maintenance and Settlement Cut-off Alerts.

Configuring Queue Actions

Queue actions can be customised for individual users to allow them to perform a specific action, such as authorise or route, on messages or a subset of those messages, residing on a particular node.

To configure custom actions, from the main menu select **Administration > Configuration > Create/modify queue actions**:

The following screen is displayed.



To add a new custom action, fill in the input form below and click **Add**.

Field	Description
Action name	Type in the name to identify the action. Entry must be unique (case sensitive).
Filter Description	Type in a description that will appear in the list of filters that can be applied to message query results.
Confirm Action	Select this option if a warning message is to be displayed when performing this queue action.
Disable Bulk Action	Checking this box disables the feature which allows a user to perform this action

	on **all** messages.
Message Note	Select this option if you want a message note tab, indicating that a message has a note attached to it, displayed in the expanded view pane of a message query. (This will be indicated as Y or N).
Custom Action	Check this box if the action is to be set up as a custom action.
Narrative Text	Enter any narrative to describe the custom action.

To delete an existing custom action, do the following:

1. Select the custom action to be deleted from the left hand list. The action will be populated in the right hand input form.
2. Click **Delete**. A confirmation message box will be displayed.
3. Click **OK** to delete the action or **Cancel** to go back. Attempting to delete a system action will result to an error displayed, informing that this action cannot be deleted.

To update an existing custom action:

1. Select the custom action to be modified from the left hand list. The action will be populated in the right hand input form.
2. Update the **Filter Description** field as necessary and click **Update** to apply the changes.

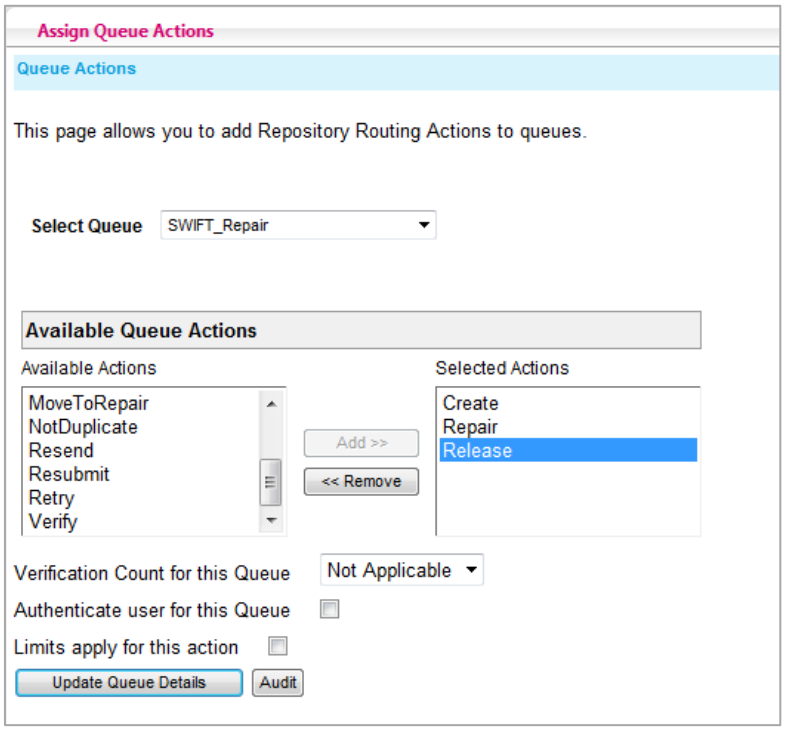
It is not possible to edit the **Action name**. To do this, the action must be deleted first and then a new one can be created with the intended **Action name**.

Assigning Custom Actions to Queues

Once a custom action has been created, it needs to be assigned to the relevant queues within the FusionBanking Payment Manager project. The queues that will be assigned these actions are those queues upon which other users can perform that action. For example, the **Delete** action (system supplied) may be assigned to several queues from where users can place messages that are not intended to go out to the network.

To assign custom actions to queues, from the main menu select **Administration > Configuration > Assign queue actions**.

The following screen is loaded:



To assign a custom action to a queue:

1. Select the queue the custom action/s will be assigned to. The available and assigned actions for that queue will be displayed.
2. In the **Available Actions** list box, select the action/s to be assigned to the chosen queue and click **Add >>**. The action will appear in the **Selected Actions** list box.

To remove a custom action from a queue:

1. Select the queue for which the custom action/s will be unassigned from.
2. In the **Selected Actions** list box, select the action/s and click **Remove**.

The Verification Count and Authentication features are described below. Click **Update Queue Details** to apply the changes.

If you want limits to apply to this action, check the **Limits apply for this action** box. For more information on setting limits, see Assigning Limits to Roles and Users.

Verification Count

The field **Verification count on this Queue** is used to control the number of verifications that can be done on a Verify action and any user-defined actions as part of the Four Eyes Verification functionality. The field provides the options: **Not applicable, 2-eyes, 4-eyes and 6-eyes** which represent the number of times the messages on the selected queue will need to be verified. Only one action can have a verification count associated with it for a selected queue. An action with a non zero action count is displayed in blue. Assigning an action count to additional queue action results in a warning message being displayed. If the user chooses to continue, the new action is displayed in blue and any action previously marked in blue will have its action count reset to 0 and will be displayed as normal.

If **2-eyes** is selected this means that when the action is chosen, the AuthoriserID check will be performed. So, an Action with **2-eyes** on one node when combined with a **2-eyes** Action on another node, will give the **4-eyes** verification required.

2 -eyes verification is a means of achieving n eyes verification by chaining queues. Each time a user performs an action with 2 eyes on one queue, the AuthoriserID field of the message(s) is updated with the user and the message(s) is/are moved to a downstream queue. A different user is required to perform the same action on the downstream node, thus achieving 4 eyes verification. This approach can be extended to achieve the desired number of verifications.

If **4-eyes** (or **6-eyes**) is selected, the AuthoriserID check will need to be performed 2 (or 3) times before the message is released from the current node.

The Filter icon allows you to display a subset of query results that match the action that was selected on the filter dropdown. When an action has been linked to 2-eyes, 4-eyes or 6-eyes verification count, and that action is selected on the filter dropdown, the system will check the value of ActionCount assigned to that specific action. If the ActionCount is 0 (zero) the system will behave normally, just filtering the messages that are on the queue on which the filter is linked to. Otherwise, if ActionCount is different from 0, the system will only show the messages that are on the queue, which the filter is linked to and which doesnt have the current user (running the filter) contained in the AuthoriserID field.

When an action has an ActionCount different from zero, the system will need to read the number of verifications that are stored on the database for the current queue and how many users have verified this message. This information will be updated on the message object, before the transmit message method in BankFusion Meridian is called.

When the user submits a manually created / repaired / modified message such that the message is persisted and then routed, the User Id that performed this action will be persisted as the first authoriser in the message object. This implies that if the message has been authorised previously, these values will be cleared from the message object – the process is effectively being re-started. Note, the audit trail of previous authorisations on the message will not be lost.

This functionality is also linked into the Input & Repair mechanism within FusionBanking Payment Manager in that if a message is created, modified or repaired, the User Id performing this action will be set as the first verifying user in the process.

Authenticating Actions

The Authenticate Action feature allows you to set up user authentication for business critical message actions such as validation and authorisation. Authentication forces the user performing the action to retype their FusionBanking Payment Manager login password and can be performed on a single message or batch of messages. For users with LDAP security setup, if the entered password is correct, the message will be routed and a success message will be shown. If the password is incorrect, the message will not be routed and an error message will be shown. For users with a non-security set-up, if the entered password is either correct or incorrect, the message will be routed.

To set the Authenticate Action feature on a queue, check the **Authenticate user for this Queue** box.

Report

See Importing Jasper Reports.

Infrastructure Maintenance

Where a user is required to receive email payment alerts, their SMTP (mail) server details need to be entered in this screen. See Setting up the Alert Notification Method.

The Security Menu

The FusionBanking Payment Manager Security function allows a security administrator to configure the messages and functions available to individual users. It provides role-based access control on various resources within the system. The following concepts are used to describe this facility.

Roles, users and permissions

The Payment Manager security model is role-based. As a member of a role, a user automatically inherits all the rights assigned with the role, though additional rights may be granted. A role is

associated with one or more permissions, essentially activities (e.g., create, modify, view, etc) applied over a 'resource' (e.g. a message, a message query, a template, etc.).

Complex permissions are permissions that can be filtered in order to restrict the availability of a function to a user. For example, when the "Originate a message" permission is attached with a filter condition "Type is equal to MT202", the user is allowed to create messages but is restricted only to message type MT202. When no restriction is set, the user is allowed to create all message types that have been set to allow input/repair capability in the FusionBanking Payment Manager project.

Security roles

There are three built in security roles that are provided as part of the installation of FusionBanking Payment Manager Security Administrator, Security Officer and Security Authoriser.

The Security Administrator role can assign Security Officer and Security Authoriser roles to users and can also authorise those changes to the security profiles. Security Administrators can either assign the Security Officer role or the Security Administrator role but not both to the same user. This user will not be seen as a day to day user of FusionBanking Payment Manager and will not have access to any functionality other than the security GUI. They will not be able to assign permissions to themselves which would allow them to view messages etc. This role is therefore an administrative role that needs to be used only occasionally to set up Security Officers and Security Authorisers whose job it is to set up relevant security profiles within FusionBanking Payment Manager.

The Security Officer assigns roles and permissions to users from permitted offices etc. and is considered the principal user of the security system. They are not able to do the following:

- Assign permissions and/or roles to themselves.
- Assign the Security Officer, Security Authoriser or Security Administrator role.
- Authorise changes to the Security Profiles

The Security Authoriser authorises changes to the Security Profile made by Security Administrators (although they can authorise as well) and Security Officers. This model prevents Security Officers from being able to authorise their own changes to security profiles. Security Authorisers can also choose to rollback changes to the Security Profile since the last time changes were authorised. To summarise, Security Authorisers can only authorise/rollback changes to security profiles, they cannot do anything else within the Security GUI.

Security Permissions

The following table describes the general permissions available in FusionBanking Payment Manager and the functions affected. Permissions specific to a particular function, for example direct debit mandates, are detailed in the relevant section.

Permission	Complex	Permission Description	Functions affected
Log in to Payment Manager	No	Permission required to log into the Payment Manager system.	User Log in
Select visible host groups for user	Yes	Users will only be able to view messages that originated from or are destined to host groups to which they have been given access. Complex permission criteria: Specify the host groups that a user can access. If no filters are specified, the user is permitted access to all host groups defined in the system.	Availability of the host group in the following trails: **View Query List** > Host group dropdown **Archive Query List** > Host group dropdown **End of Day Query List** > Host group dropdown

Permission	Complex	Permission Description	Functions affected
Define which messages are visible	Yes	Limit the messages that a user is allowed to view. Complex permission criteria: The permission can be filtered on message properties. This conditions logically AND'ed to the query conditions, which has the effect of narrowing down the results returned by a message query.	Availability of the message in the following trail : **View Query List** >running a query Archive Query List >running a query **End of Day Query** List > running a query
Originate a message	Yes	Create a new message without the use of a template – i.e. all fields available for input. Complex permission criteria: Specify the message types that the user can create.	Availability of the message type when creating a message using the following trail: **Create Message** >Any Messages
Use template to originate a message	No	Originate a new message using a message template. Users can only select a template defined for a role of which they are a member of.	Availability of the creation method "template" in the following trail: **Create Message** > Any Messages
Modify a message	Yes	Modify an existing message without the use of a template – i.e. all fields available. Complex permission criteria: specify the messages that the user can modify.	Availability of 'free form' type of modification in the message modification dropdown when selecting the edit icon in the following trail : **View Query List** > run a query > select a message on the query result pane
Use template to modify a message	Yes	Modify an existing message using a Modification Template. Users can only select a template defined for a role of which they are a member. Complex permission criteria: The permission can be filtered on message properties to limit the messages that the user can modify.	Availability of a message template in the message modification dropdown when selecting the edit icon in the following trail : **View Query List** > run a query > select a message on the query result pane. Note that in addition to the above, there are other factors that are checked when displaying a particular template in the message modification dropdown: The template must be in the same message type as the message currently being viewed. The user must be a member of the role that owns the template
Create manual message for HostID	Yes	Contains the hosts for which a user can create messages and templates.	The HostIDs displayed when inputting manual ACBS messages and templates.

Permission	Complex	Permission Description	Functions affected
Repair a message	Yes	Fix fields of host system-originated message that fails validation (all non-null fields that are not in error are locked). Complex permission: criteria can be specified to limit the messages the user can modify	Availability of the repair icon when viewing a message in the following trail: **View Query List** > run a query > select a message on query result pane The repair icon is activated when all of the following conditions are met : The current user must have a 'Repair a message' permission The message must reside in a queue that has been assigned the custom action 'Repair'. See Performing Custom Actions on Messages. The message must have existing validation errors.
Create MTn95	No	Create a Mtn95, MTn96 or MTn99 message	Availability of options MTn95, MTn96 and MTn99 from the Create Message dropdown on the menu task bar. Availability of the MTn95 icon when viewing a message in the following trail: **View Query List >** run a query > select a message on query result pane Availability of the MTn96 icon when viewing a relevant message in the following trail: **View Query List** > run a query > select a message on query result pane
Create message note	No	Write a note against a message.	Availability of the Notes input form to write a note against a message selected in the following trail: **View Query List** > run a query > select a message on query result pane > click on Notes tab on the detailed message pane.
Perform custom action	Yes	Assign custom actions to users that are allowed to perform them. Complex permission criteria can be specified to limit the custom actions that a user can perform. If no filters specified, the user is allowed to perform all custom actions defined in the system.	Availability of certain custom actions in the custom action dropdown when the custom action icon is selected in the following trail **View Query List** > run a query > select a message on query result pane.
Maintain message templates	No	Templates are linked to Roles. When a new template is saved, the role to which it is linked is a	Availability of the Template Editor option in the Administration dropdown on the

Permission	Complex	Permission Description	Functions affected
		mandatory attribute. The role must be one that the user preparing the template is a member of. In order to modify an existing template a user must have Maintain Message Templates permission and be a member of the role to which the template belongs.	menu task bar.
View/run queries	No	View message query definitions and run them	Availability of the View Query List option in the menu task bar.
Maintain queries	No	Create, edit message query definitions	Availability of the New Query icon within the query toolbar in the **View Query List** navigation pane. Availability of the Edit Query icon beside each query in the **View Query List** navigation pane.
Toggle visibility for message query	No	Make the query available to other users	Availability of the 'Visibility' checkbox in the input form when creating a new query in the following trail: **View Query List** > click on the New Query icon within the query toolbar
View/run archive queries	No	View archive query definitions and run them	Availability of the **Archive Query** option in the **View Query List** dropdown menu task bar.
Maintain archive queries	No	Create, edit archive query definitions	Availability of the New Query icon within the query toolbar in the **Archive Query** navigation pane. Availability of the Edit Query icon beside each query in the **Archive Query** navigation pane.
View/run End of day queries	No	View end of day query definitions and run them	Availability of the **End of Day Query** option in the **View Query List** dropdown menu task bar.
Maintain End of day queries	No	Create, end of day query definitions	Availability of the New Query icon within the query toolbar in the **End of Day Queries** navigation pane. Availability of the Edit Query icon beside each query in the **End of Day Queries** navigation pane.
View/run audit query	No	View audit query definitions and run them	Availability of the Audit queries within the View Query List navigation pane. Availability of Audit queries

Permission	Complex	Permission Description	Functions affected
			within the **Archive Queries** navigation pane.
Maintain audit query	No	Create, edit audit query definitions	Availability of the New Audit Query icon within the query toolbar in the **View Query List** navigation pane. Availability of the Edit Query icon beside each query in the **View Query List** navigation pane. Availability of the New Audit Query icon within the query toolbar in the **Archive Queries** navigation pane. Availability of the Edit Query icon beside each query in the **Archive Queries** navigation pane.
Limit visibility for audit records	Yes	Allow user to view audit records. Can be filtered by audit properties to limit the kind of audit records the user can view.	Availability of certain audit records in the following trail : **View Query List** > run an audit query **Archive Query List** > run an audit query
Send from BIC Address	Yes	Specify BIC addresses to send the messages from. If no filter is specified, the user can send messages to any destination	Ability to use certain BICs as Sender of the message created/modified from the following functions: **Create Message > Any Message** **Create Message > Mtn95** **Create Message > MTn96** **Create Message > MTn99** **View Query List > click on a query > modify a message** Note that if this permission is not granted, the user will not be able to proceed with any of the above functions.
Send To BIC Address	Yes	Specify BIC address to send the messages to. If no filter is specified, the user can send messages to any destination	Ability to use certain BICs as Destination of the message created/modified from the following functions **Create Message > Any Message** **Create Message > Mtn95** **Create Message > MTn96** **Create Message > MTn99** **View Query List > click on a query > modify a message**

Permission	Complex	Permission Description	Functions affected
Acknowledge errors	No	Mark error messages as acknowledged	Click on error icon in the menu task bar and acknowledge an error message.
Acknowledge alerts	No	Mark alert messages as acknowledged	Click on alert icon in the menu task bar and acknowledge an alert message.
View alerts	No	View received alerts that are of medium category	Controls availability of the error and alert icons in the menu task bar.
Raise alerts	No	Send another user an alert message	Availability of option **'Raise Alerts'** under the **Administration** dropdown menu.
Receive alerts	Yes	Allow payment alerts to be received by user on basis of host system and/or business entity	Availability of types of alert.
Configure system tables	Yes	Maintain static data tables	Availability of all options under this trail: **Administration > Configuration**
Use repository	No	A basic permission to allow FusionBanking Payment Manager users to access the project components in order to view, maintain and route messages. Note that this is a BankFusion Meridian-specific permission.	Use of repository.
Maintain Batch File query definitions	No	Allows a user to create, modify and delete query definitions	Creation of batch file query definitions.
View/use Batch File query definitions	No	Allows a user to view queries and query results	Viewing of batch file query definitions.
Configure System Control Data	Yes	Allows a user to configure system control data. See The System Control Data Menu.	Use of static data in routing processes.
View System Tables	Yes	Allows a user to view system tables.	
View System Table Audits	No	Allows a user to view system table audits.	
Authorise System Tables	Yes	Allows a user to authorise changes to static data tables.	Use of static data in routing processes.
View Message Templates	No	Allows a user to view message templates.	
Cancel Credit Transfer and Direct	Yes	Allows a user to cancel Credit Transfer and Direct Debit.	Performing manual cancellation returns

Permission	Complex	Permission Description	Functions affected
Debit			
Reject Credit Transfer and Direct Debit	Yes	Allows a user to reject Credit Transfer and Direct Debit.	Performing manual rejection returns
Return Credit Transfer and Direct Debit	Yes	Allows a user to return Credit Transfer and Direct Debit.	Performing manual returns

Minimum Permissions to Assign

All FusionBanking Payment Manager users, regardless of how wide or restricted their access rights are, should be granted a minimum number of permissions in order to get started with the system. These permissions should allow them to (1) log in to the system; (2) run messages queries, and (3) view messages. The basic permissions are:

- Log in to FusionBanking Payment Manager
- View/run queries
- Select visible host groups for user
- Define which messages are visible
- Use Repository

On top of the above permissions, other permissions or set of co-dependent permissions may be added to give them access to specific functions in the system. The following table will guide the Security Administrator or the Security Officer to assign the correct permissions for a specific function.

Resource	Activity	Minimum permission/s required
Alerts	Raising alerts	Basic Permissions, plus: Raise Alerts
	Viewing alerts	Basic Permissions, plus: View Alerts
	Acknowledging errors	Basic Permissions, plus: View Alerts Acknowledge errors
	Acknowledging alerts	Basic Permissions, plus: View Alerts Acknowledge alerts
Archive Query Definition	Viewing archive query list , or Viewing archive query definitions, or Viewing results returned by an archive query	Basic Permissions, plus: View/run archive query
	Creating a new archive query (non-system queries) or Modifying an existing archive query Deleting an existing archive query	Basic Permissions, plus : Maintain archive queries

Resource	Activity	Minimum permission/s required
	Creating system archive queries	Basic Permissions, plus: Maintain archive queries Toggle visibility for query
Audit records	Viewing audit records	Basic Permissions, plus: Limit visibility for audit records
Audit Query Definition	Creating a new audit query or Modifying an existing audit query	Basic Permissions, plus: Maintain audit query
End-of-Day Query Definition	Viewing end-of-day query list , or Viewing end-of-day query definitions, or Viewing results returned by an end-of-day query	Basic Permissions, plus: View/run end-of-day queries
	Creating a new end-of-day query or Modifying an existing end-of-day query Deleting an existing end-of-day query	Basic Permissions, plus : Maintain end-of-day queries
Message Query Definition	Viewing query list , or Viewing message query definitions, or Viewing results returned by a query	Basic Permissions
	Creating new query (non-system queries) or Modifying an existing query	Basic Permissions, plus : Maintain queries
	Creating system queries	Basic Permissions, plus: Maintain queries Toggle visibility for message query.
Message template	Creating message templates	Basic Permissions, plus Maintain message templates
Messages (non-common group)	Creating a message	Basic Permissions, plus Originate a message Send to BIC Address
	Creating a message via templates	Basic Permissions, plus Use Template to Originate a Message Send To BIC Address
	Modifying a message	Basic Permissions, plus Modify a message
	Modifying a message via templates	Basic Permissions, plus Use Template to Modify Message
	Repairing a message	Basic Permissions, plus

Resource	Activity	Minimum permission/s required
		Perform Custom Action and attach a filter Custom action is equal to Repair
	Deleting a message	Basic Permissions, plus Perform Custom Action and attach the filter 'Custom action is equal to Delete'
	Performing custom actions on a message	Basic Permissions, plus Perform Custom Action
	Attaching a note to a message	Basic permissions, plus: Create a note against a message
Message (common group)	Creating MTn95, MTn96 and MTn99 messages	Basic permissions, plus: Create MTn95 messages
System Tables	Maintaining system tables: • Market Centre • Market Centre holidays • Host Groups • Hosts • Host Features • Character Conversions • Business Entities • Currencies • BIC • Queue Actions • Assign Queue Actions	Basic Permissions, plus: Configure system tables

Adding users in LDAP

If the implementation of FusionBanking Payment Manager links to an LDAP server for its authentication model then any users set up within the Payment Manager Security function must also exist in the LDAP directory. FusionBanking Payment Manager supports interaction with the majority of LDAP compliant directories. For more information on adding users to LDAP directories, refer to the relevant LDAP documentation.

The Security Navigation Pane

The Security Navigation pane can be accessed by selecting **Administration > Security** from the main menu. The pane is divided into three submenus:

Security (Live)

The links under this submenu refer to the read-only view of the security profiles that are currently in operation (live). These functions are available to all security users.

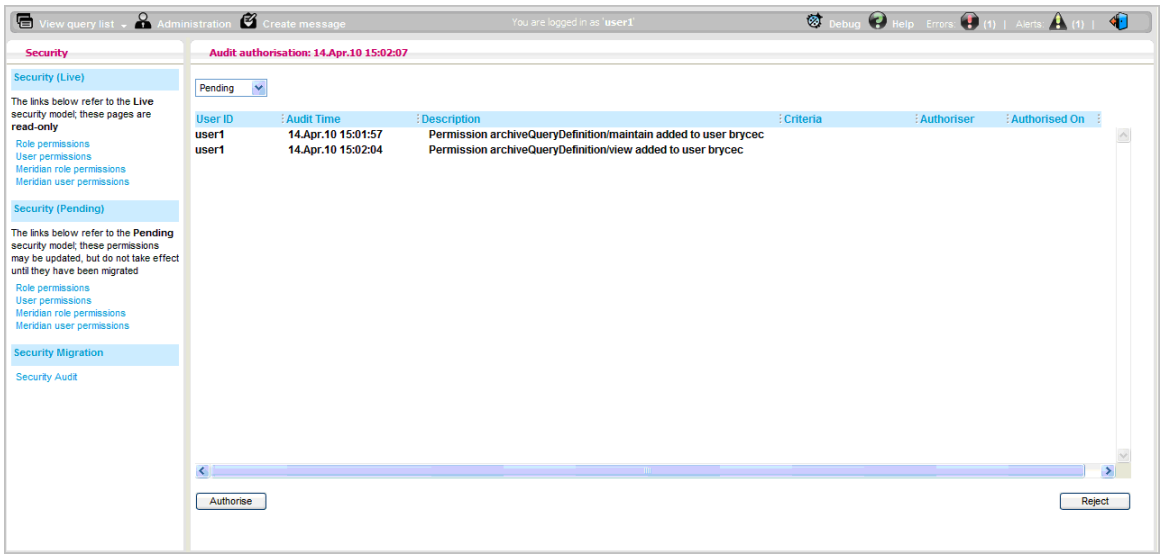
Security (Pending)

The links under this submenu refer to the administration of roles and user permissions. They offer the same screens as those of the "Live" links, the difference is that these are in read/write mode. Changes

made to security profiles may only be made "live" once these have been authorised by a Security Administrator or a Security Authoriser.

Security Migration

All security profile changes made under the Security (Pending) are recorded in the Security Audit link of this submenu.



Only Security Administrators or Security Authorisers can access this link and can either authorise or reject the changes made to security profiles. When the changes are accepted, they can then be viewed in the "Live" version. When rejected, the changes made in the "pending" version are rolled back.

Working with Roles

This section describes how to create and delete roles and add permissions and users to and remove them from roles. FusionBanking Payment Manager provides the following roles:

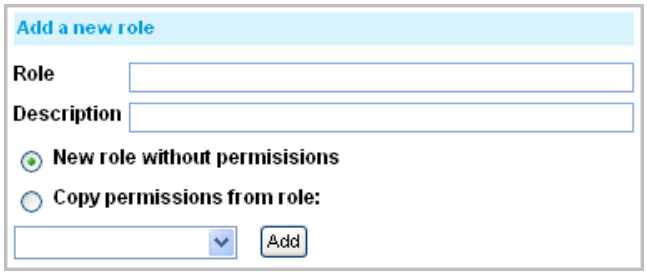
Role Name	Description
System	Application role.
Security Officer	Can make but not authorise, changes to the Security Profile.
Security Authoriser	Can authorise changes made to the Security Profile.
Security Administrator	Can modify / authorise changes made to the Security Profile. This role can create Security Officers and Authorisers.
Administrator	Can perform any action within the application. Cannot make changes to Security profiles.
Normal User	Can perform normal non-administrative tasks.
Developer	Developer (all permissions granted).
Meridian Controller	Role specific to the BankFusion Meridian Management Console.
Meridian User	Standard BankFusion Meridian API User.

Role Name	Description
Standard Meridian API User	Receiver of email alerts.

A user can be set up both as a verifier and as an authoriser. If these are required to be incompatible you should ensure that the same user is not set up for both roles.

To create a new role:

1. Select the Role maintenance link under the Security (Pending) submenu on the Security Navigation pane. The Role configuration pane displaying the roles defined in the system will be displayed on the right hand pane
2. Fill in the input form at the bottom of the pane. The new role will be created without permissions unless you want to copy existing permissions from another role. To do this, click **Copy permissions from role** and select the existing role from the dropdown. Click **Add** to save the new role.



Field	Description
Role	Enter a unique name for the role.
Description	Enter a narrative to describe the role.
New role without permission	Click this radio button to create the role without assigned permissions.
Copy permissions from role	Click this radio button to copy the permissions from an existing role. That role can be selected from the dropdown under this radio button.

To delete a role, select it and click **Delete** .

To assign permission to a role:

1. Select a role in the Roles grid and click **Edit** .
2. Click the **Permissions** tab. Two grids will be displayed. The Available Permissions grid displays all the permissions that are enrolled in the system. The Current Permissions grid displays all the permissions that are assigned to this role.
3. Select the permission to be added on the Available Permissions grid. If the permission is complex, the complex criteria form will appear in the space under the two grids. See Creating Complex Permissions for details on how to use this.
4. Click **Add Permission**. The permission will appear in the Current Permissions grid.

To remove permission from a role:

1. Select the permission from the **Current Permissions** grid.
2. Click the **Delete** icon located above the **Current Permissions** grid. The permission is then moved to the **Available Permissions** grid.

To assign a user to a role:

1. Create the user. See Working with Users.
2. Select a role in the Roles grid.
3. Click on the Users tab on the right of the Roles grid. Two grids will be displayed. The Available Users grid displays all the users that are enrolled in the system. The Current Users grid displays all the users that are assigned to this role.
4. On the Available Users grid, select users by checking the box against them then click **Add**. The selected users will be moved from the Available Users grid to the Current Users grid.

To remove a user from a role:

1. Repeat steps 1–3 of assigning a user to a role.
2. On the Current Users grid, select users by checking the box against them and click **Remove**.

Working with Users

This section describes how to add and delete users and assign roles to and remove roles from users.

To create a new user:

1. Select the User permissions link under the Security (Pending) submenu on the Security Navigation pane. The User Configuration pane will be displayed on the right hand pane. The following default users are supplied:
   - system - system
   - user1 - sample user
   - secadmin - sample security administrator
   - admin - sample administrator
   - shiva - sample BankFusion Meridian controller
2. Fill in the input form at the bottom of the Users grid and click **Add**. The new role will now appear on the Users grid.

Field	Description
Name	Enter a narrative to describe the user.
User ID	Enter a unique name for the user.
New user without roles	Click this radio button to create the user without assigned roles.
Copy roles from user	Click this radio button to copy the roles and permissions from an existing user. That user can be selected from the dropdown under this radio button.

To delete a user, select the user and click **Delete**  .

Assigning Roles to Users

To assign a role to a user:

1. Select the User permissions link under the Security (Pending) submenu on the Security Navigation pane. The User Configuration pane will be displayed on the right hand pane. On the left of this pane is the User grid which will display the available users in the system.
2. Select a user in the Users grid.
3. Click on the Roles tab on the right of the Users grid. Two grids will be displayed. The Available Roles grid displays all the Roles that are defined in the system. The Current Roles grid displays all the roles that are assigned to this User.

4. On the Available Roles grid, select the roles by checking the box against them then click **Add**. The selected users will be moved from the Available Roles grid to the Current Roles grid.

Deleting a Role from a User

To remove a role assigned to a user:

1. Select the User permissions link under the Security (Pending) submenu on the Security Navigation pane. The User Configuration pane will be displayed on the right hand pane. On the left of this pane is the Users grid which will display the available users in the system.
2. Select a user in the Users grid.
3. Click on the Roles tab on the right of the Users grid. Two grids will be presented. The Available Roles grid displays all the users that are enrolled in the system. The Current Roles grid displays all the roles that are assigned to this role.
4. On the Current Users grid, select users by checking the box against them then click **Remove**.

Authorising Security Changes

Once the security changes have been made, they will need to be authorised before the changes could take effect. Only users with Security Administrator or Security Authoriser role will be able to perform this.

To authorise security changes:

Select the Security Audit link under the Security Migration submenu from the Security Navigation pane. All the security audit changes since the last authorisation (pending changes) will be shown in the audit grid on the right hand pane.

The audit grid contains the following information:

- User ID - The identification of the user responsible for the change.
- Audit time - The date and time when the change took place.
- Description - A narrative text describing the security change.
- Criteria - If the change involves a complex permission, this will show any filter conditions that have been added attached to or removed from the permission.
- Authoriser - The identification of the user who authorised this security change
- Authorised On - The date when the security change was authorised

Click **Authorise** to accept the changes or **Reject** to discard them.

Once the changes have been authorised, an affected user who is currently logged in will have to log out then log in again before the new privileges/restrictions can take effect.

As part of the authorisation process, it is possible to view the security audit history which may help decide whether to accept the current security changes or not. The Category dropdown located above the grid contains the following selections that control the type of audit changes that will be displayed:

- Pending - Only security changes since the last authorisation will be displayed. This is the default value.
- Authorised - All authorised security changes will be displayed
- Rejected - All rejected security changes will be displayed.
- All - All pending, authorised and rejected security changes will be displayed

Creating Complex Permissions

Filters may be attached to User or Role permissions that are tagged as complex permissions. When complex permissions are selected on the Available or Current Permissions grid of the User or Role

permission's Permission tab, the Complex Permission Builder appears at the bottom of these two grids. Fill in the input form as follows:

Field	Description
Show records where	Use one of the following clauses to determine how to combine different conditions defined in the query. *All of the following conditions are true* Only messages that pass all the conditions will be included in the query. *At least one of the following conditions is true* A message needs only to pass one of the conditions to be included in the query result. *At least one of the following conditions is false* A message needs only to fail one of the conditions to be included in the query result. *None of the following conditions are true* Only message that fail all of the conditions will be included in the query result.
Conditions	An expression composed of two operands evaluated by an operator. The left-hand-side operand of a condition is the property to filter the complex permission. For example, the Select Visible Host Groups for User permission is filterable by the property host group; the Define Which Messages are Visible permission is filterable by message properties; etc. The right-hand-side operand of a condition is a literal value (e.g. user-supplied text, date, or monetary value) or a simple function (e.g. nextWorkingDay). It may also contain multiple values (for 'between' style comparisons). Depending on the format of message property on the left hand-side of the expression, the right hand side may provide dropdowns or pickers for ease of input. For example, a date picker is provided for date-based properties, a currency dropdown is provided to pick out values for currency-based properties. The operator is the evaluator of the expression which may take one of the following forms: • Equality operator, e.g. "equals" "not equals" • Relational operator, e.g. "greater than", "less than", greater than or equals", "less than or equals" • Boolean functions, e.g., "between", "not between", "starts with", "ends with", "like" Examples of conditions are: • Message type equals MT202; • Value date is after nextWorkingDay; • Sender's Address starts with CHAS.

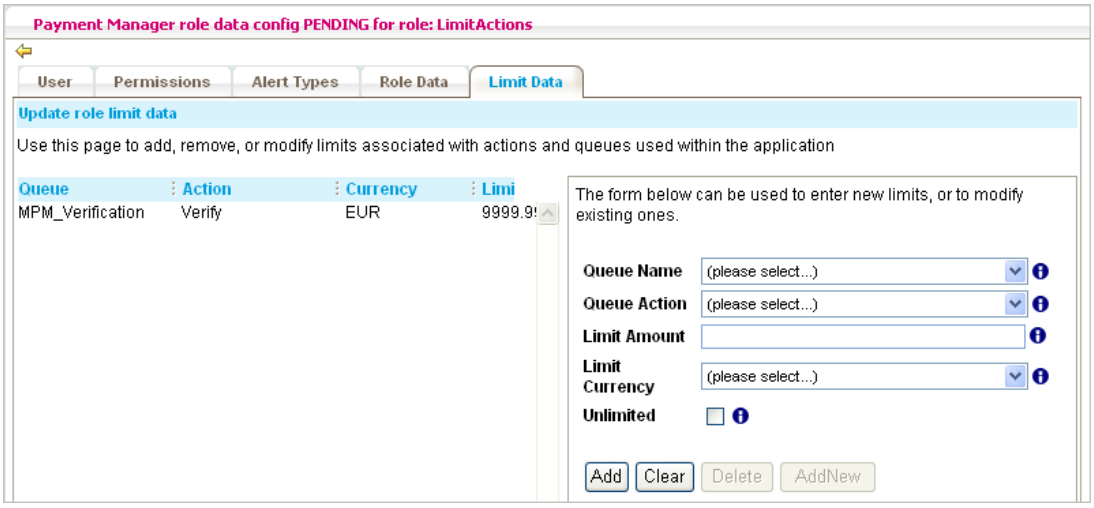
Assigning Limits to Roles and Users

Custom Queue Actions can be set up for requiring a limit check when they are assigned to a queue. Typical actions which you might want to set limits on could be, for example, authorisation and approval. The limits are defined through the security function by assigning them to individual roles and users. Different limits can be applied per role/user per action per queue. Limits defined for a user override those defined for a role.

To assign a limit to a role:

1. Select one of the Role Maintenance links under the Security (Pending) submenu on the Security Navigation pane. The Role Configuration pane displaying the roles defined in the system will be displayed on the right hand pane.

2. Click on a role and click **Edit** .
3. Click **Limit Data** tab.



4. Enter the details as described in the table below and click **Add**.

Field	Description
Queue Name	Select the queue the limit should apply to.
Queue Action	Select the action on the queue the limit should apply to
Limit Amount	Enter the limit amount.
Limit Currency	Select the currency of the limit
Unlimited	If you check this box no limit will apply

To assign a limit to a user, follow the procedure above, selecting one of the User Maintenance links and subsequent user attributes.

Payment Alerts

FusionBanking Payment Manager alerts are used to notify an end user of the system that a particular business condition has occurred in the workflow. They are role based, meaning that the user(s) belonging to a particular role will inherit the alerts assigned to that role. Notification of an alert can be via email, screen popup or both of these.

FusionBanking Payment Manager provides twenty three types of alert and these cannot be modified.

The table below lists the types of alert supplied by FusionBanking Payment Manager.

	Alert Type	Description	Error Code
1	Authorisation	Authorisation required	AuthorisationRequired
2	Invalid CSM	CSM validation failure	CSMValidation
3	Compliance Fail	Watch list check failure	ComplianceFailure
4	DuplicateFailure	Duplicate check failure	DuplicateFailure
5	Embargo	Embargo check failure	EmbargoFailure

	Alert Type	Description	Error Code
6	NWD check	A value today payment fails a non-working day check	Holiday/Validation
7	SWIFT Mapping	Technical mapping failure	Mapping Failure
8	Query Notification	Notification of query	QueryNotification
9	SWIFT Repair / authorisation	Payment that cannot be authorised sent for repair	RepairAuthorisation
10	Repair CSM	CSM validation failure sent for repair	RepairCSMValidation
11	SWIFT Repair / duplicate	Payment that failed duplicate check sent for repair	RepairDuplicate
12	SWIFT Repair / embargo	Payment that failed embargo check for sent repair	RepairEmbargo
13	SWIFT Repair / NWD check	Payment that failed NWD check sent for repair	RepairHoliday/Validation
14	SWIFT Repair / validation	SWIFT validation failure sent for repair	RepairValidation
15	SWIFT Repair / verification	Payment that cannot be verified sent for repair	RepairVerification
16	STP Rules failure	Generic STP failure warning	STPFailure
17	SWIFT ACK/NAK timeout	SWIFT ACK / NAK not received within a specified time	SWIFTACKNotReceived
18	SWIFT Negatively Acked	SWIFT responds to outgoing payment with a NAK	SWIFTNAKReceived
19	Missed SCO	Outgoing payment has missed settlement cut-off time	SettlementCutOffBreach
20	Settlement Cut Off	Payment is close to its settlement cut-off time	SettlementCutOffProximity
21	Value Before Today	Payment received with expired settlement date	SettlementDateFailure
22	SWIFT Validation	SWIFT Validation failure	ValidationFailure
23	Verification	SWIFT Verification required	VerificationRequired

You can edit the descriptions of these alerts by selecting **Administration > System Control Data > Error Codes** from the main menu.

To configure a payment alert you need to carry out the following four steps. These are described in detail in the following sub-sections.

1. Assign the relevant alert permissions to the user.
2. Assign the user to a suitable role. Where it is required to allow a user to receive alerts which they cannot view, this is achieved by ensuring the user does not have the View Alerts permission and then assigning them to a role which has the Receive Alerts, but not the View alerts, permission.
3. Assign the alert to the role.

4. Set up the method of alert notification. For email alerts this requires setting up the user's SMTP server details. See Infrastructure Maintenance.

Additional configuration is required for settlement cut-off alerts and this is described in detail in *Settlement Cut-off Alerts*.

Configuring Payment Alerts

To configure a payment alert you need to carry out the following four steps. These are described in detail in the following sub-sections.

1. Assign the relevant alert permissions to the user.
2. Assign the user to a suitable role. Where it is required to allow a user to receive alerts which they cannot view, this is achieved by ensuring the user does not have the View Alerts permission and then assigning them to a role which has the Receive Alerts, but not the View alerts, permission.
3. Assign the alert to the role.
4. Set up the method of alert notification. For email alerts this requires setting up the user's SMTP server details. See Infrastructure Maintenance.

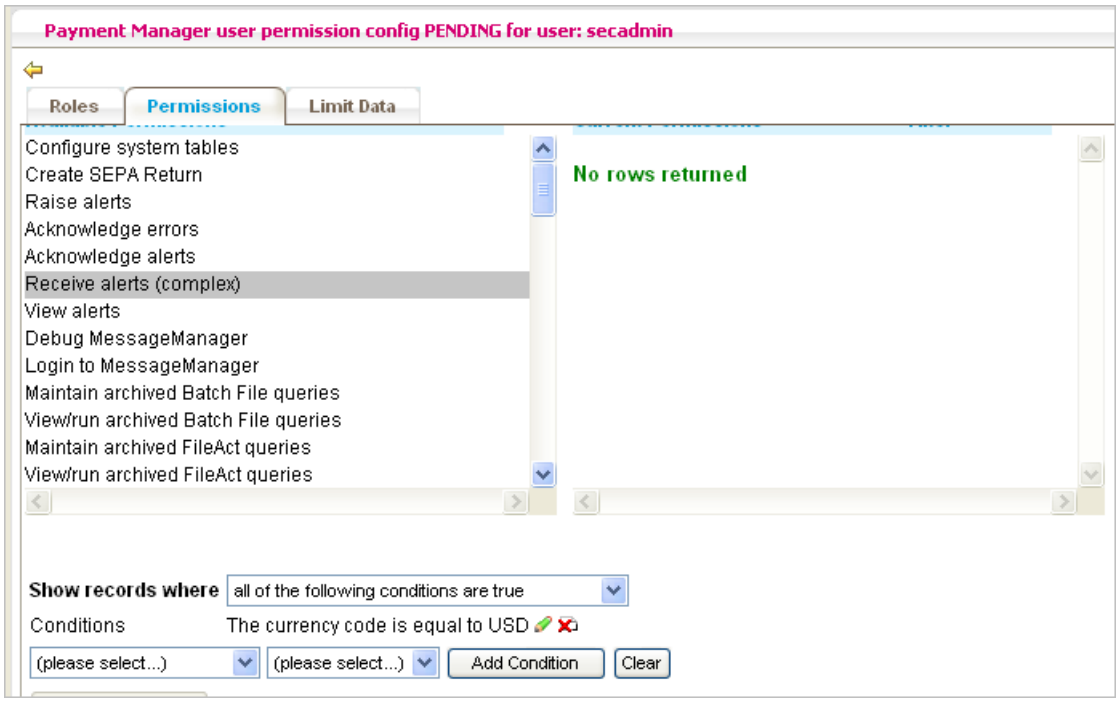
Additional configuration is required for settlement cut-off alerts and this is described in detail in *Settlement Cut-off Alerts*.

Alert Permissions

The following alert permissions are available:

Permission	Allows a user to
Receive alert	Receive alerts but not view them
View alert	View alerts

The Receive Alerts permission is a complex permission. Below is an example of how the permission can be filtered to, for example, allow a user to receive only alerts for payments in USD.



Another example might be to set up a role for a group of users to ensure they receive only alerts relevant to their particular source system or business entity. For example, for a group of Summit users you could set up the condition 'HostID equals SUMMIT', or something similar.

Assigning an Alert to a Role

Alerts can be configured to be received either via a screen popup or email, or both.

To assign an alert to a role:

1. Select one of the **Role Maintenance** links under the Security (Pending) submenu on the Security Navigation pane. The Role Configuration pane displaying the roles defined in the system will be displayed on the right hand pane.
2. Click on a role and click **Edit** .
3. Click on the **Alert Types** tab. Two grids will be displayed. The Available Alert Types grid displays all the alerts that are enrolled in the system. The Current Alert Types grid displays all the alerts that are assigned to this role.
4. On the Available Alert Types grid, select an alert by highlighting it and then click **Add**. The selected alert will be moved from the Available Alert Types grid to the Current Alert Types grid.

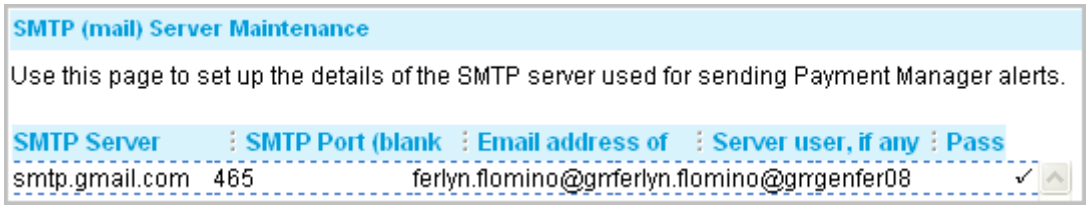
Setting up the Alert Notification Method

Alerts can be configured to be received either via a screen popup or email, or both.

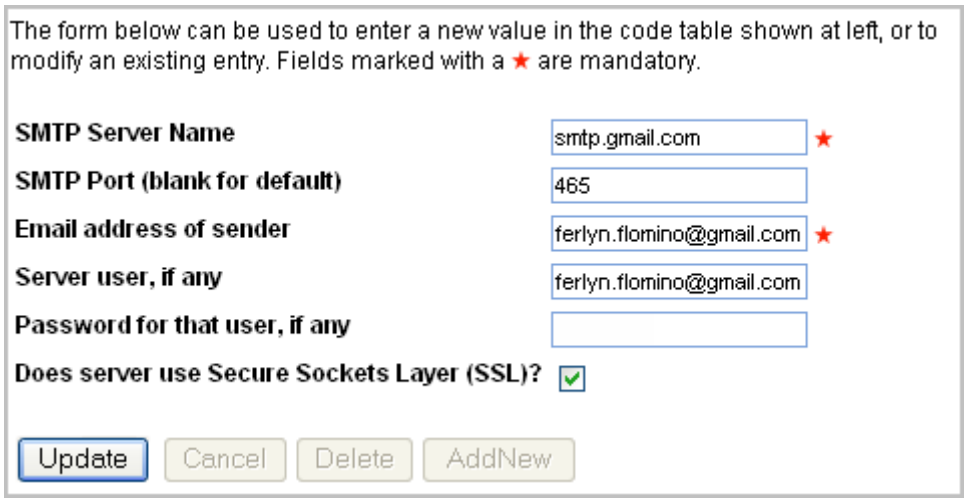
To configure email alerts for a user, you need to enter the user's SMTP server details as follows:

Select the menu option Administration > Configuration.

In the Infrastructure Maintenance menu click on SMTP (mail) Server Maintenance. Entries displayed in the left hand grid can be used to add new entries.



Click on an entry and enter the new details in the form provided.

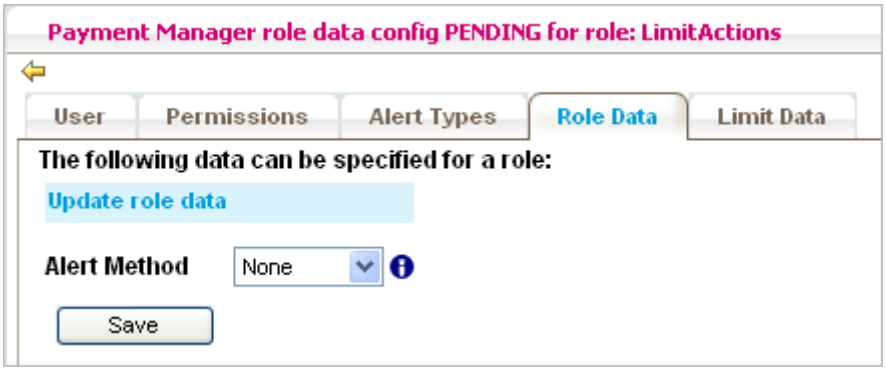


Click **Update** to save the details.

To set the alert notification method:

1. Select the role you want to set up as an alert receiver. See *Working with Roles and Working with Users*.
2. Click the **Role Data** tab.

3. In the Alert Method dropdown, select the chosen method of notification. If you select **All** the user will receive all methods of notification set up in the system.



Settlement Cut-off Alerts

A settlement cut-off alert is a particular type of payment alert used to inform a user that queued/pending payments which require manual intervention are approaching their settlement cut off time and can be released (See Payment Release Maintenance). It is possible to set criteria for the alert so that a user can be alerted when certain conditions are met. Such conditions could include a high value payment, a payment originating from or destined for a specific customer or a payment in a specific currency.

Setting up static data tables

Settlement cut-off alerts are set up using static data tables which will be used to trigger alerts. Alerts will be sent for those messages which match this data and also have a "Value Date" of "Today", a "Message Status" of "Not Sent" and a "Direction" of "Outgoing"

To set up static data tables:

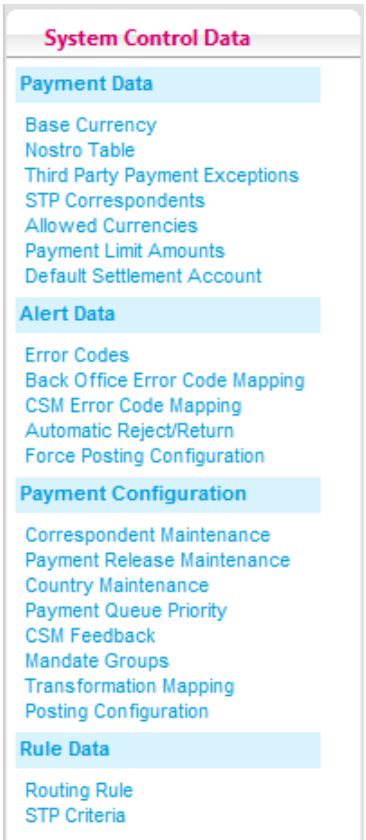
1. Select the menu option Administration > Configuration > Payment Configuration > Payment Release Maintenance.
2. Select the Host Group from the dropdown.
3. Enter information into the fields below and click Update to save the details.

Field	Description
Host ID	The ID of the system that originated the payment. A Host ID belongs to a specific Host Group.
Business category	The definition of the business category, e.g. FX High value.
Network	Outgoing payment format, e.g. SWIFT, SEPA, CHAPS.
Message type	SWIFT 103 / 202 / 205, SEPA CT, etc.
Currency	Settlement currency. You must specify a currency if a value is entered in Amount Greater Than field below.
Destination address	Correspondent bank, CSM.
Notice period	The number of days before the settlement date that a payment should be sent out (as directed by a correspondent or payment network). It relates to the amount of time the correspondent needs to process particular types of payment. See Payment Release Maintenance. A switchable feature Release Payment with Insufficient Notice Days allows you to release payments without applying the full notice days. For example, a payment with a value date of tomorrow where Notice period =2 can be released without applying the full 2 days' notice if the feature is turned on.

Field	Description
Release time	The time at which this payment can be released, or the "default time". See Payment Release Maintenance. For a payment with a value of today, if no value is entered here, the payment will be sent immediately.
Cut off time	The latest time that this payment can be safely released. See Payment Release Maintenance.
Cut off alert offset	Settlement cutoff alerts are raised on payment settlement days. This field allows you to raise settlement cut off alerts on a day previous to the settlement date. This might be useful where, for example, the settlement agent is in a country with a large time difference, such as Japan or Australia.
Cut off breach offset	When a Value Today payment is processed, and its Settlement Cut Off time has passed, the payment is queued and an alert is raised. Selecting the offset shifts this Settlement Cut Off check backwards by the number of days selected for the **Cut off alert offset**.
Interval time	The time between each alert.
Number of alerts	The total number of alerts to be generated.
Amount greater than	Enter a threshold above which payment release alerts will be sent.

In the example above where the user is alerted one hour before the cut-off time, if Cut off time = 23:00 hr, interval time = 15, and Number of alerts = 2, the user will receive alerts at 22:30 hr and 22:45 hr.

The System Control Data Menu

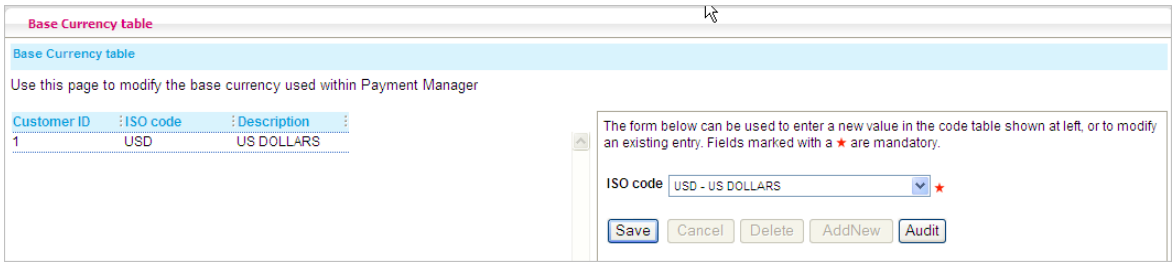


Payment Data

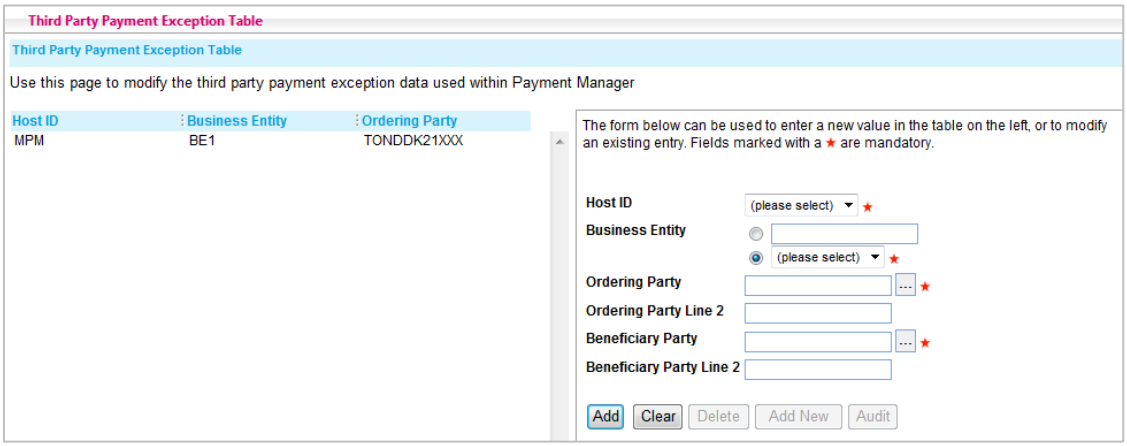
This menu contains a number of options for modifying static data associated with payments.

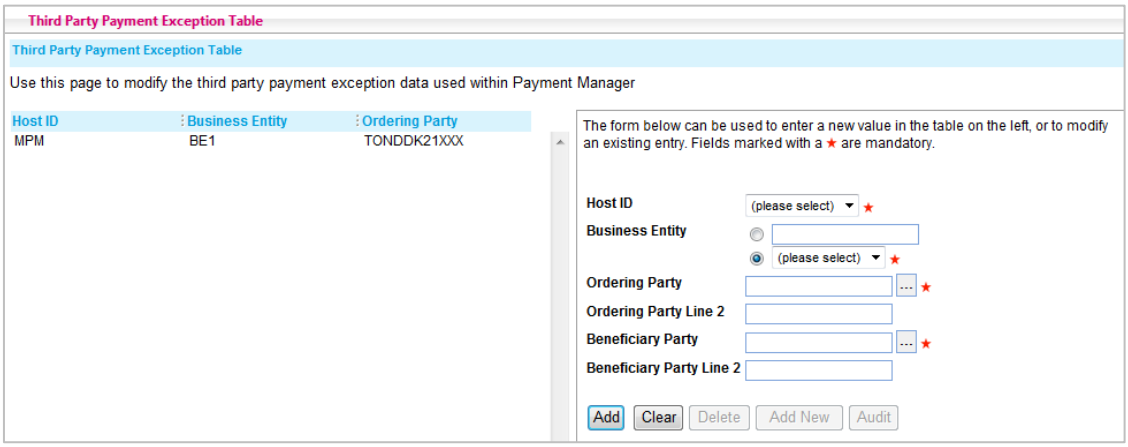
To change the system base currency:

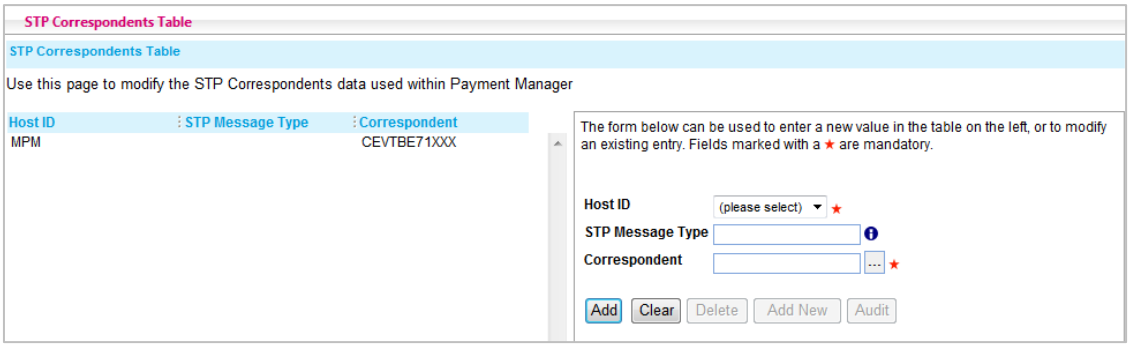
1. Click **Base Currency** and select the base currency in the Base Currency Table.
2. Select the new base currency from the **ISO code** dropdown and click **Save**.

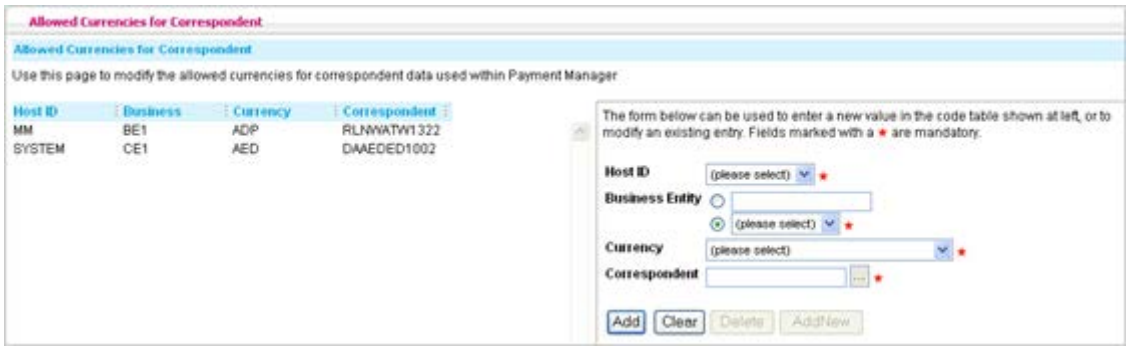


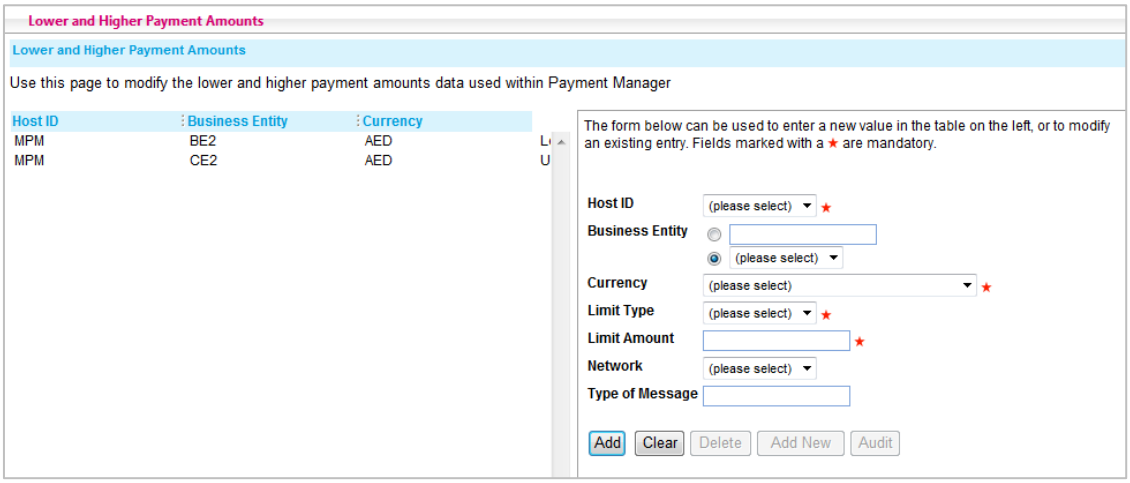
The payment control module supports a set of straight through processing rules which are applied to payment messages received from specific back office system/s. The following options are available for entering static data which is used where your bank has opted to apply such rules. An authorised user can create, modify or delete any value in any table and amendments will be effective immediately. Some Misys Professional Services support will be required in order to fully utilise the data in these tables in routing processes.









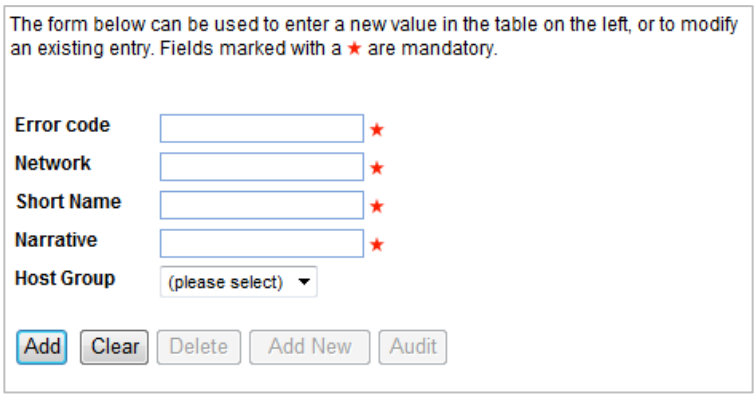


Alert Data

This option allows you to modify data associated with the payment alert error codes (see Payment Alerts).

Error Codes

This page has the Error Codes Tables for FusionBanking Payment Manager. This can also be used to modify an existing error code or add a new one through the screen below.



Field	Description
Error code	Enter a unique error code. This can be alpha-numeric.
Network	Enter the network where it will be used, e.g. QATCH.
Short Name	Enter a short name for the error code.
Narrative	Add a short description about the error code.

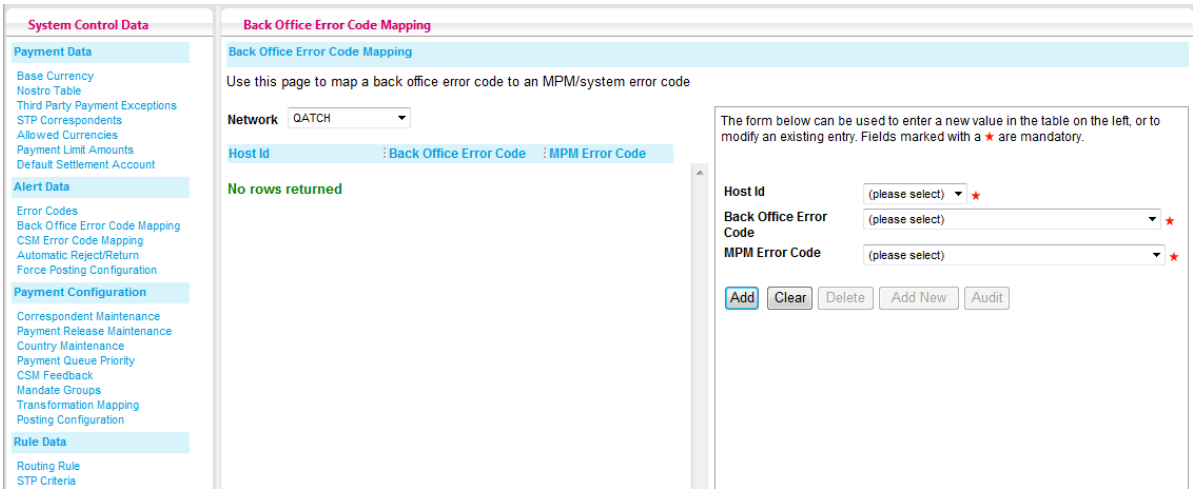
Back Office Error Code Mapping

FusionBanking Payment Manager allows the users to identify which back office error codes can produce automatic rejections / returns. This is done in three steps:

1. Map back office error code to MPM error code.
2. Map that mapped MPM error code to CSM error code.
3. Set that mapped CSM error code to automatic reject / return.

Back Office Error Code Mapping allows the user to map back office error codes to MPM error codes through the following steps:

1. Go to Administration > System Control Data > Back Office Error Code Mapping.
2. Select a Network.
3. Provide the values for the following fields.



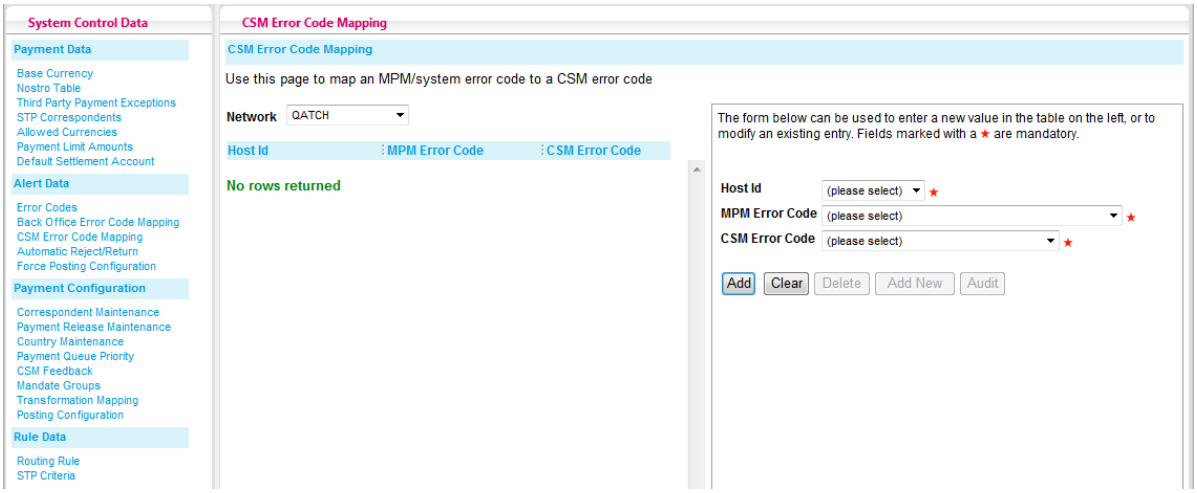
Field	Description
Host Id	Select Host Id.
Back Office Error Code	Select the specific back office error code that will be mapped eventually for automatic reject / return.
MPM Error Code	Select the preferred MPM error code equivalence from the list.

4. Click **Add**.

CSM Error Code Mapping

This screen is where the mapped back office code to MPM error code is being mapped to CSM error code.

1. Go to Administration > System Control Data > CSM Error Code Mapping,
2. Select the same Network used in section 4.5.2.3.
3. Provide the values for the following fields.



Field	Description
Host Id	Select the Host Id used in section 4.5.2.3.
MPM Error Code	Select the mapped MPM error code in section 4.5.2.3.
CSM Error Code	Choose from the CSM error codes; this will eventually be mapped for automatic reject / return.

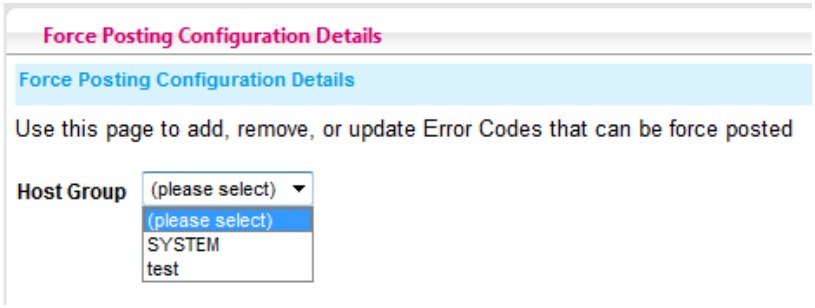
4. Click **Add**.

Force Posting Configuration

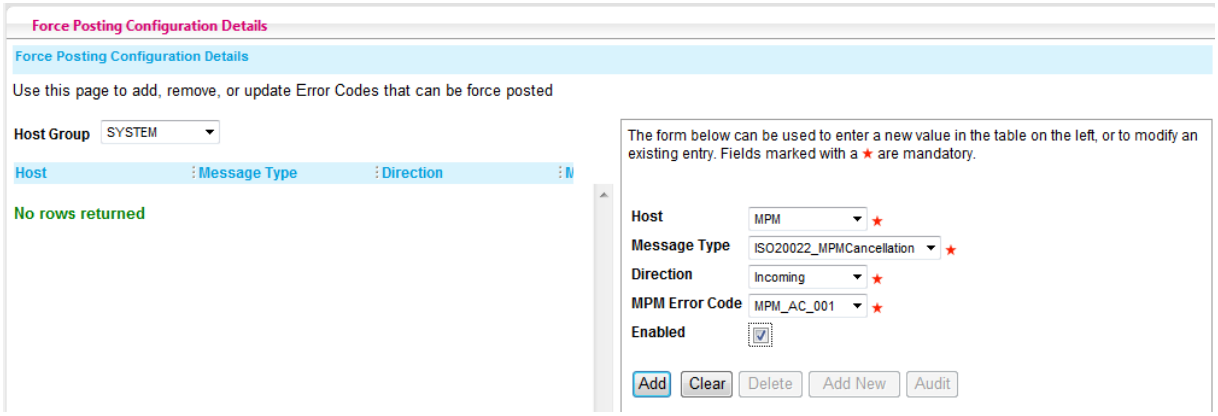
Force posting is when incoming canonical messages routed to the Manual Intervention Queue that failed posting are resubmitted and then moved to Posting In Progress Queue.

To use this:

1. Go to **Administration > System Control Data > Force Posting Configuration**.
2. Select a Host Group.



3. Provide the values for the following fields.



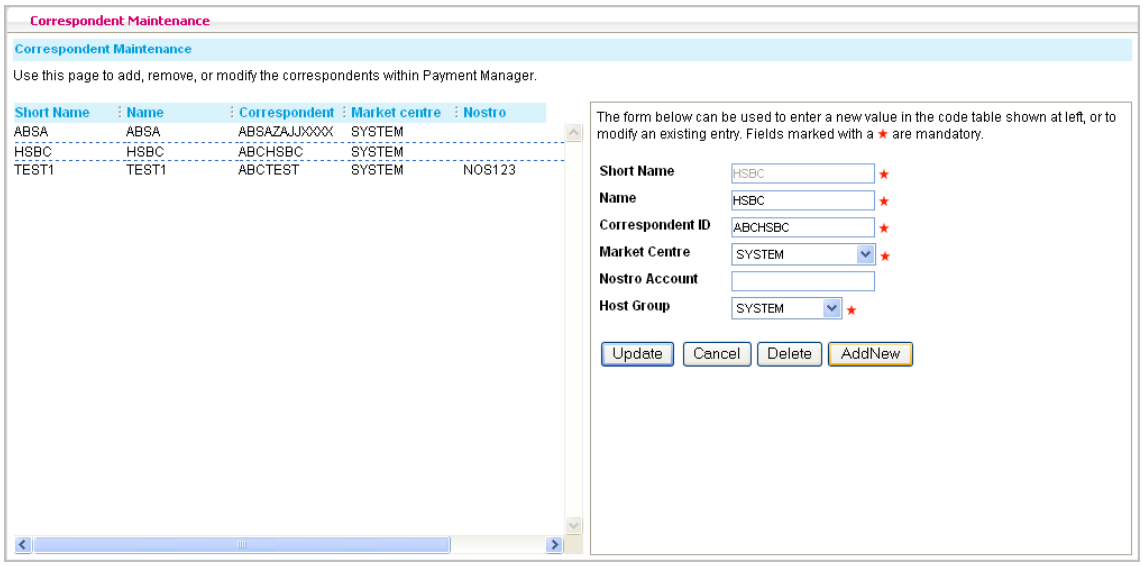
Field	Description
Host	Select a host.
Message Type	Select a message type that will be force posted.
Direction	This can either be Incoming or Outgoing.
Error Code	Choose between the two available error codes: • MPM_AC_001 – Account Unavailable • MPM_AC_002 – Insufficient Funds
Enabled	Ticking this will enable the rule.

4. Click **Add**.

Payment Configuration

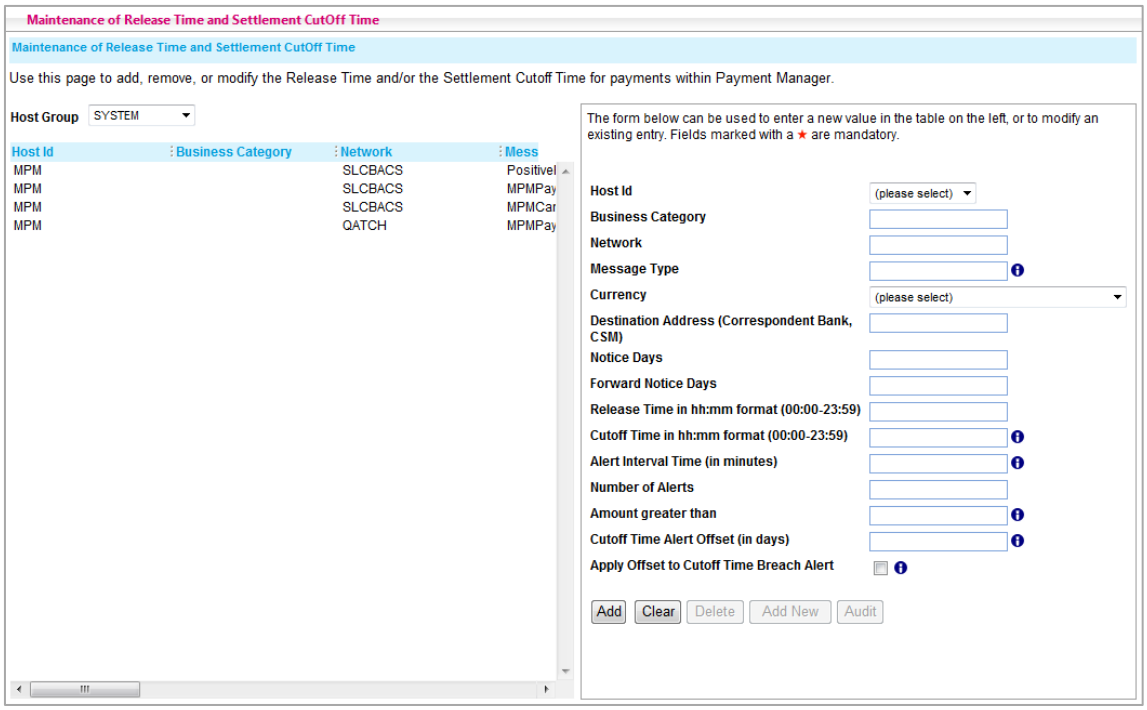
Correspondent Maintenance

This screen allows you to add, remove or modify correspondent bank details.



Field	Description
Short Name	Enter the short name for the correspondent bank.
Name	Enter the full name for the correspondent bank.
Correspondent ID	Enter a unique identifier for the correspondent bank.
Market centre	Select the correspondent bank's market centre. This will be used to determine the holidays associated with the bank. See Market Centre Holidays.
Nostro account	Enter the correspondent bank's nostro account.
Host group	Select the host group.

Payment Release Maintenance



Field	Description
Host Id	Select a host id.
Business Category	Enter a definition of business category
Network	Enter a payment network (or clearing and settlement mechanism).
Message Type	Enter the message type (e.g. MT103).
Currency	Select a currency.
Destination Address	Enter the destination address (Correspondent bank).
Notice Days	Enter the notice days.
Forward Notice Days	Enter the forward notice days.
Release Time	Enter the time at which this payment can be released.
Cutoff Time	Enter the latest time that this payment can be safely released.
Alert Interval Time	Enter the alert interval time.
Number of Alerts	Enter the total number of alerts to be generated.
Amount greater than	Enter a threshold above which payment release alerts will be sent.
Cutoff Time Alert Offset	Enter the cutoff time alert offset
Apply Offset to Cutoff Time Breach Alert	Ticking this will apply an offset to the cutoff time breach alert.

The release of any outgoing payment on its release date is conditional upon a number of factors, including settlement cutoff time and release time. Users can apply a notice period (in days) allowing specific payments to be released a number of days before their settlement date. Where notice period is applied, the release date of the payment is automatically updated. Payments can be released early, ahead of their release date, by assigning the facility to release a payment as a custom action to a user. See Assigning Custom Actions to Queues.

Prior to the release of any payment, a non-working day check is undertaken on the payment to ensure that the clearing & settlement mechanism (CSM) or correspondent bank (and your bank if it is a payment with a value in the future) are open for business on the day that the payment is due to go out.

The non-working day validation is a combination of the following checks, depending on whether the payment has a value of today or in the future:

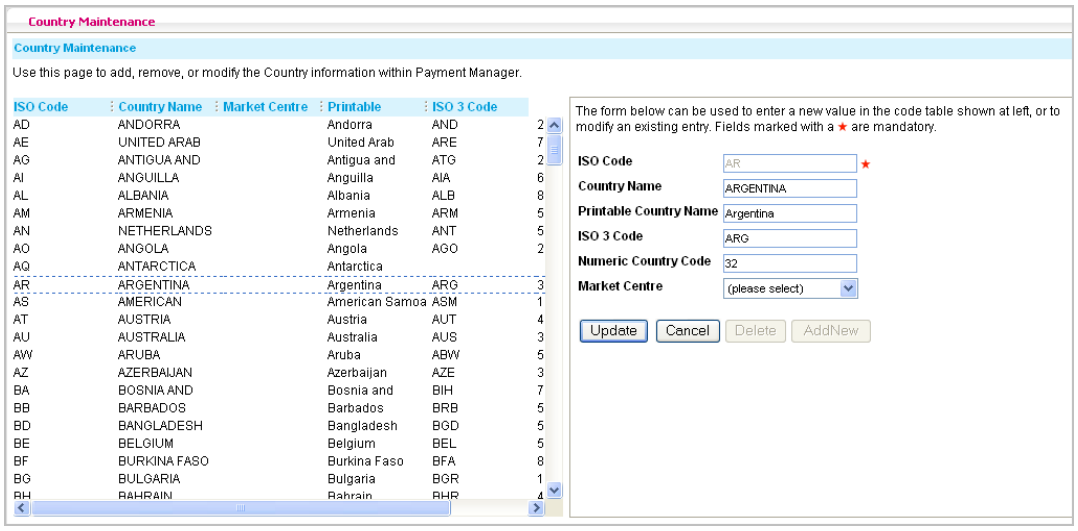
- a notice period check (see Settlement Cut-off Alerts)
- an originator check. This is a check for payments with a value in the future in order to verify that you, as the originator of the payment, are open for business on the day that the payment is due to go out
- a settlement currency check. This is a check made on the settlement currency to verify that it is a working day in the country aligned with the payment currency (e.g. USD = USA, JPN = Japan). This is a switchable feature Appendix C - Switchable Features.
- a CSM check
- a correspondent check
- holiday dates. These checks use the holiday calendars loaded for the tradable currencies your bank uses. These calendars can be amended and any changes will take effect immediately. See Market Centre Holidays.

Where a non-working day check for a payment with a value in the future fails any of the above checks, a check is made backwards for the next working day. If the previous day is a working day, a new release date is applied automatically; if it is not a working day the check is continued backwards until a working day is found, or until today's date is reached. If switchable feature Automatic Release Date Update is on, a payment which fails a non-working day check will have its release date reset. If this is not on, the payment will be queued.

If the Process Late feature is switched on, late payments will skip cycle checks and will be allowed through.

Country Maintenance

This screen allows you to add, remove or modify country information.

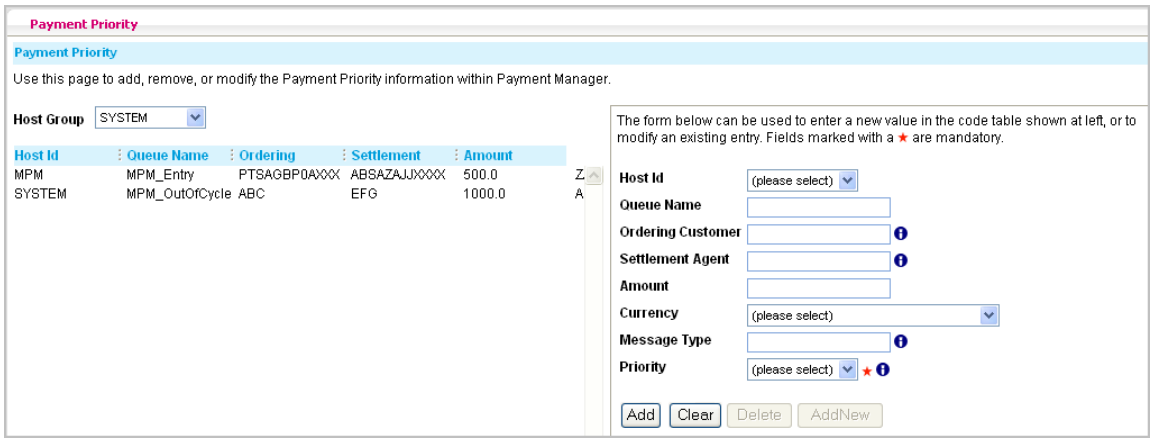


Field	Description
ISO code	Enter the country's ISO code.
Country name	Enter the name of the country.
Printable country name	Enter how you require the country name to appear in printed form, for example on reports.
ISO 3 Code	Enter the country's ISO 3 code.
Numeric country code	Enter the country's numeric code.
Market centre	Select the correspondent bank's market centre. This will be used to determine the holidays associated with the bank. See Market Centre Holidays.

Payment Queue Priority

The payment priority feature is used to assign priority to queued payments that require manual intervention. It can be useful to help users prioritise urgent and/or important business.

A priority range of one to ten can be applied based on message status, ordering customer, settlement agent, amount, currency and message type, or any combination of these. Priority one is the highest and ten the lowest. Priority can be assigned to any queue. The criteria can be changed during the day with any modification taking effect on all payments received subsequently. Where a payment does not match any of the criteria entered, a default priority of 9999 (the lowest) is assigned.



Field	Description
Host ID	Select the host from the dropdown.
Queue name	Enter the queue on which the payment resides. If you do not know the queue name you can use the view query functionality to determine it.
Ordering customer	Enter the name of the ordering customer.
Settlement agent	Enter the name of the settlement agent.
Amount	Enter the payment amount.
Currency	Select the amount currency.
Message type	Enter the message type e.g. MT103.

Field	Description
Priority	Select the priority you want to assign to the payment.

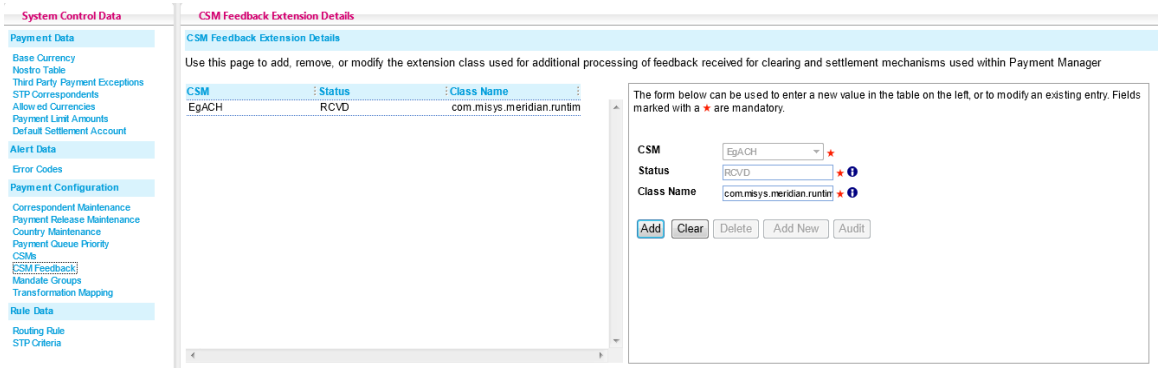
CSM Feedback

Feedback is received from the CSM and passes through the CSM Feedback Filter. This filter identifies the original message(s) and can make the following changes:

- Update CSM Status of the message(s)
- Link the feedback message to the original message(s)
- If the status is one of “ACTC” (Accepted), set the Window Id of the original message(s) and the feedback message.

CSMFeedbackExtensionsFilter

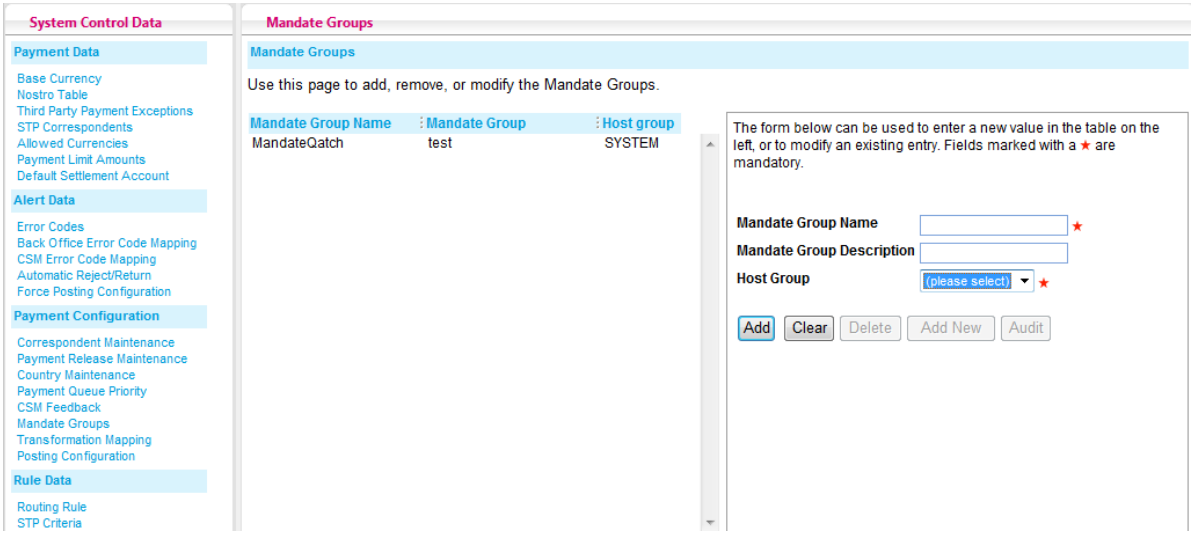
This filter is run after the “CSMFeedbackFilter” and allows users to set up additional processing according to the feedback received. This filter runs in conjunction with the CSM Feedback table data entered through the BFPM System Control Data interface.



Field	Description
CSM	The CSM as defined in the Clearing And Settlement Mechanism table.
Status	The status as received or set by the CSM.
Class Name	The full path to the class to be invoked.

Mandate Groups

This option allows you to set up new direct debit mandate groups.



Enter the details for the group and click **Add** to save them.

Transformation Mapping

The Transformation Mapping screen is used to manage records in the TRANSFORMATION_MAPPING table.

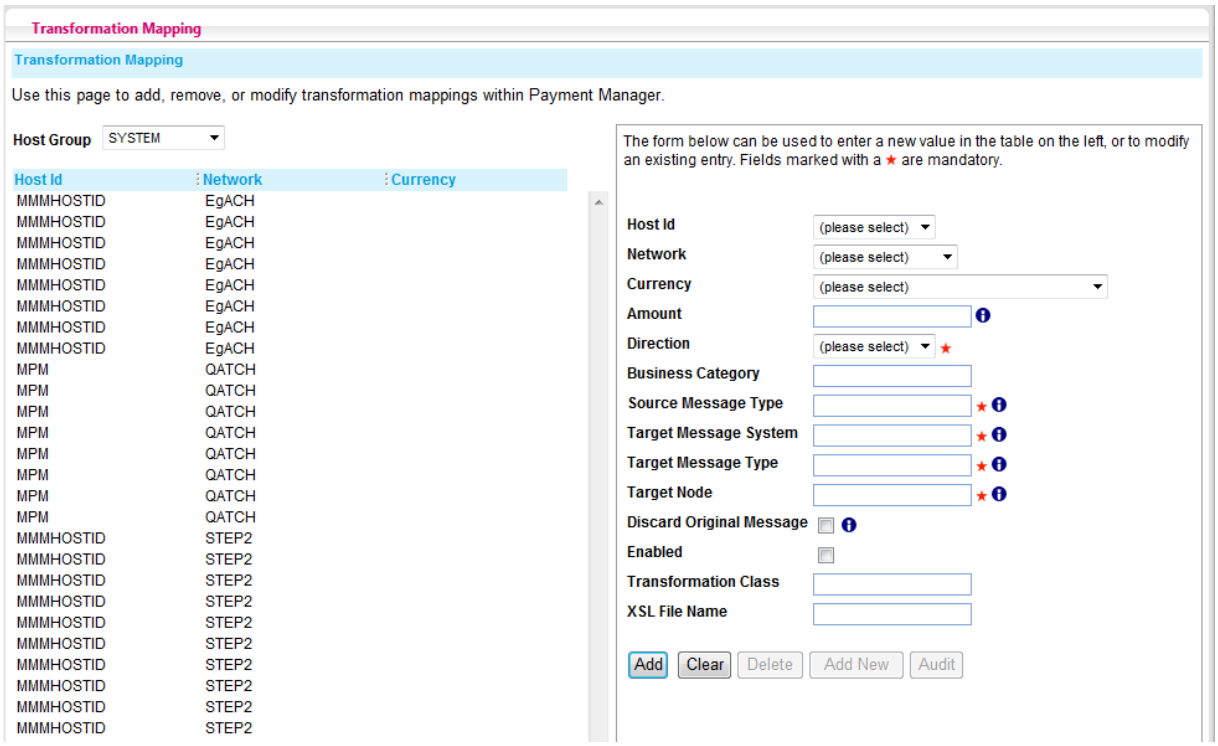
The records in the TRANSFORMATION_MAPPING table are the rules used, by the Transformation Service, to determine what class or XSL will map the message.

Transformation Mapping List

The Transformation Mapping list shows all the entries in the TRANSFORMATION_MAPPING table.

Transformation Mapping Form

The Transformation Mapping form is used to add and edit entries in the TRANSFORMATION_MAPPING table.



The fields are described in the following table:

Field	Description
Host Id	The Host identifier.
Network	Name of the financial network for this message.
Currency	The currency of payment.
Amount	The amount of payment.
Direction	It has three values: Incoming Outgoing Both The direction indicates whether this entry applies to incoming or outgoing, or both incoming and outgoing, payments.
Business Category	The Business Category; this is compared to the Line of Business field in the message.
Source Message Type	The Message Type of the source message.
Target Message System	The System name for the new, transformed message.
Target Message Type	The Message type of the new, transformed message.
Target Message Node	The Message node of the new, transformed message.
Discard Original Message	Checked: The original message will not be transmitted onward. Unchecked: The original message is transmitted onward using the normal node routing Note: In both cases, the new message is transmitted onward.
Enabled	Ticking this box turns on this activation mapping rule.
Transformation Class	The fully qualified class name of the class that will perform the transformation. It must implement the abstract class AbstractXSLTransformationMapping.
XSL File Name	The the XSL file name (with path) that will perform the transformation.

A Transformation Mapping rule may have either a Transformation Class *or* XSL File Name defined, but not both—one of these two fields must be blank.

Posting Configuration

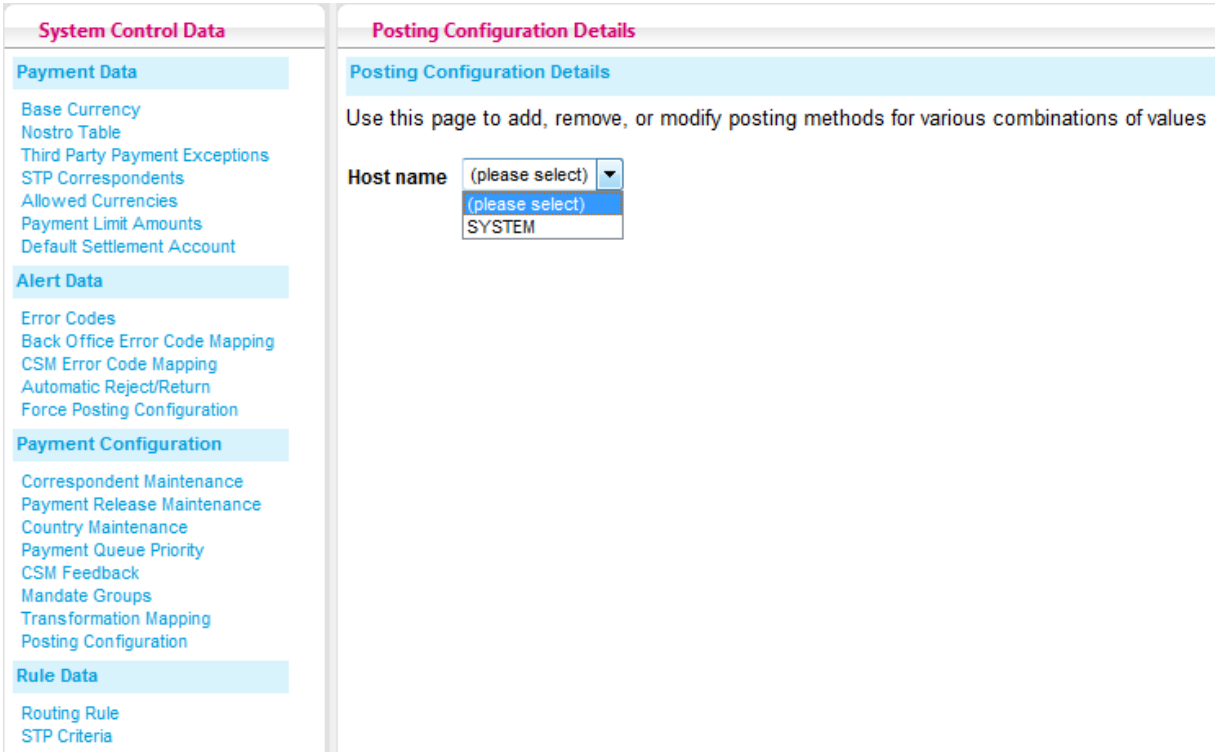
FusionBanking Payment Manager interfaces with an accounting system which enables the validation of the accounts involved in the payment and initiation of postings. This page allows the user to add, remove, or modify posting methods, i.e. single leg or dual leg, to payments/direct debit.

Single Leg posting method is when an accounting posting is performed; both the Creditor and Debtor Leg posting operation are performed in a single call.

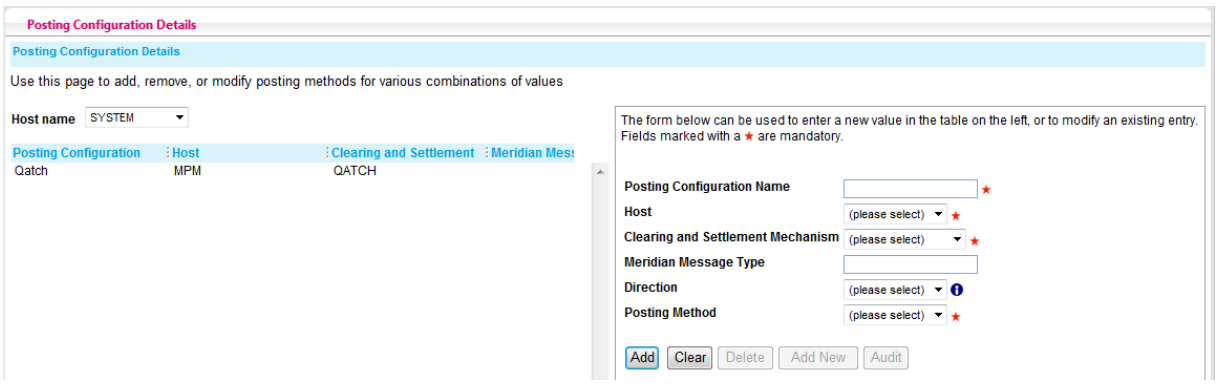
In Dual Leg posting, the creditor and debtor leg posting operation are executed as separate calls. In this case there will be two calls to the back office posting interface, one for creditor leg and another for debtor leg. In case of debits, it is vice-versa. Whereas in the Single Leg there will be just one call to the back office interface. Both the creditor leg and debtor leg posting will be performed in one call.

To use this:

1. Go to Administration > System Control Data > Posting Configuration.
2. Select a Host.



3. Enter the values for the following:



Field	Description
Posting Configuration Name	The name of the posting configuration.
Host	Select from the available hosts.
Clearing and Settlement Mechanism	Select a CSM.

Field	Description
Meridian Message Type	Add a note about the message type.
Direction	It has three values: • Incoming • Outgoing • Both The direction indicates whether this entry applies to incoming or outgoing, or both incoming and outgoing, payments.
Posting Method	This can either be Single Leg or Dual Leg.

4. Click **Add**.

Rule Data

The Routing Rule Data table allows you to enter new rules, criteria and outcomes for messages entering FusionBanking Payment Manager. Three tabs are available:

- Rule
- Criteria
- Outcome

You can specify conditions in a rule that query the data in the payment. Where these match, one or more outcomes (actions) will be applied.

Tab	Description of Table
Rule	This defines the purpose of the rule.
Criteria	This table stores a set of criteria for a rule.
Outcome	This holds the result that will be applied to the message should it match the criteria.

You must have the Configure System Control Data permission assigned in order to configure rules.

Rule tab

Enter the details as follows and click **Add** to save the rule.

Field	Description
Rule name	Enter a name for the rule.
Status	Indicate whether the rule is active (A) or inactive (I)
Description	Enter a description for the rule.
Criteria name	Enter the criteria name to be associated with the Rule. A same criteria can be assigned to different rules.
Outcome name	Enter the outcome name to be associated with the Rule. A rule can be applied to more than outcome and regardless of whether the outcome has already been

Field	Description
	applied to another rule.
Direction	Indicate whether the rule should be applied to an incoming or outgoing message.

Criteria tab

Enter values in any of the fields in this tab to define the conditions for the rule. Select **Add** to assign the criteria to the rule indicated in the Rules tab. A criterion can be assigned to different rules, if needed.

Field	Description
Criteria name	Enter the criteria name to be associated with the Rule. Note that a same criterion can be assigned to different rules.
Message Type	Indicate the type of message
Host ID	Choose a host in the drop-down list
Business Entity	Enter the Business Entity name in the first field or select one in the drop-down list.
Line Of Business	If needed, you can add the code of the business line.
Queue	Indicate the queue name
Network	Choose a Network in the drop-down list
TRN	Enter the transaction number either as an exact string or as a regular expression.
Sender	Enter the sender's name
Destination	Enter the destination address, if needed
Priority	The priority that can be Normal, Urgent, etc.
Currency	Choose in the drop-down list the applicable currency
Amount	The amount in the selected currency
Ordering Party	The characteristics of the ordering party
Beneficiary Party	The characteristics of the beneficiary party
Validation Status	The status of the message according to the network validation rules: Valid = message passed the validation Invalid = message failed the validation In Error = an exception occurred during validation
Error Details	Error code that can be entered either as an exact string such as X200 or by using a regular expression (e.g. F9..)
Cover Status	The type of cover e.g. Primary Message, Cover Message
Message Text	Short message text that you can enter as an exact string or as a regular expression.

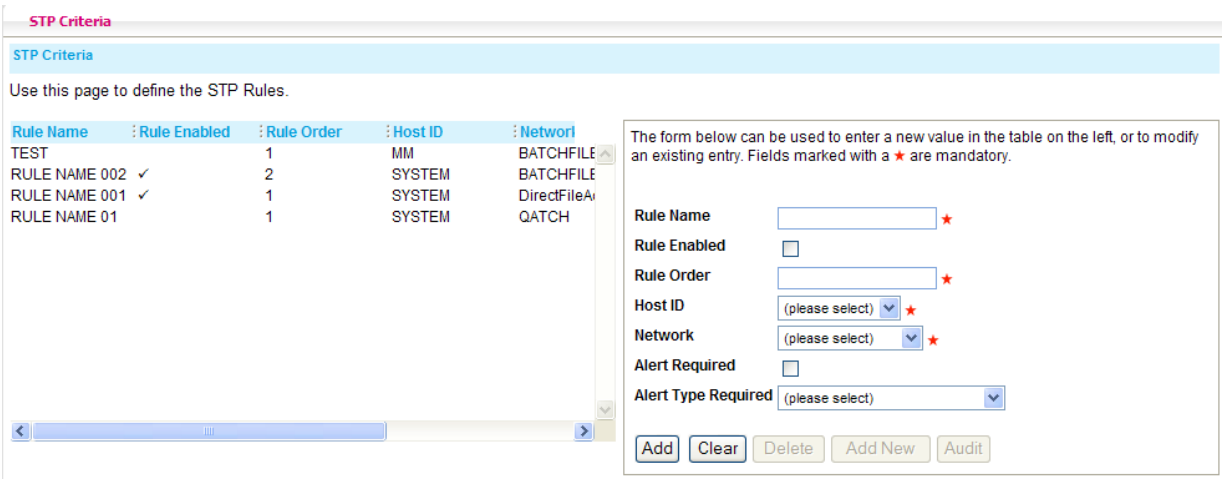
Outcome

Outcome name	Enter the outcome name to be associated with the Rule.
Endpoint	A node.
Endpoint action	An action which will be performed on the node.
Assign field	The field in the message that will change.
Assign field value	The value of the field.

STP Criteria

The STP Criteria feature allows you to define the STP rules based on which the payments will be processed.

If enabled, a STP rule will be applied, and the payments processed accordingly.



Enter the details as follows and click **Add** to save the rule.

Field	Description
Rule name	Enter a name for the rule.
Rule enabled	Check the box if you want to enable the selected rule.
Rule Order	Specify here an integer that will indicate in which order the rules will be applied (if several rules are assigned to a message matching a Host ID and Network Type).
Host ID	Choose in the drop-down list the host name to which the rule will apply.
Network	Choose in the drop-down list the network name to which the rule will apply.
Alert Required	Check this box if you want an alert (of the type you have specified) is raised if a message fails a rule validation.
Alert Type Required	Choose in the drop-down list the type of alert you want will be raised.

Configuring the FileAct Application

This section describes how to configure the FileAct application which allows you to transfer files via SWIFTNet FileAct.

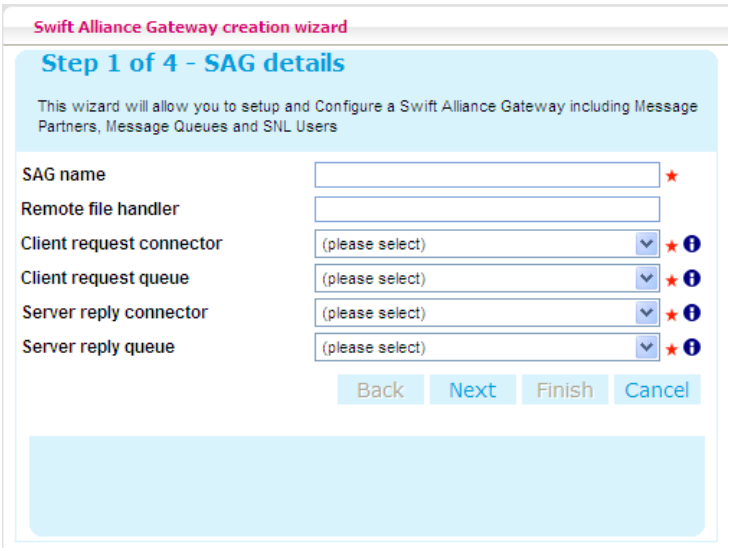
Configuring the SWIFT Alliance Gateway

The MQHA Interface is used to connect to SWIFT Net Link (SNL) via the SWIFT Alliance Gateway (SAG).

Creating a SAG Configuration

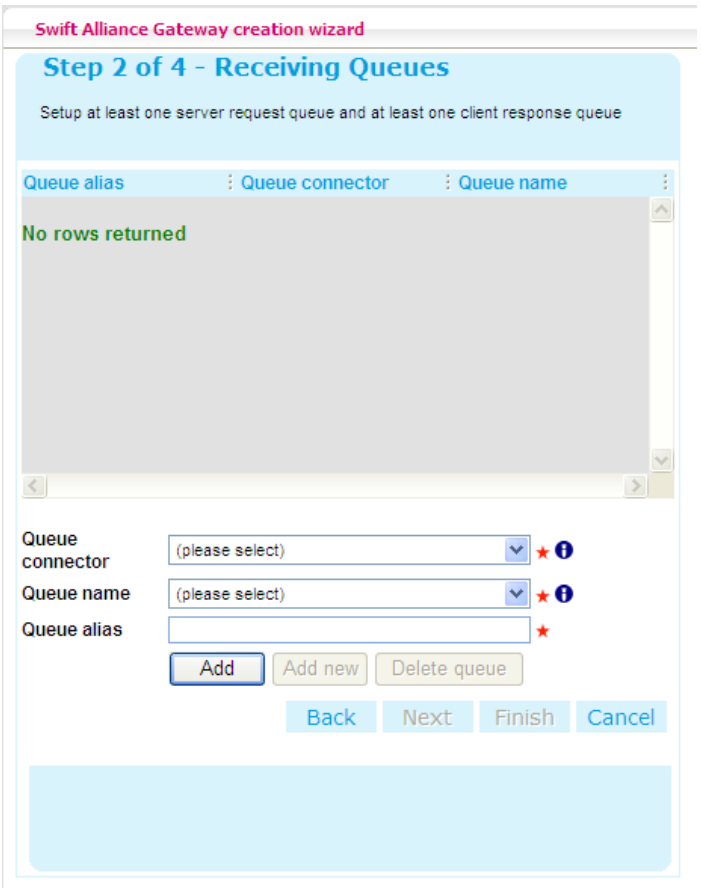
From the Administration menu, select **FileAct configuration > Create SAG**.

You will be guided through the SAG creation process in a series of steps.

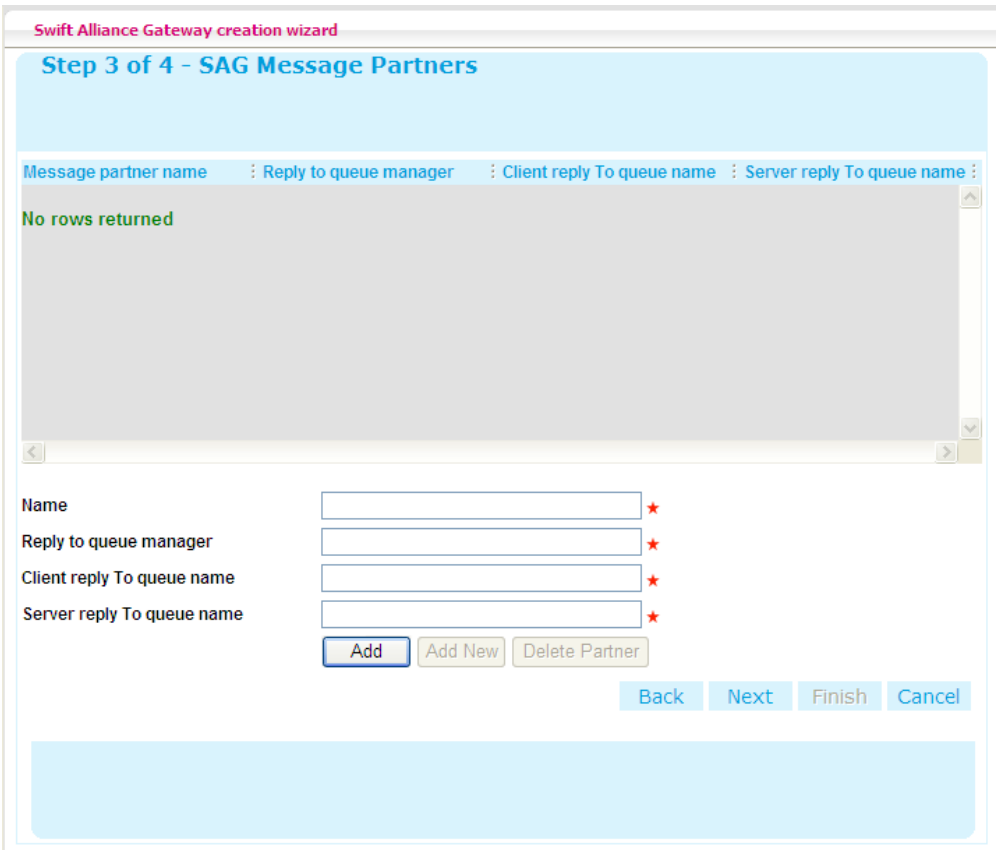


1. **Sag name** is used to identify this particular gateway instance.
   Remote file handler is a unique string that will be used to identify this particular gateway instance to the **Remote File Handler Manager** process, which is a separate application which communicates with the SAG itself.
   Client request connector and **Server reply connector** are connectors defined in the BankFusion Meridian project.
   Client request queue and Server reply queue are the WebSphere MQ queues to which client request and server reply messages will be sent. The dropdowns shows the ones that are defined in the project.
   Complete the fields and click **Next**.

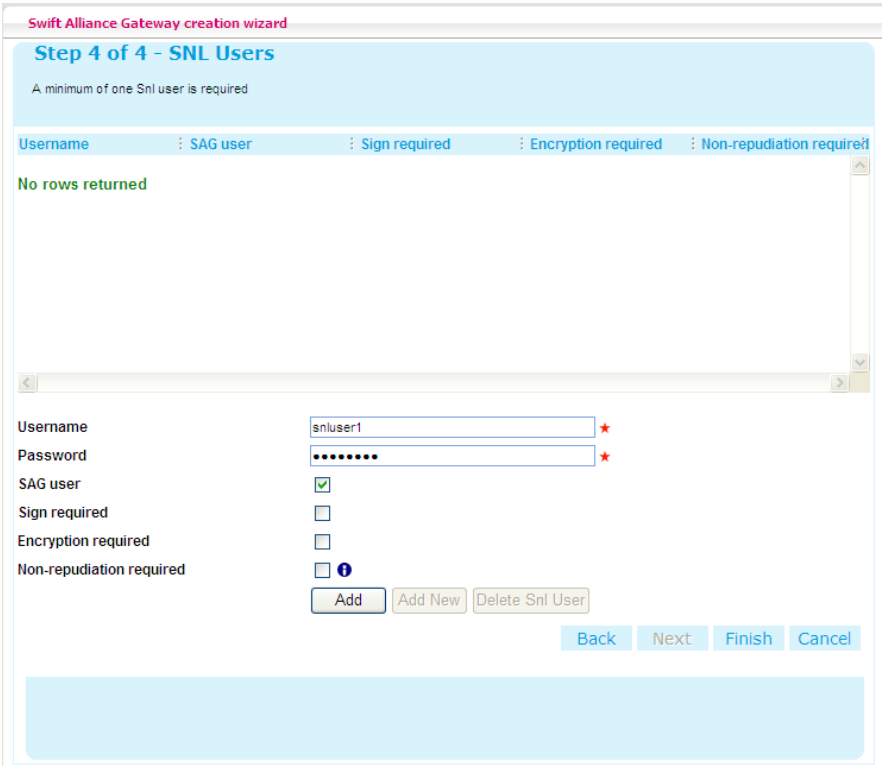
As the instructions on the following screen indicate, you have to specify at least one server request queue and one client response queue. Select the Queue Connector and Queue Name from the dropdowns, specify a Queue alias, and click **Add**, for each.
When you have finished, click **Next**.



2. Add the details for communicating with the SAG, then click **Next**.



3. Fill in the details for the SWIFTNet Link user. Note that the **Sign required** and **Encryption required** checkboxes only appear if you check Sag user.
Click **Finish** to complete SAG creation.

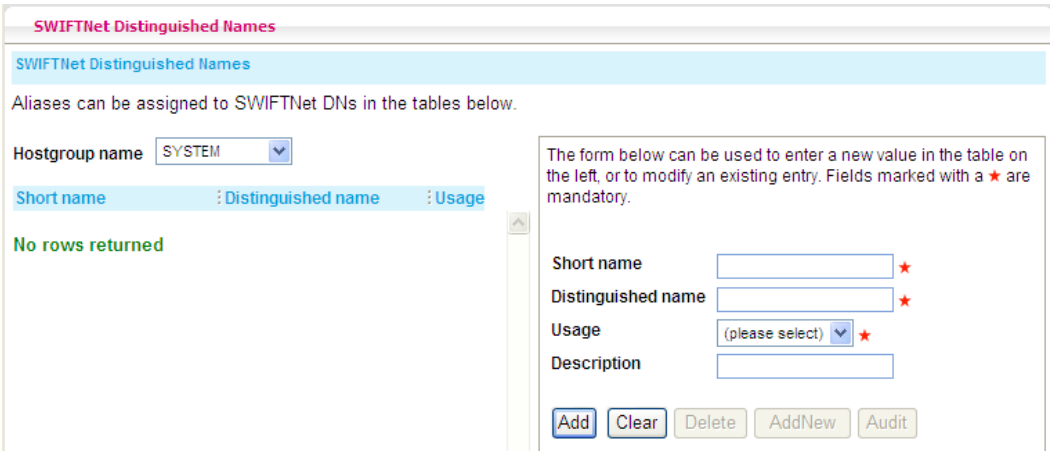


Configuring an existing SAG

You can configure existing SAGs by clicking **Configure existing SAGs** on the FileAct configuration menu and selecting the one you want to configure from the dropdown.

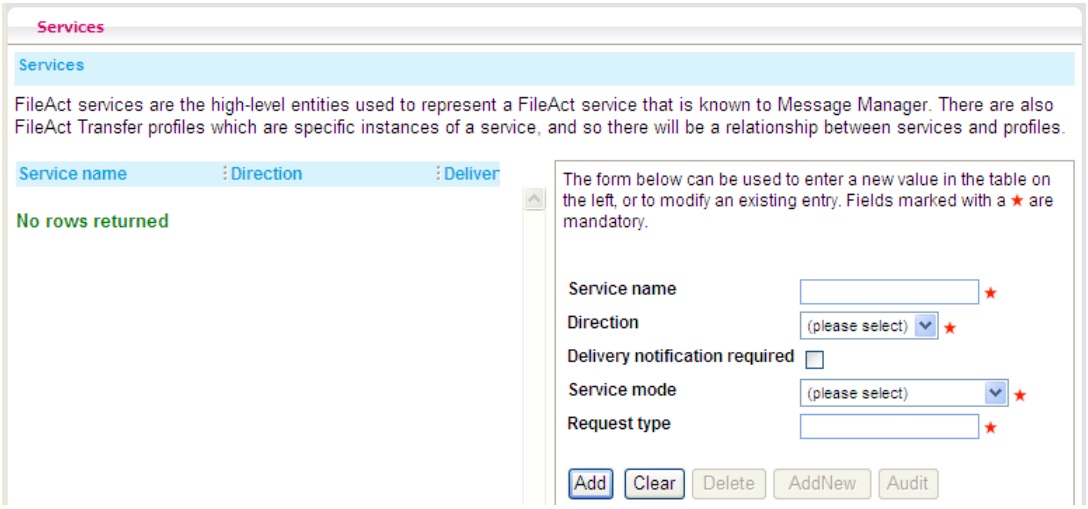
Configuring SWIFTNet DNs

Use this function to configure the Distinguished Names (DNs) that FileAct will use.



Select the hostgroup to which the DN belongs from the dropdown then fill in the other details in the fields to the right. **Usage** can be 'Sender', 'Receiver' or 'Both'. Click **Add** to save the details.

Configuring FileAct over SAG Services



Service name is defined as follows in the SWIFTNet Service Design Guide:

The Service name defines the context for interpreting many other names and parameters in SWIFTNet. It is defined by agreement between SWIFT and the Service Administrator. It is established through the provisioning process for a new business service.

Direction can be 'Send' or 'Receive'.

Delivery notification required is only applicable for Services with Direction = 'Send'. If checked, the file Sender indicates to the Receiver to send a Delivery Notification if a delivery is successful.

Service mode can be 'Realtime' or 'Store and Forward (SnF)'. This is the SWIFT-administered name of the business service to be used for the transfer.

Request type is the specific request type for the service identified in the Service Name above. Both Service Name and Request Type must refer to an operationally valid business service registered with SWIFT. The SWIFTNet Service Design Guide has this to say about Request Type Names:

All messaging begins with a Request message. Every such Request must be identified in its Request Header as belonging to a Service. Taken together, the Service and Request Type elements define the structure and contents of the Request. They also implicitly define the structure and contents of the associated Response.

Transfer Profiles

FileAct File Transfer Profile Wizard

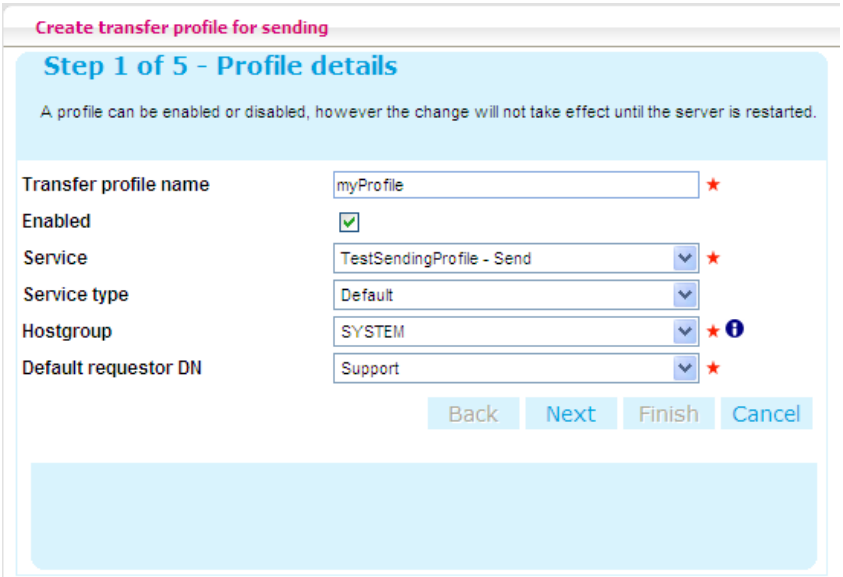
There are two menu options for creating transfer profiles in the FileAct configuration page under the FileAct Transfer profiles heading:

- Create transfer profile for sending
- Create transfer profile for receiving

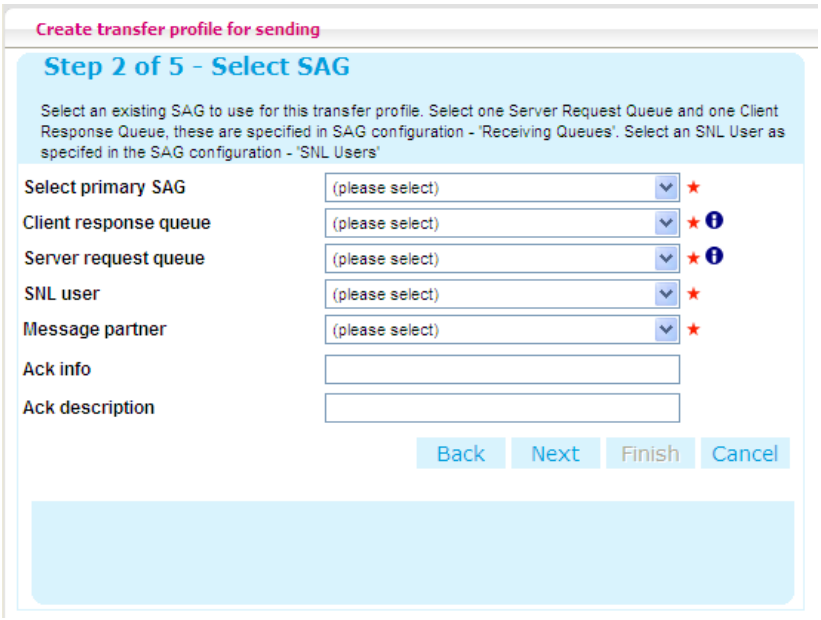
Creating a transfer profile for sending

1. Profile Details

   The Enabled checkbox will enable and disable a transfer profile. This takes effect only when the server is restarted.
   Select a FileAct service and host group. These are mandatory. When the host group is selected, the default request DN will update dynamically with DN's created for the selected service. This will also update the **Default FileAct Destination (DN)** on the **Destination details** tab.
   If 'Store and Forward (SnF)' is selected as the service mode in the underlying service as selected on the profile details page, then an SnF Service Request Queue will be displayed on the **Sending details** tab. This will be mandatory.



2. Select a SAG created in the Sag Wizard. A profile cannot be created if no SAGs exist. The Client response and Server request queues must be different from each other, otherwise an error message will be returned.



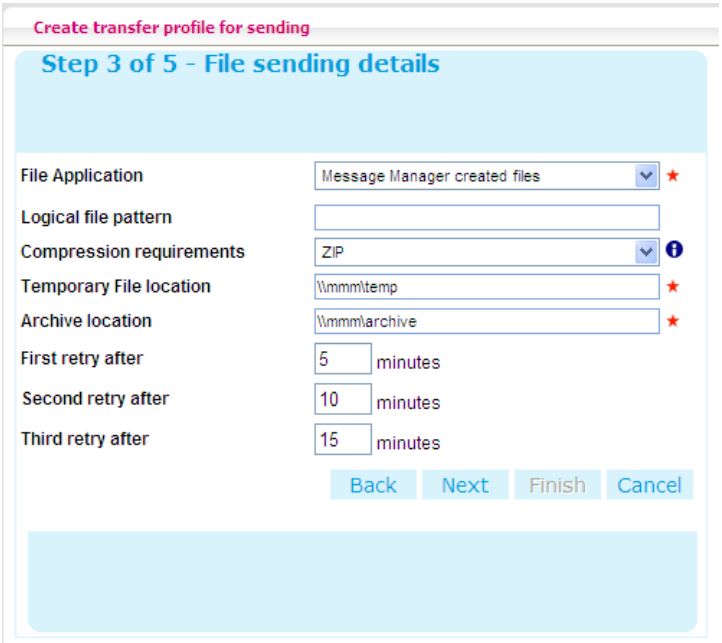
3. The file application drop-down list displays Message Manager created files and **Files created by an external application**. Select the type of file application.

   The next tab - **Destination details** will display different information relevant to the File Application selected. The **Compression requirements** dropdown list is populated with: none, GZIP, ZIP.

   The **Archive location** is mandatory.

   The retry information is set as default to 5, 10 and 15.

   If **Store and Forward (SnF)** is selected as the service mode in the underlying service as selected on the profile details page, then an SnF Service Request Queue is displayed on the page.



4. Destination Details

   The **Logical filename pattern** and **User reference** use the Filename pattern details form to validate regular expressions.

5. Destination details – Message Manager created files

Queues

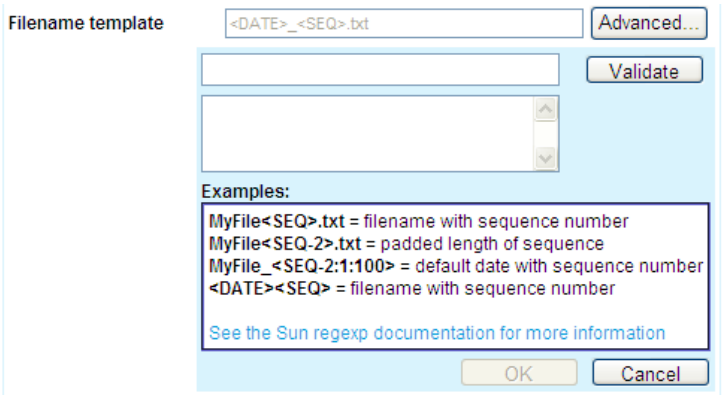
The source queue drop down list displays a mixture of MMDA and non-MMDA nodes setup in the project. When a queue from the list is selected which is an MMDA queue then a target queue dropdown list becomes visible. The target queue field is mandatory.

Message Information

The **Message format** dropdown list is populated with the formats specified from the project.

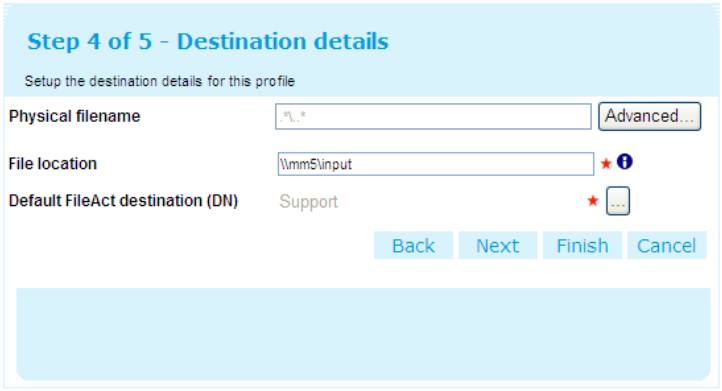
The **Message type** dropdown list is populated with all the messages specified in the SWIFT system of the project.

The filename template is populated using a popup window. The window displays helpful examples of typical filename patterns. To set the Filename template field the pattern needs to pass validation. The file is validated against regular expressions.

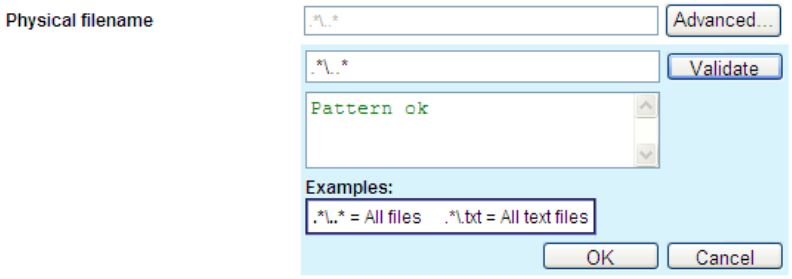


6. Destination details – Files created by an external application

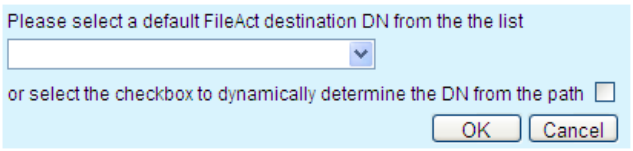
Files created by an external application do not require any information from BankFusion Meridian. A filename and location are mandatory. The filename has a default value setup already.



The **Physical filename** is populated using a popup window. The window displays helpful examples of typical filename patterns. To set the **Physical filename** field the pattern needs to pass validation.



The destination DN does not have a drop down list instead a popup window displays two choices – a drop down list and a tick box where you can choose to dynamically determine the DN from the path during runtime.

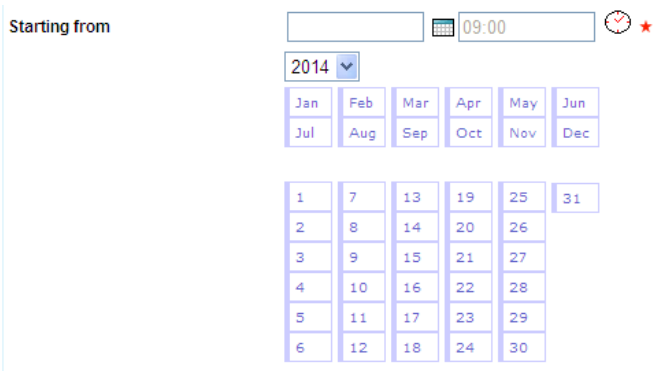


7. Transfer schedule details

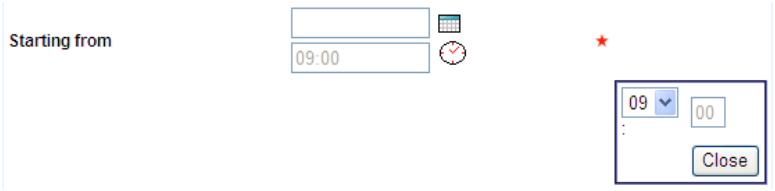
   The Transfer Scheduler has been designed with simplicity and flexibility in mind. The transfer schedule page is used for making choices of when the transfer profile is invoked.

   It is mandatory to select a start date and time from when the scheduler is to start. This is done via a simple date and time picker, as shown below:

   Date Picker



Time picker

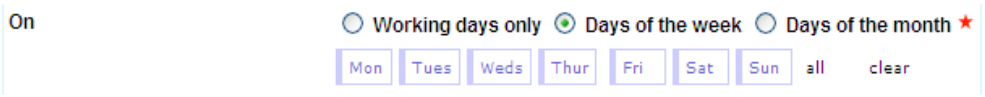


The days for which the scheduler is to be run on has three options, **Working days only, Days of week and Days of month.**

Working days only will run the scheduler on the working days according to the selected host group's market centre. The Host group is selected in 'Step 1 Profile details'.

Days of the week

If you select the Days of the week option you will be presented with a multiple picker with the days of the week.

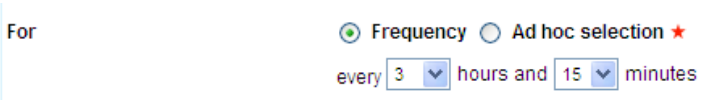


Days of the month

If you select the Days of the month option you will be presented with a multiple picker with for 31 days of the month. If the 31st is picked and the current month doesn't have 31 days, the scheduler will not run.

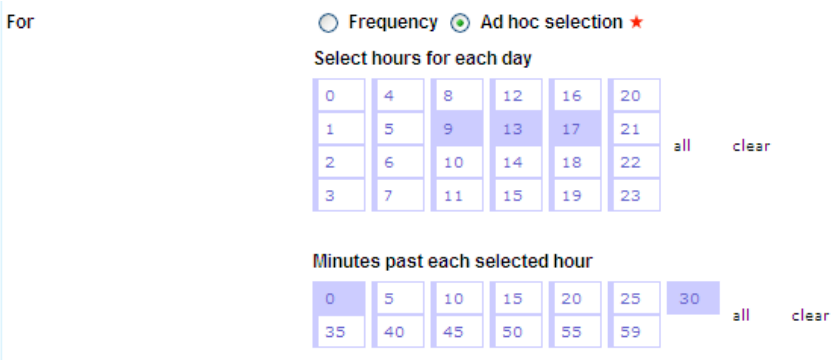
Frequency

During a day the simplest approach to run the scheduler is by a frequency. If the frequency is option is selected an hour and minute picker is displayed. The scheduler will run when every time the hour and minutes frequency has elapsed. In the case below, the scheduler will run every 3 hours and 15 minutes.



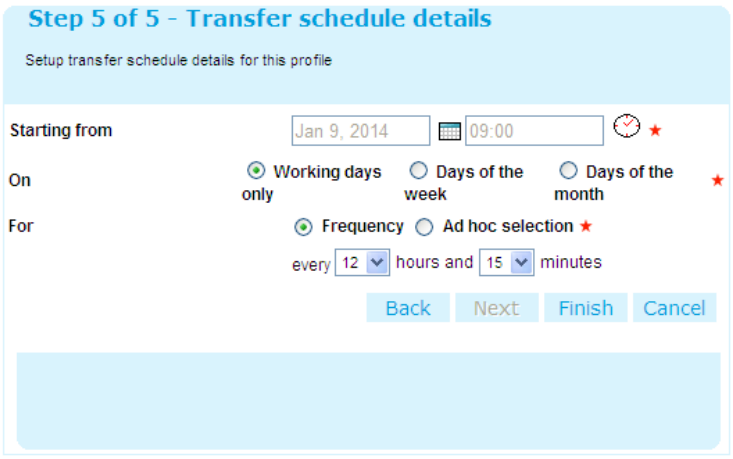
Ad hoc selection

The Ad hoc selection option provides a more flexible approach. You may randomly select a multiple number of hours based on a 24 hour clock. You may make multiple selections of when the schedule will run pass the hour.



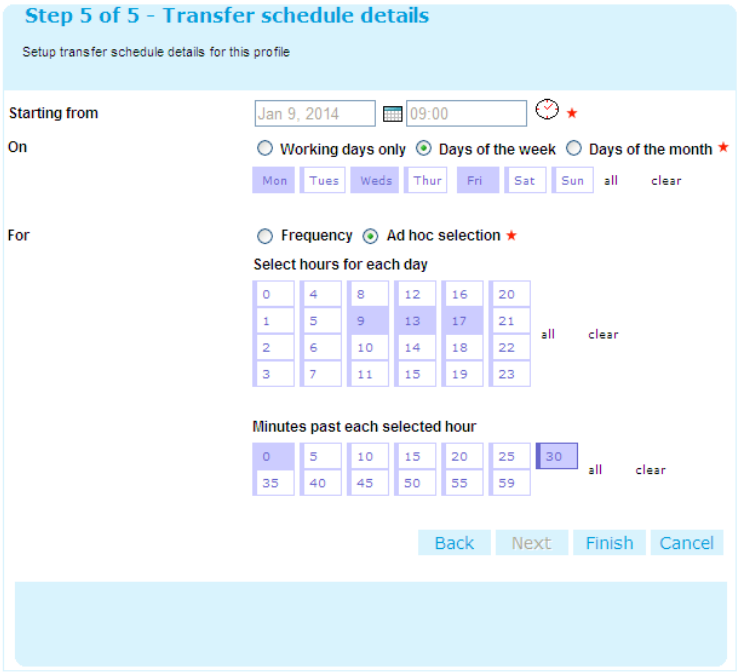
Simple setup example

The most common and simple setup will regularly use the working days of the current market centre and a frequency.



Advanced setup example

An ad hoc setup could typically use specific criteria as selected below:



Creating a transfer profile for receiving

Four steps are required for setting up a transfer profile for receiving.

1. Profile details
2. Setup sags
3. Receiving details
4. Transfer schedule details

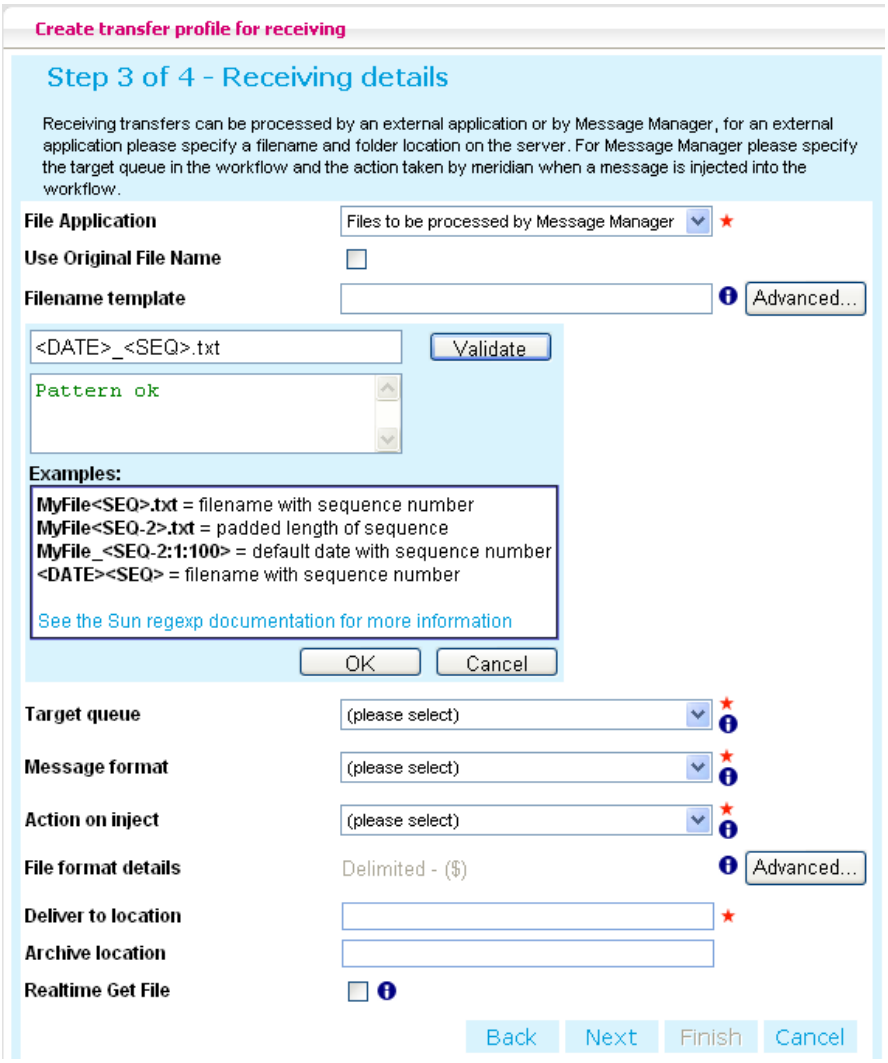
Steps 1, 2, and 4 are the same as setting up transfer profiles for sending. For more detail on these steps please refer to the section above - **'Creating a transfer profile for sending'**.

Step 3 – Receiving details

Like sending transfer profiles Files can be processed by Message Manager or an external application.

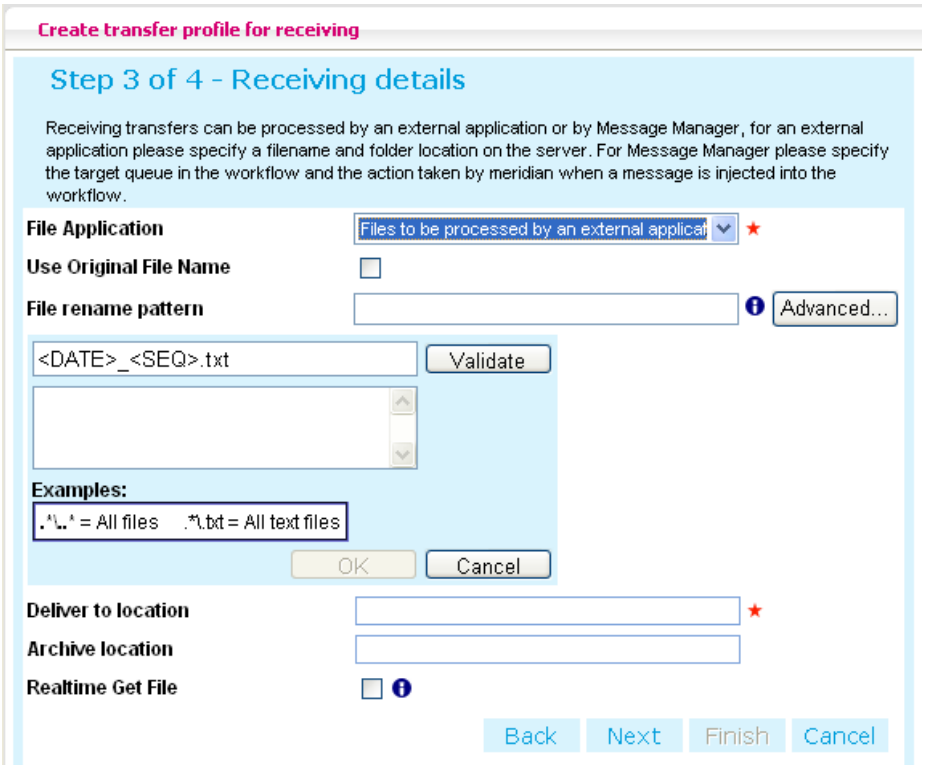
Files to be Processed by FusionBanking Payment Manager

If the files are to be processed by FusionBanking Payment Manager then a target queue defined within the project and the action to **Transmit** or **Put** the file is required. The **Target Queue** field is populated with the nodes defined in the project. The **Action on inject field** defines the action. If the action **Put** is selected the file is **Put** on the node. If the action **Transmit** is selected the file will be put on the node and then transmit through the project.



Files to be processed by an external application

Files delivered to a location require a valid location to deliver the file.



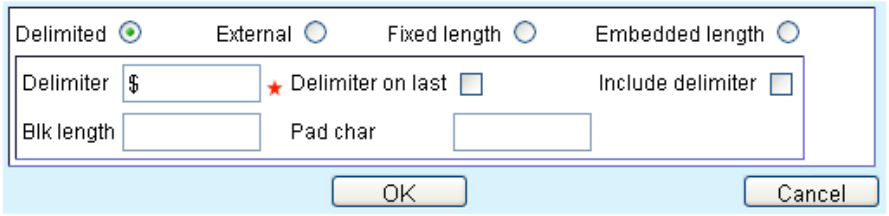
File format details

The File Format Details page is used for Splitter and Joiner information for receiving and sending files. The file format information will be stored as XML. The page will display the same layout as the `File Formats` tab on the Flat file adaptor. The file Formats page will be accessible via an Advanced button on the FileAct Transfer Profile page:

Common to all message formats is Encoding and Batch size. The encoding is set as default to UTF-8, which is the most commonly used.

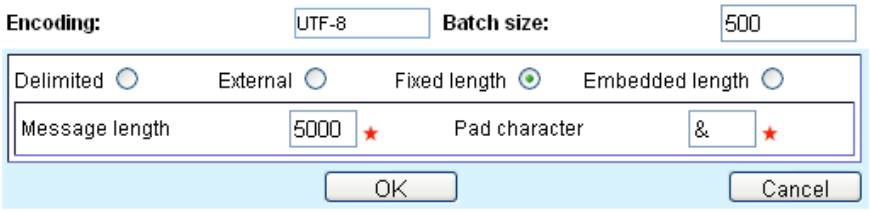
Delimited (default)

The delimited file format is the most commonly used and is therefore set as the default option. The delimiter is used to split the messages. If the file has a delimiter at the end of the last message in the file please check the **Delimiter on Last** field. The **Pad Char** field is used to separate fields.



Fixed Length

For fixed length messages the message will be parsed by splitting each field at the field length specified. A pad character is used to pad out the remainder of characters that aren't used in the field. Typical the pad character is white space.

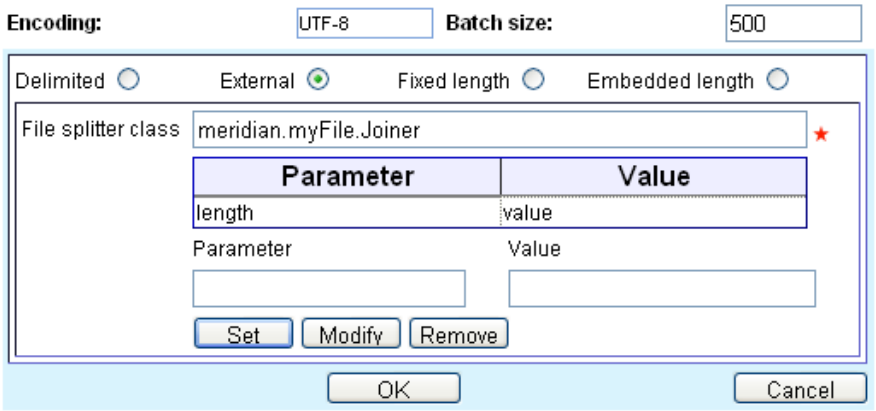


External

If the file format covered by the system is not adequate, the user may extend the Splitter and Joiner interfaces provided by BankFusion Meridian to provide their own external solution. For receiving profiles the splitter class is used to split the messages, for sending profiles the Joiner class is used to batch up the messages for sending. Include the class and path in the **File joiner class** field. Any number of parameters can be added to the grid view to pass through to the class constructor.

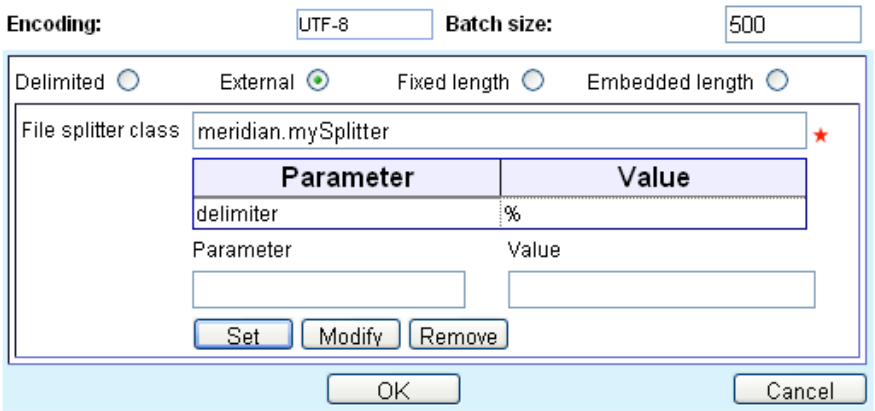
Joiner class for setting sending Transfer Profiles

External file format which uses a class that implements the com.misys.meridian.userapi.receptacle.Splitter interface.



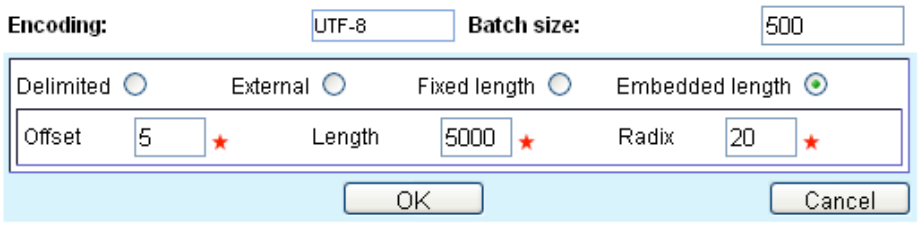
Splitter class for setting receiving Transfer Profiles

External file format which uses a class that implements the com.misys.meridian.userapi.receptacle.Joiner interface.



Embedded Length

In certain legacy systems the message length is embedded within the body of the message. Each message has an offset which acts a buffer between messages. After the offset, the message length is defined in bytes. The **Length** field defines the number of bytes for holding the message length. The **Radix** field is the base for the positional numerical system.



Scheduling tasks

This maintenance function allows you to configure the Scheduler service, which is defined in the FileAct project.

It is accessible from the **Administration/Configuration** menu (note: not **FileAct configuration**). Click on the **Schedule tasks** link, under the **Scheduler** heading.

The fields are self-explanatory. Note that **Month**, if specified, must be a numeric value, where January is 1, and December is 12.

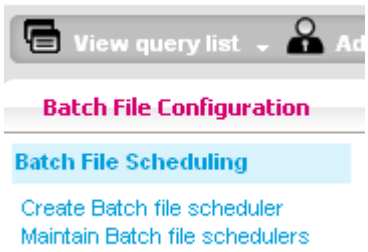
The **Task** field refers to a **Service** name, specified in the project.

Configuring Batch Files

Enabling Batch File Functionality

The Security option 'create and maintain Batch file profiles', is provided to view batch file configurations in read only mode and to create, modify and delete batch file profile configurations.

Select Administration > Batch File configuration from the main menu:



The batch file configuration menu allows you to create new batch file configurations and modify existing ones:

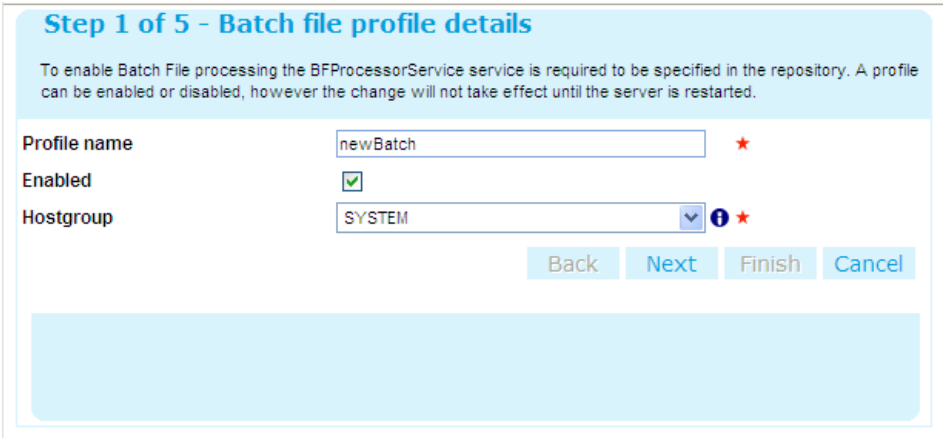
Batch File Profile Details

A series of five screens will be displayed, the first of which allows you to enter details of the new batch file profile.

In the **Profile name** field, enter a name for the batch file. The profile will automatically be enabled.

The Hostgroup is included here for subsequent querying purposes.

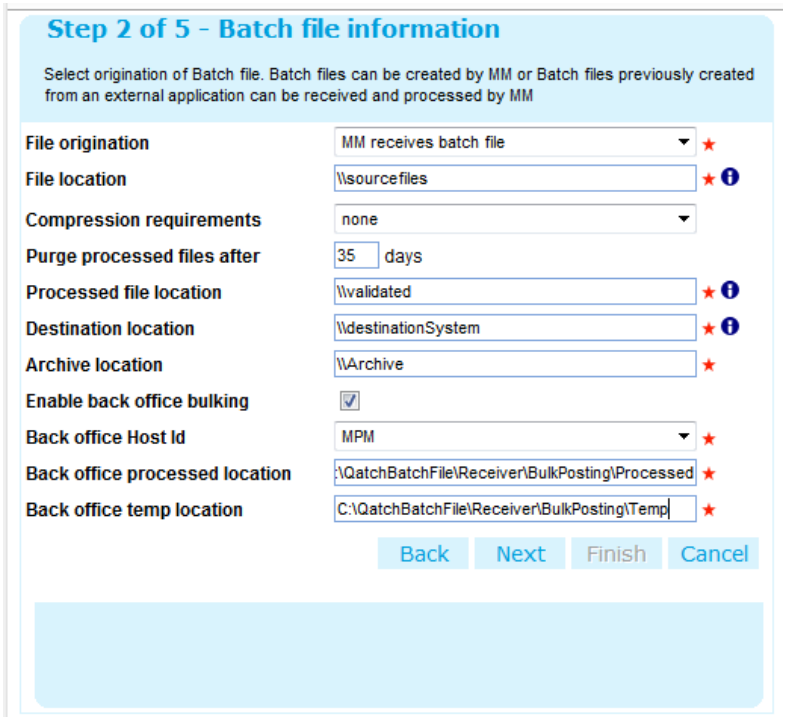
Click **Next** to proceed to the next screen.



Batch File Information

This screen displays fields for the entry/selection of:

- File origination - whether the batch file is created by FusionBanking Payment Manager or comes from an external application
- File location - the location of the batch file if it comes from an external application
- Number of days after which files within the processed folder (below) will be purged
- Processed file location - the location of the file after it has been checked for duplicates and validated for valid formats. The batch file will remain here until the file is transmitted either via the GUI manually or when the scheduler is invoked
- Destination location - the location the batch file is moved to when it is transmitted
- Enable back office bulking – When enabled, a bulk file will be rendered that contains the BFPM event block messages in canonical format.
- Back office Host Id
- Back office processed location – Where the processed files are located.
- Back office temp location - Where the temporary files are located.

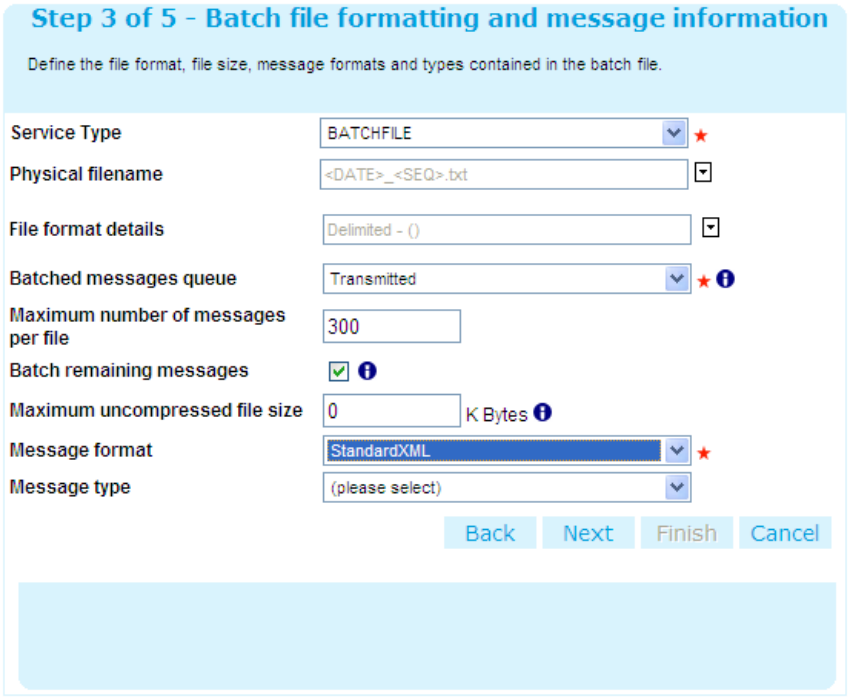


Batch File Formatting and Message Information

This screen displays fields for the entry/selection of:

- Physical filename
- File format details
- The Batchable messages queue. This displays MMDA nodes in the project where individual messages can be held ready to be grouped into a batch file. **This is not available if messages are received from an external application for this profile**. Project routing will be required to allocate messages to this node. This could be done for all SWIFT MT210 messages, for example
- Batched messages queue - once messages are batched they are moved here
- Maximum number of messages per file - this is used to specify the number of messages which can be bulked together per file. The checkbox 'Send remaining messages' is used to send the remaining messages held on the Batchable messages queue even if the number of messages does not reach the maximum size. e.g. If the Batchable message queue contained 620 messages with a Maximum message size of 300 specified, then 2 batch files containing 300 messages will be sent and the remaining 20 messages will also be batched and sent
- Message Format. Batch files are restricted to contain messages of the same format. The dropdown provides message formats as specified in the project.
- Message Type. This is optional as batch files are not restricted to one message type

There must not be more than one STEP2BIC batch file profiles.



For Outgoing SEPA CSM, the Physical filename must confirm with the EBA File Naming Convention.

The Network File Name is the identifier of the file as it is transferred over the file exchange.

STEP2 network filenames structures are as follows:

EEVVSSSBBBBBBBBX…X.Z

- The meaning of these fields is as follows:
- EE must be S2 (STEP2);
- VV is the format version (02 = XML for files and text format for reports);
- SSS is the three character service identifier, SCT in this case;
- BBBBBBBB is the BIC(music) of the Direct Participant;
- X…X (optional) is up to 15 characters for use by the Direct Participant; and
- Z indicates the type of the file, where:
    - I = ICF;
    - V = CVF;
    - N = SCF;
    - C = CCF;
    - L = PCF;
    - R = CRR;
    - D = DRR
    - M = MSR
    - T = RTF

All Direct Participants sending files to the STEP2 central system must adopt this convention. The X…X field is not validated.

The STEP2 central system generates files with X…X fields as follows:

YYMMDDHHMMSSNNN

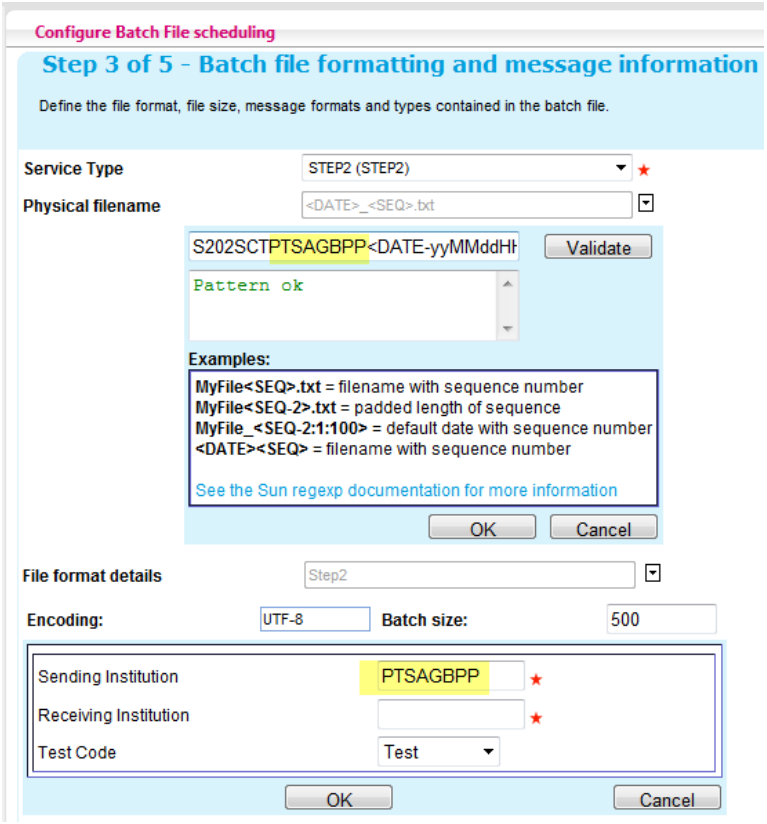
where:

- YYMMDDHHMMSS, which is the file creation date and time, and
- NNN, which is an incremental number starting from 000 that is reset to 000 every time DD (date) changes (this number is global for all files sent by CS and not specific to a single DP).

Note that in the case of STEP2 generated files, the BIC part of the Filename (BBBBBBBB) is the BIC of the Direct Participant (and not the STEP2 BIC).

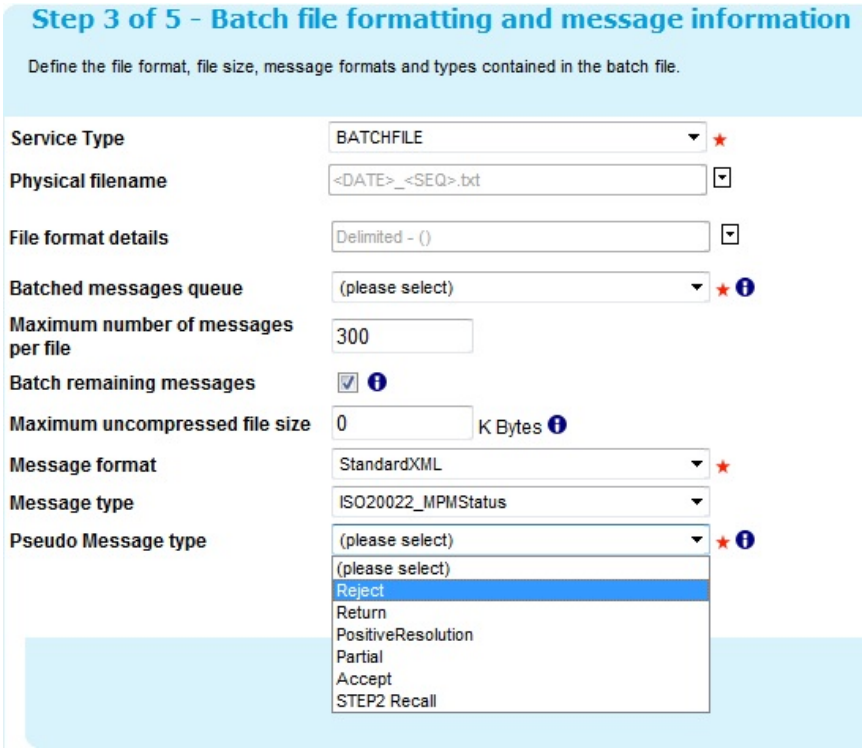
The following standards apply to filenames:

- No leading spaces are allowed;
- No internal spaces are allowed;
- Trailing spaces are ignored; and
- Alpha characters are case insensitive, e.g. “filename” is the same as “FILENAME” and “Filename”.



Pseudo Message Type

This field will appear if the Message Type field has a value of ISO20022_MPMStatus. The dropdown values contain all the message types that are categorized as MPMStatus.



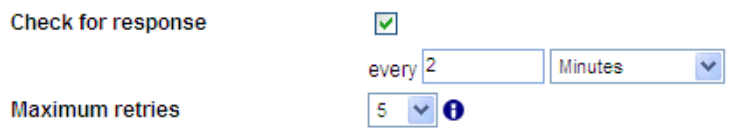
For QATCH and EgACH networks, this field is mandatory for all outgoing MPMStatus messages, and optional for all incoming MPMStatus messages.

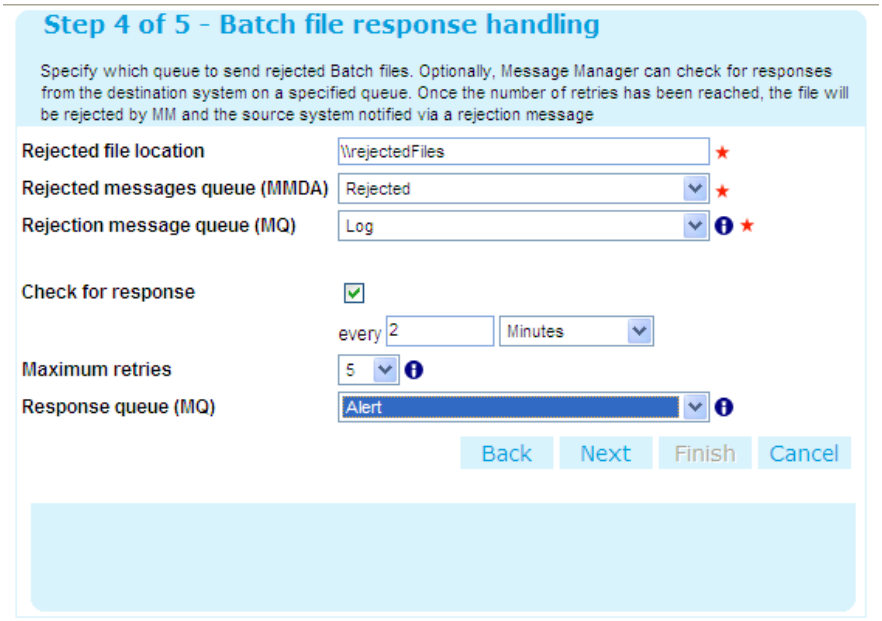
Batch File Response Handling

This screen displays fields for the entry/selection of:

- Rejected file location - Files can be rejected via FusionBanking Payment Manager, user interaction or the destination system. When a file is rejected it will be moved here
- Rejected messages queue - If the batch file was created by Payment Manager, the messages within the batch file will be moved to the rejected MMDA queue, thus allowing individual processing.
- Rejection message queue - When a file is rejected, a rejection message is created and put on an MQ queue. This drop down provides all the MQ queues specified in the project.

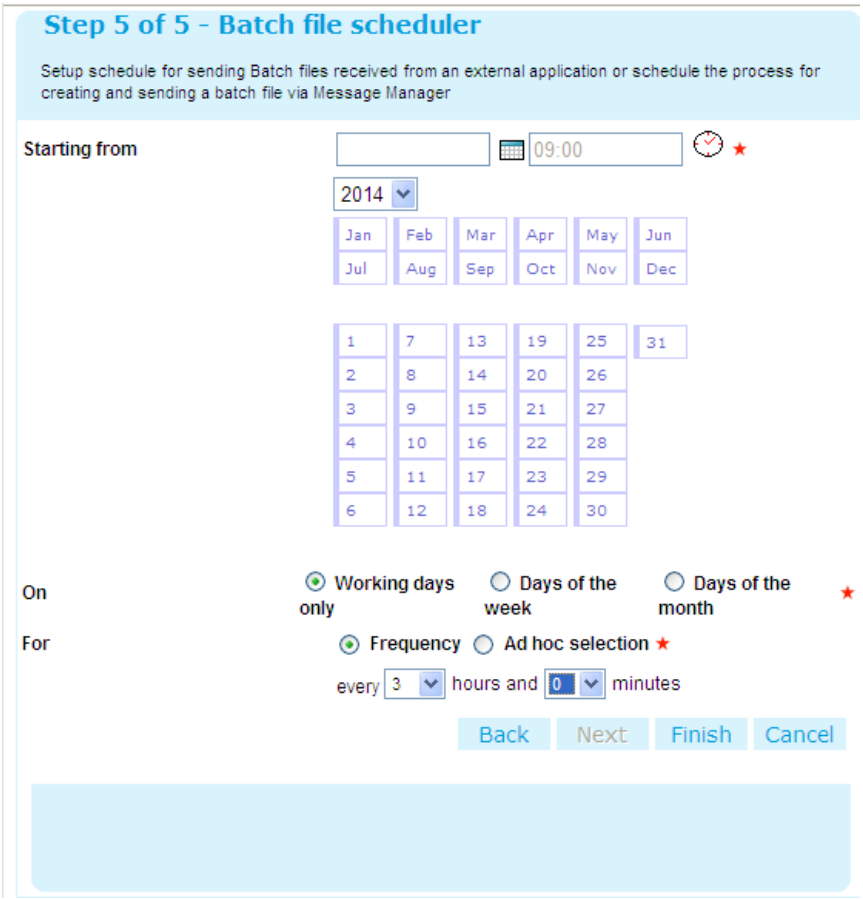
Although optional, it is expected that FusionBanking Payment Manager will poll a specified queue for the response from the destination system. The user is able to specify how often the response queue is checked in milliseconds, seconds and minutes, with a maximum number of retries. The check for response information has the default values:





Batch file scheduler

The schedule is used for sending received processed batch files and for creating and sending batch files containing individual messages held in the Batchable message queue field. The scheduler uses the generic scheduler provided by FileAct.



Configuring Message Templates

Templates may be used, during message creation and modification, to constrain user input at the individual message field level. Each template is assigned to a specific security role.

When using templates for message creation, you can specify:

- Pre-defined field values
- Whether other fields **must**, **may** or **may not** be entered when the template is used.

Templates used for message modification do not specify pre-defined field values, only whether fields **must**, **may** or **may not** be entered when the template is used.

When the same template is used for both message creation and modification, during modification, any pre-defined values will be ignored and will not cause the existing values in the message to be overridden.

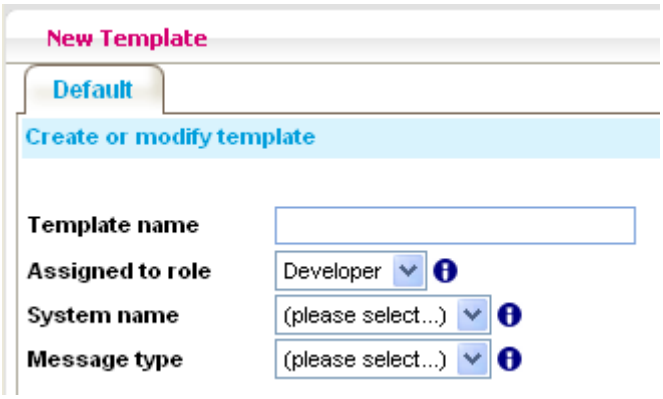
To access the template functions you must have the Maintain Message Template permission assigned.

From the main menu, select Administration >Template Editor.

The Template Navigation pane on the left lists all existing templates associated with user roles.

To create a new template:

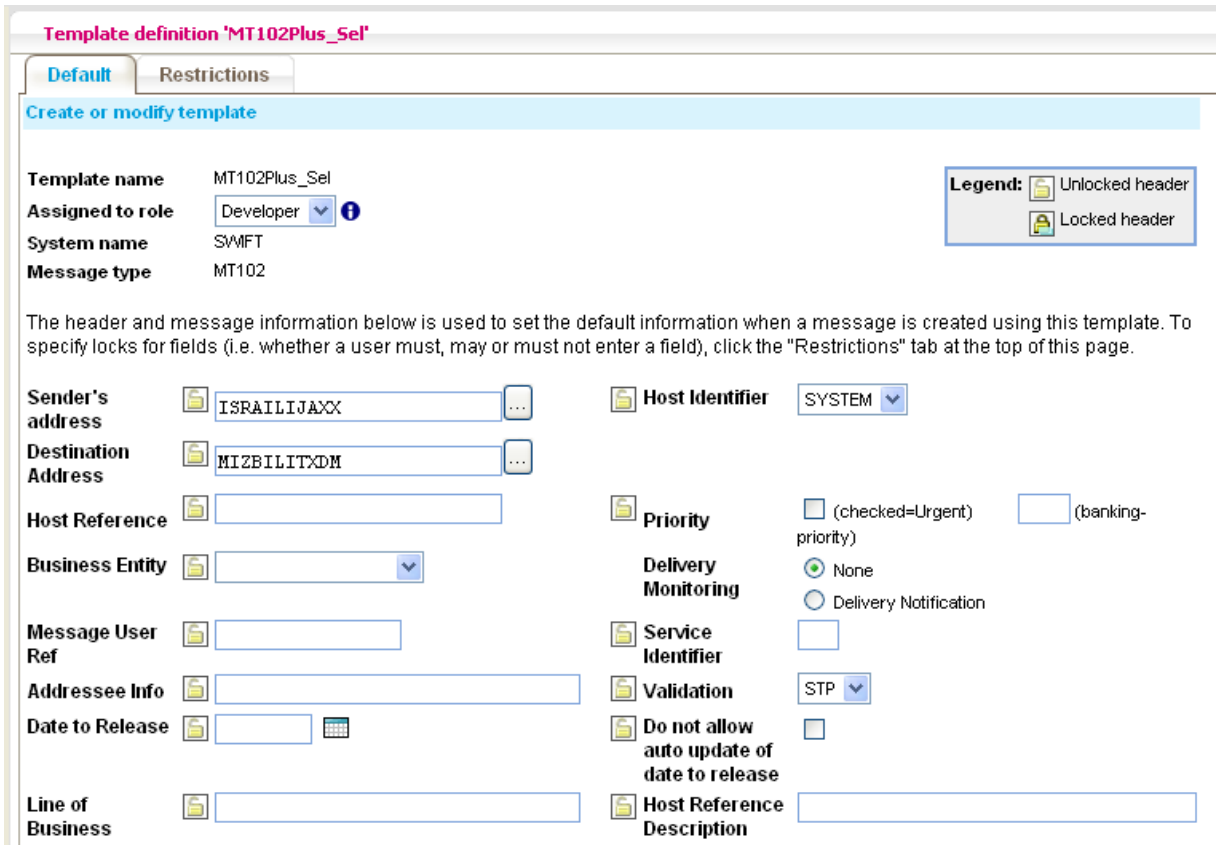
1. Click **New Template**. The New Template form will be loaded on the right hand pane.
2. Fill in the form on the left hand pane.



Field	Description
Template Name	Enter a name for the template.
Assigned to Role	Select a role. The roles included in the drop down are those that you are currently assigned to.
System name	Select for which system this message template will be used for.
Message Type	Select a message type.

The Explorer will then load the main template default form according to the format of the message type specified in the previous screen.

The following is an example of a template which has been created previously.



Users can then add any default data to the fields of the message as required and lock these fields (see below).

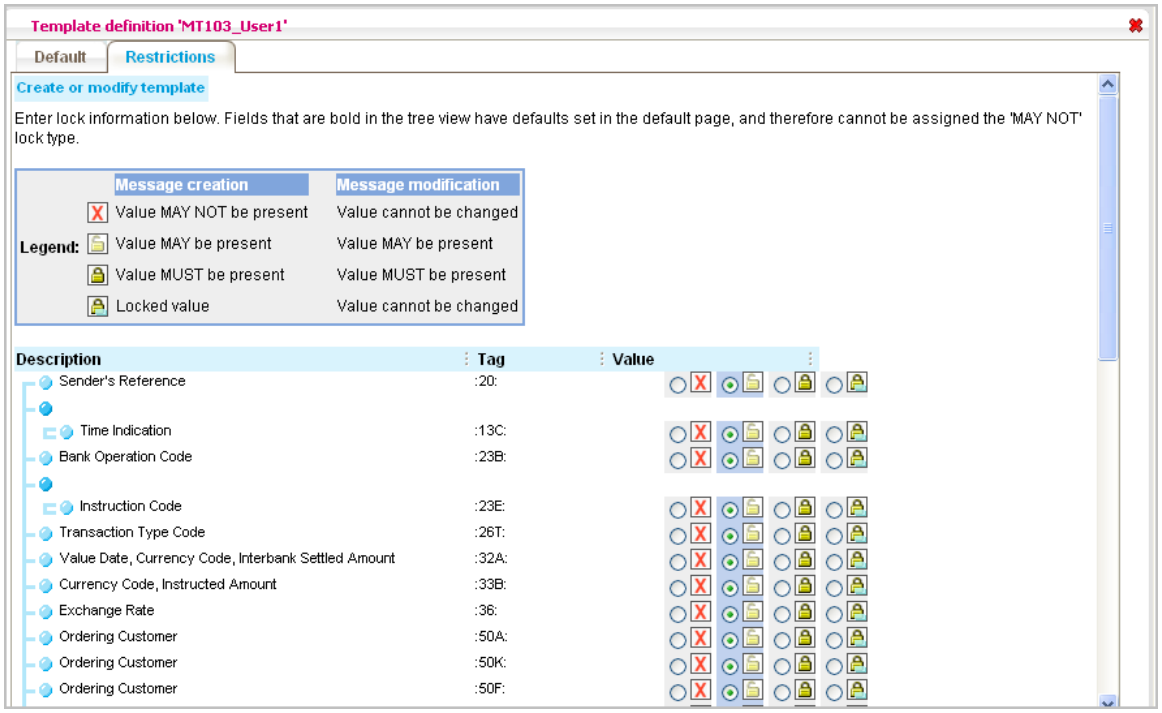
Note that the **Default** tab is only used for message creation. If this template is used in message modification, any pre-defined values are ignored.

The fields are as follows:

Field	Description
Sender's address	Enter the sender's BIC address or select it from the adjacent BIC picker.
Destination address	Enter the destination BIC address or select it from the adjacent BIC picker.
Host reference	Enter a reference which can be subsequently used to search for the host and payment.
Host identifier	Select the host system.
Business entity	Enter the business entity associated with the payment.
Message user ref	Enter a reference which can be used by SWIFT for retrievals and to identify the message in associated system messages and acknowledgments. If not entered, SWIFT will use the Transaction Reference (field :20: or :20C:SEME of the text block of user-to-user FIN messages).
Addressee info	A reference which can be subsequently used to search for the addressee.
Date to release	The date the payment should be released.
Priority	The left hand box indicates the payment is urgent. The right hand box allows a user to assign priority for queued payments that require manual intervention. It can

Field	Description
	be useful for prioritising urgent and/or important business. The priority is in the range one to ten, one being the highest and ten the lowest.
Date to release	Enter the date the payment is required to be released. A check will be undertaken when the payment is submitted to determine if this is a non-working day.
Do not allow auto update of date to release	This is used if you do not want to automatically change the release date when changes have been made to relevant static data that influence the calculation of release date (e.g., changes made in holiday data, settlement cutoff, etc).
Line of business	Enter the line of business associated with the payment.
Host reference description	Free format text to provide more information for the host.

When this is complete, you can use the **Restrictions** tab to allow users to modify default data, lock fields to disallow change of default data or to hide optional fields.



Here the message fields are arranged in a tree view. On the right of each field are four lock types, one of which may be chosen by clicking the radio button against it.

The options for locks are described below:

Symbol	Use in Message Creation	Use in Message Modification
X	Value may not be present. When this lock option is specified against a field in the template, a default value may not be specified in the Default tab. When this template is used during message creation, input to the field is disabled and the text "This field cannot be entered due to template restrictions" is displayed. This lock type is not available for mandatory fields.	Value cannot be changed. Any existing value will be displayed but input to this field is disabled.

Symbol	Use in Message Creation	Use in Message Modification
	Value may be present. During template definition, the user has the option to enter a pre-defined value for this field. During message creation, the user has the option to: • Leave the field blank (except for mandatory fields). • Fill in a value for this field • Change the value if a pre-defined value exists. This is the default lock type.	Value may be present. The user has the option to: • Leave the field blank (except for mandatory fields). • Fill in a value for this field • Change existing value, if present. This is the default lock type.
	Value must be present. During template definition, the user has the option to enter a pre-defined value for this field During message creation, the user must not leave the field undefined. This is particularly useful if a value is required for optional fields.	Value must be present. The user must not leave the field undefined. This is particularly useful if a value is required for optional fields.
	Locked value. During template definition, the user has the option to enter a pre-defined value for this field. During message creation, the user cannot change the pre-defined value set for this field if one exists. The field is disabled for input.	Value cannot be changed. Any existing value will be displayed but input to this field is disabled.

Click **Save Template** to save the template.

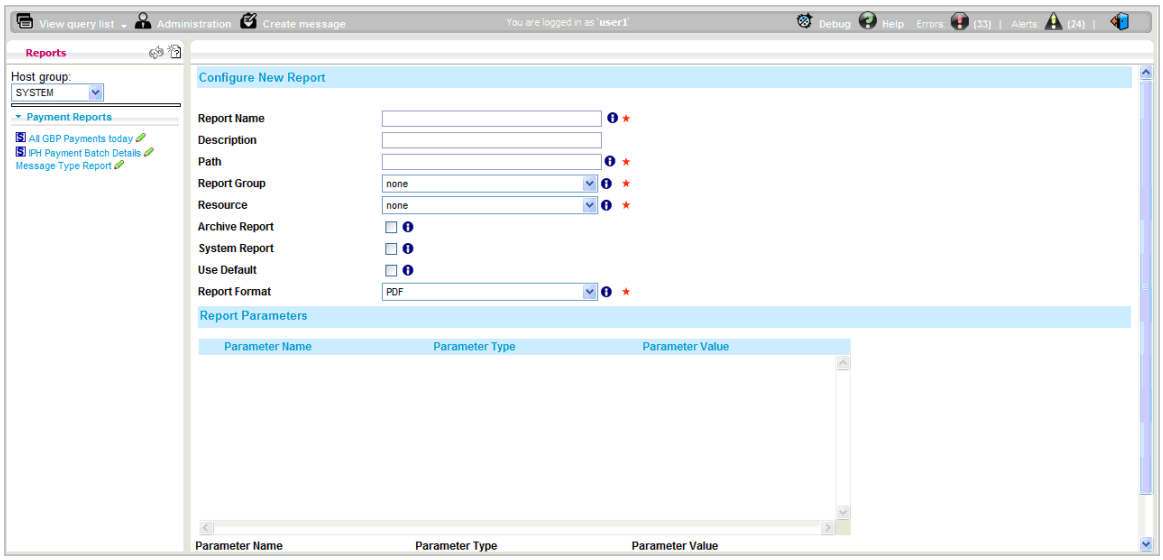
When any of the above lock types is used on a field enclosed in a repeat block, the restriction is applied to the field for all instances of the repeat block.

Importing Jasper Reports

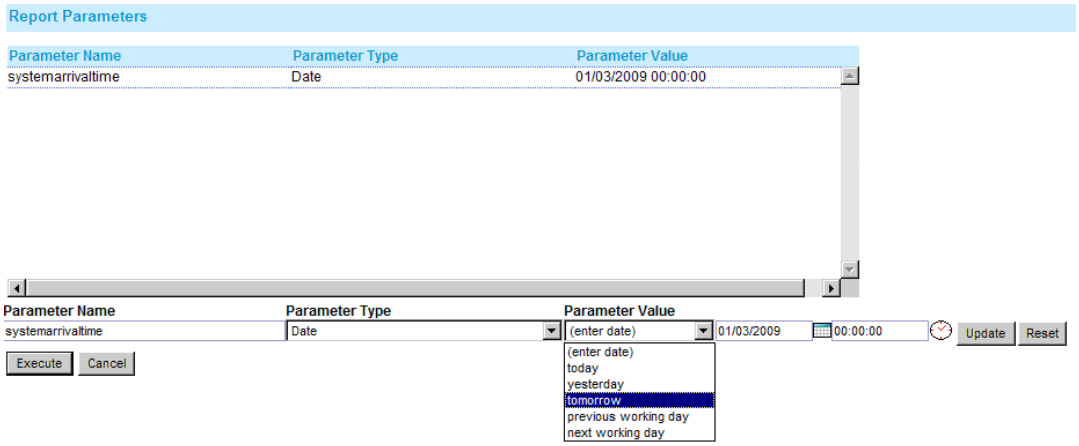
The reports menu can be accessed, if you have the necessary permissions, from the menu option **Administration** > **Reports**.

To import a new report:

1. Click **New Report**  .
2. Enter the details as described in the table below.



Field	Description
Report Name	User friendly name for an external report.
Description	Optional description.
Path	Complete and exact path and report name of compiled report in jar file including '.jasper' extension and leading forward slash.
Report Group	The report group under which the report will be displayed.
Resource	The resource that the report is based on. Can be Message or Audit. Required in order to propagate view restrictions on the displayed content. Refer to the section on Security at the end of this document for more details.
Archive Report	If checked, the report is executed against the Archive database. All other aspects remain the same.
System Report	Toggles visibility. If checked, all authorized system users can view this report.
Use Defaults	This checkbox is for user convenience and can be used for access control. If checked, a report is executed without prompting for parameter values. One click execution for reports that either don't have parameters or have parameters that don't require changing such as currency and amount limits. Another use could be to limit users with execute only permissions from overriding/modifying configured report parameters. Needless to say, for this option default values must be provided for all parameters.
Report Format	Desired output format of the report.



The user interface also allows for the definition of parameters that are expected by a Jasper report. At runtime, the parameters defined here are passed to the Jasper API so names must match exactly. Default values for parameters can be provided at design time and can be of string, numeric and date types. For specifying date and time values, there are calendar and time pickers. Furthermore, to allow 'one click' execution of reports, for date parameters, there are placeholder values for 'today', 'yesterday', 'tomorrow', 'next working day' and 'previous working day'. Working day values are calculated based on the market centre associated with a host group, which is in turn is associated with a report. If a report is defined for all host groups it does not have a host group assigned to it from which to determine the market centre. In this special case, the currently logged in user's preferred 'timezone' is used to determine values for working days.

In addition to the parameter names needing to match exactly, for the successful execution of reports, the data types also need to be compatible. General parameter type mapping rules are as follows:

MM parameter type	Jasper parameter type
String	java.lang.String
Numeric	double
Date	java.lang.String

To modify a report, select **Payment Reports** and click **Edit** .

In Edit mode it is possible to delete a report definition. The **Delete** icon is located in the top right corner, below the **Logout** toolbar icon.

Configuring iReport

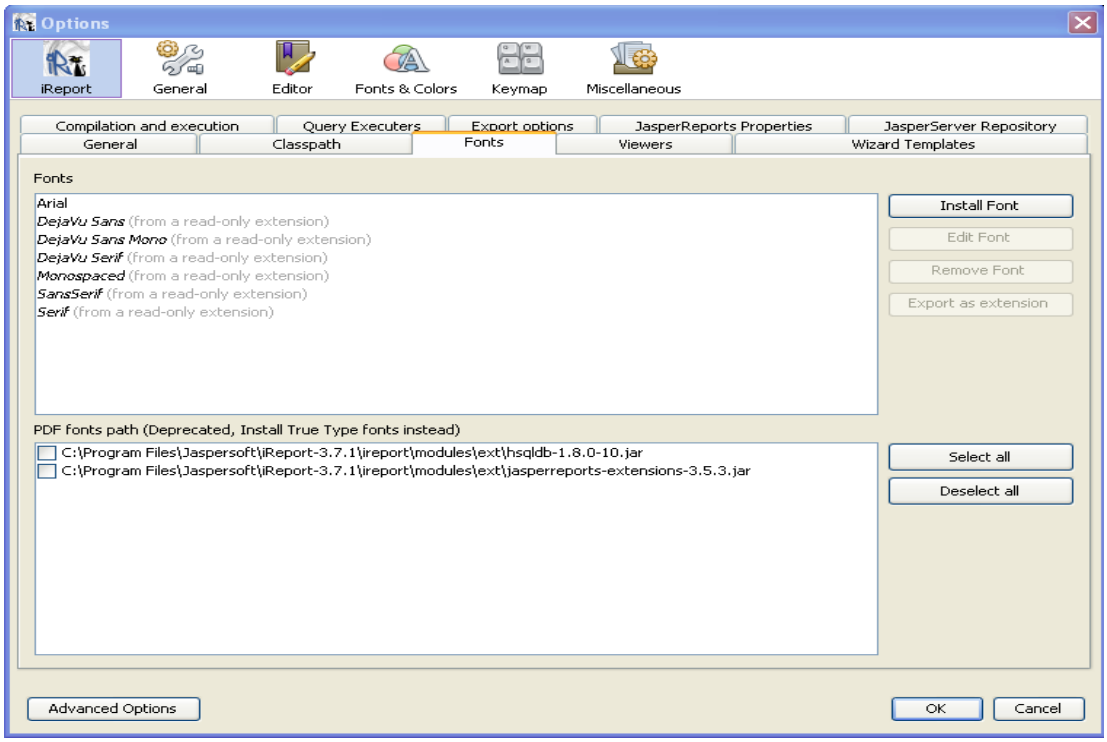
FusionBanking Payment Manager uses the iReport 3.7.1 version to support the multibtyte character in reporting. All customized reports must be compiled with this version to avoid errors on generating reports on BFPM.

In addition, iReport 3.7.1 version now uses the font extension feature for the parameters PDF font name and PDF Encoding as these were deprecated in the Text property.

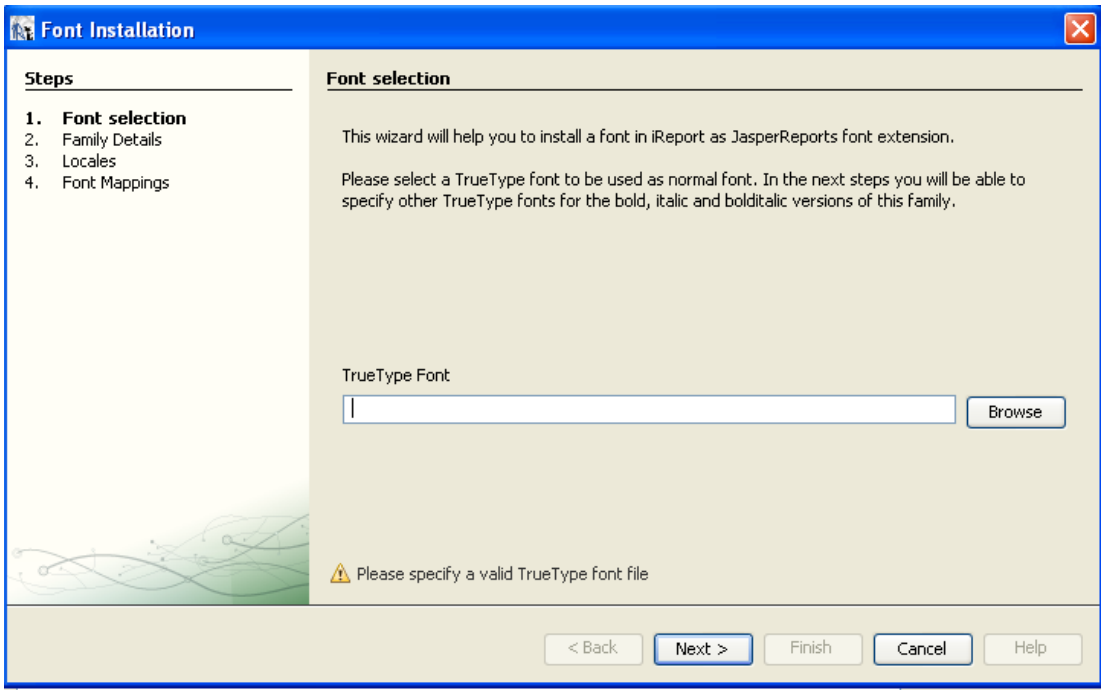
Text properties	
Font name	Arial
Size	18
Bold	☑
Italic	☐
Underline	☐
Strike Through	☐
~~Pdf Font name is now deprecated.~~	Helvetica
Pdf Embedded	☐
~~Pdf Encoding~~	CP1252 (Western European...
Horizontal Alignment	Left
Vertical Alignment	Middle
Rotation	None
Line Spacing	Single
Markup	none
~~Report font~~	

Jasper Reports have built-in font extension only for the Dejavu fonts. To use other fonts on your report that will supports Multibyte character, you must do the following:

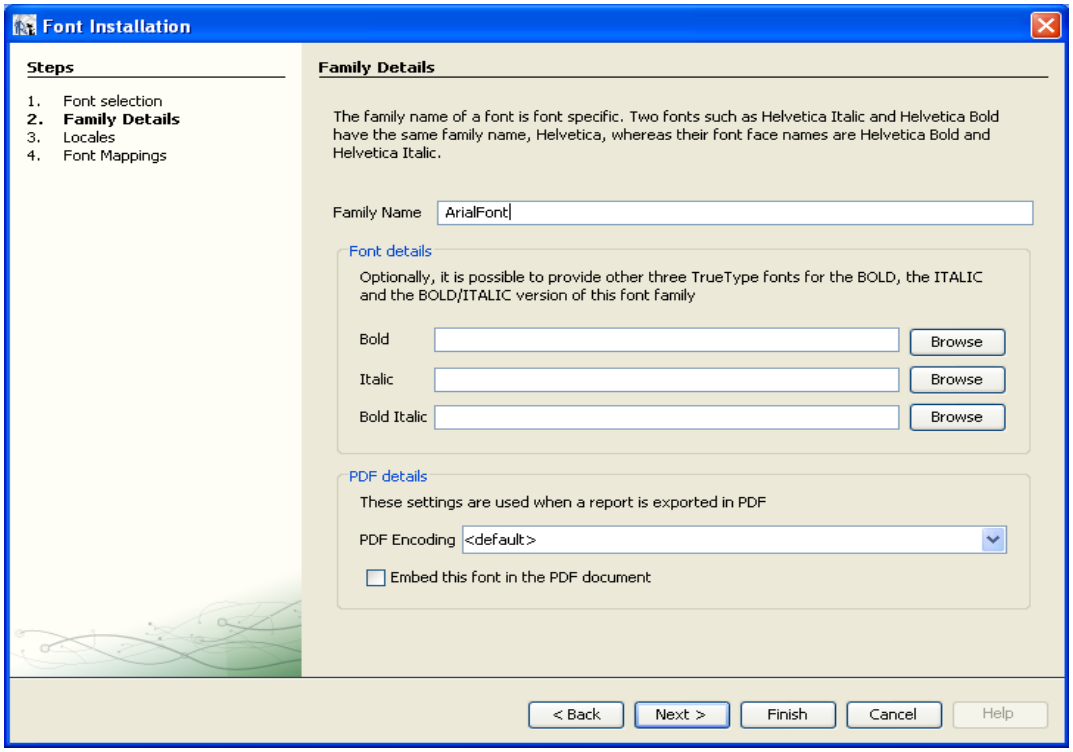
1. Go to **Tools > Option > Fonts tab**.



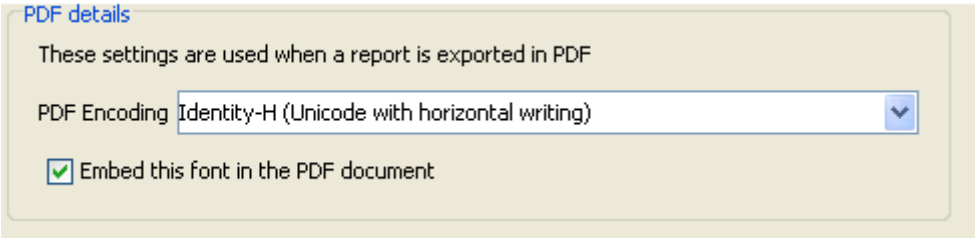
2. Click **Install Font**.



3. Browse on the True Type font to be used. Make sure that the True Type font supports the multibyte character you used in your report.
4. After selecting, click **Next**.



5. Fill in the Family name and font details. For PDF details, the PDF encoding should be set to “Identity-H (Unicode with horizontal writing)”.
6. Tick **Embed** this font in the PDF document.

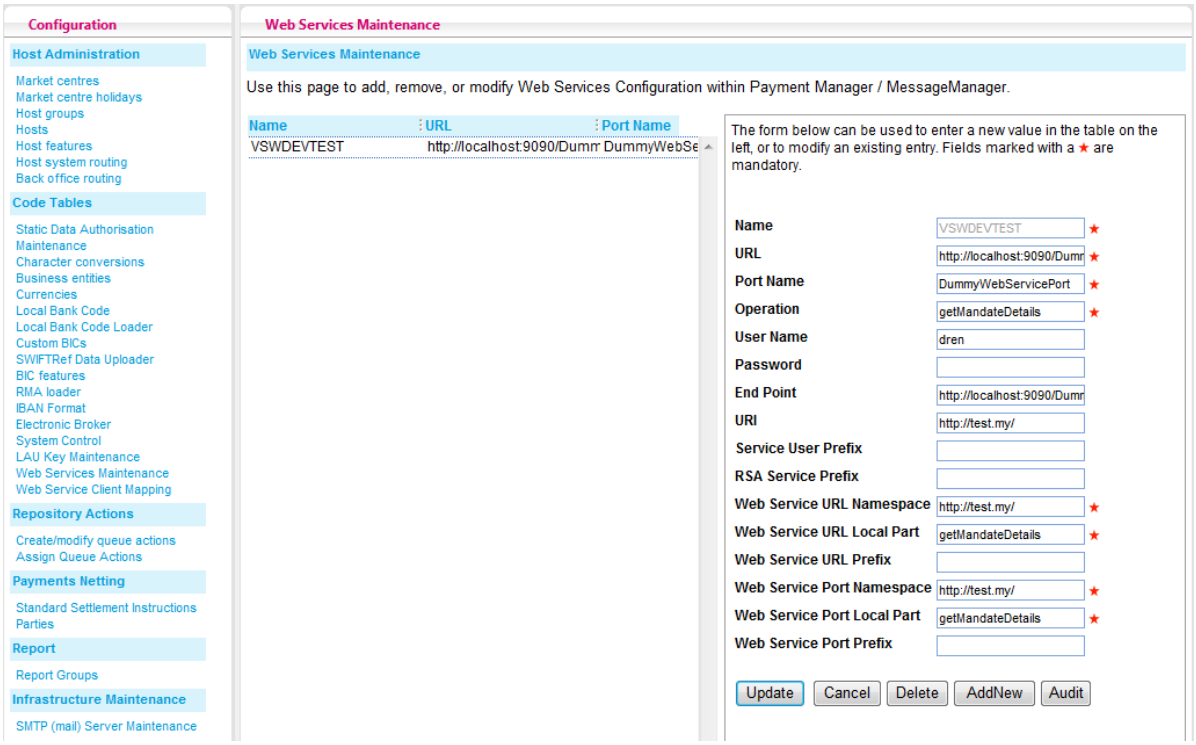


7. Click **Finish**.
8. To use the installed font, go back to the fonts tab, select the font and click **Export as Extension**. It will generate a *.jar file. Put the jar file on the directory where the compiled jasper report is located.

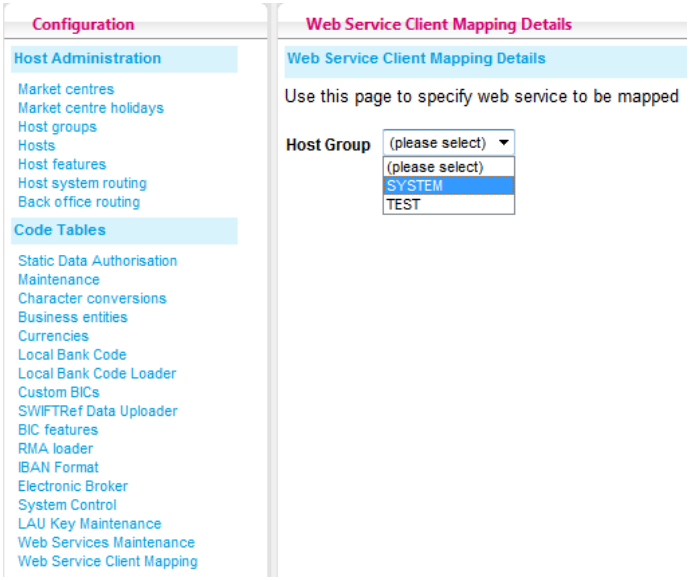
Configuring Credit / Debit Mandate Lookup

To enable the credit/debit mandate lookup:

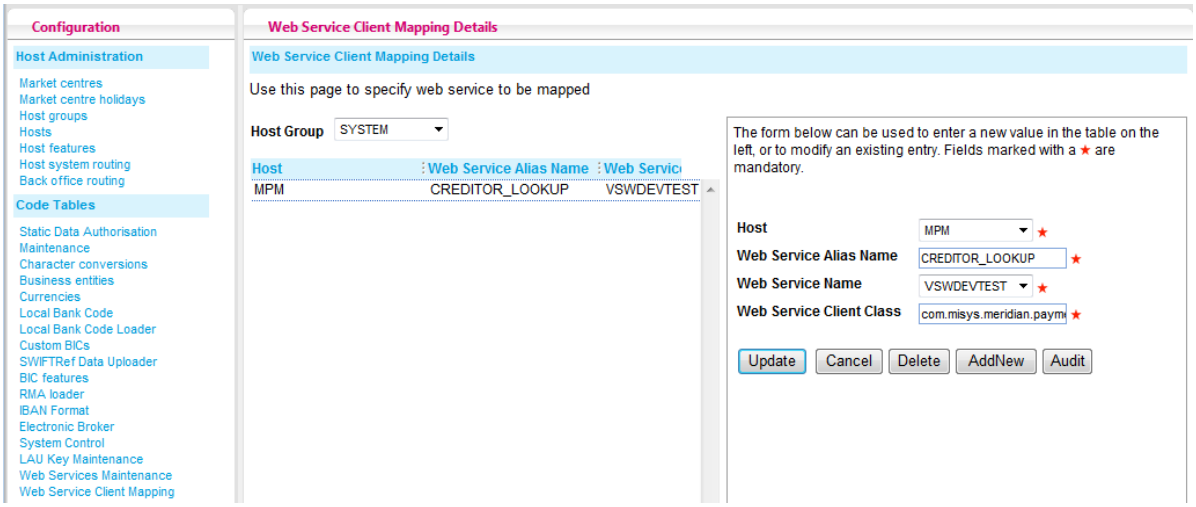
1. Go to **Administration > Configuration > Web Services Maintenance**.
2. Set up a web service. See Web Services Maintenance.



3. Then go **to Web Service Client Mapping** and select a Host Group, e.g. System.

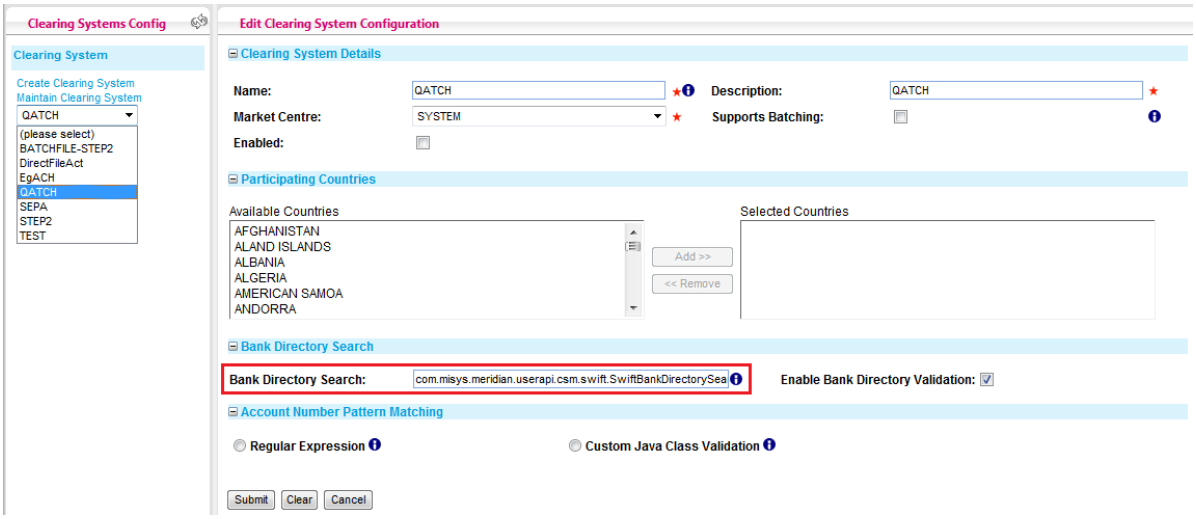


4. Configure the **Web Service Client Mapping Details**. See section 4.3.2.15.



> For credit mandate type, use the alias name **CREDITOR_LOOKUP**. For debit mandate type, use the Alias Name **DEBTOR_LOOKUP**.

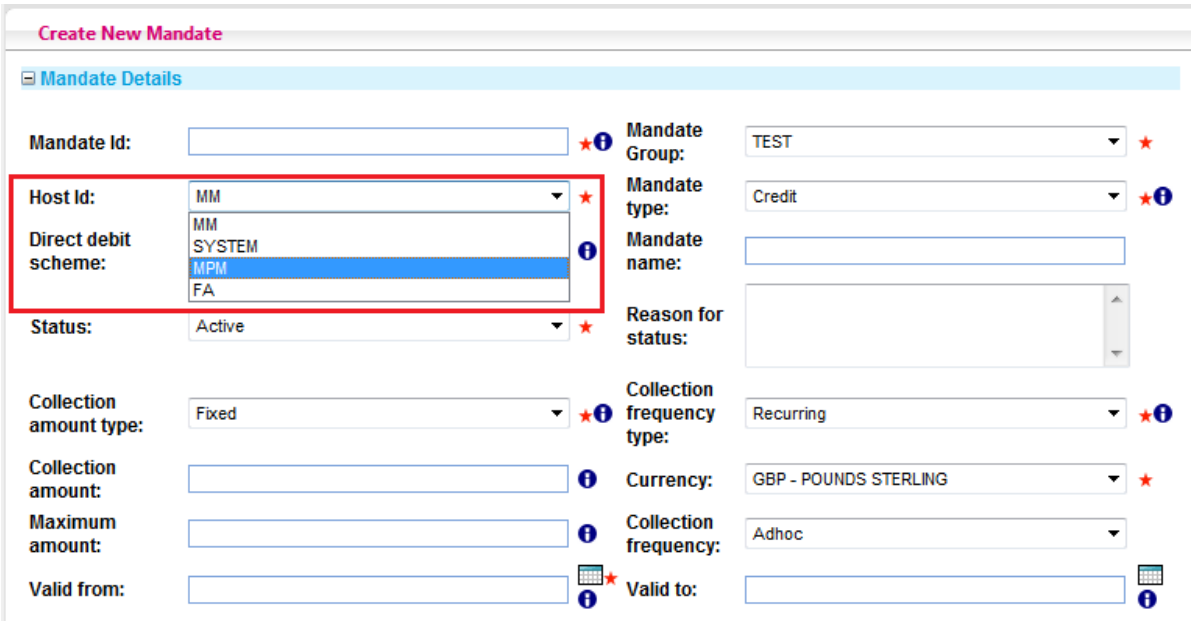
5. Go to **Administration > Clearing System** then select a Clearing System, e.g. QATCH.



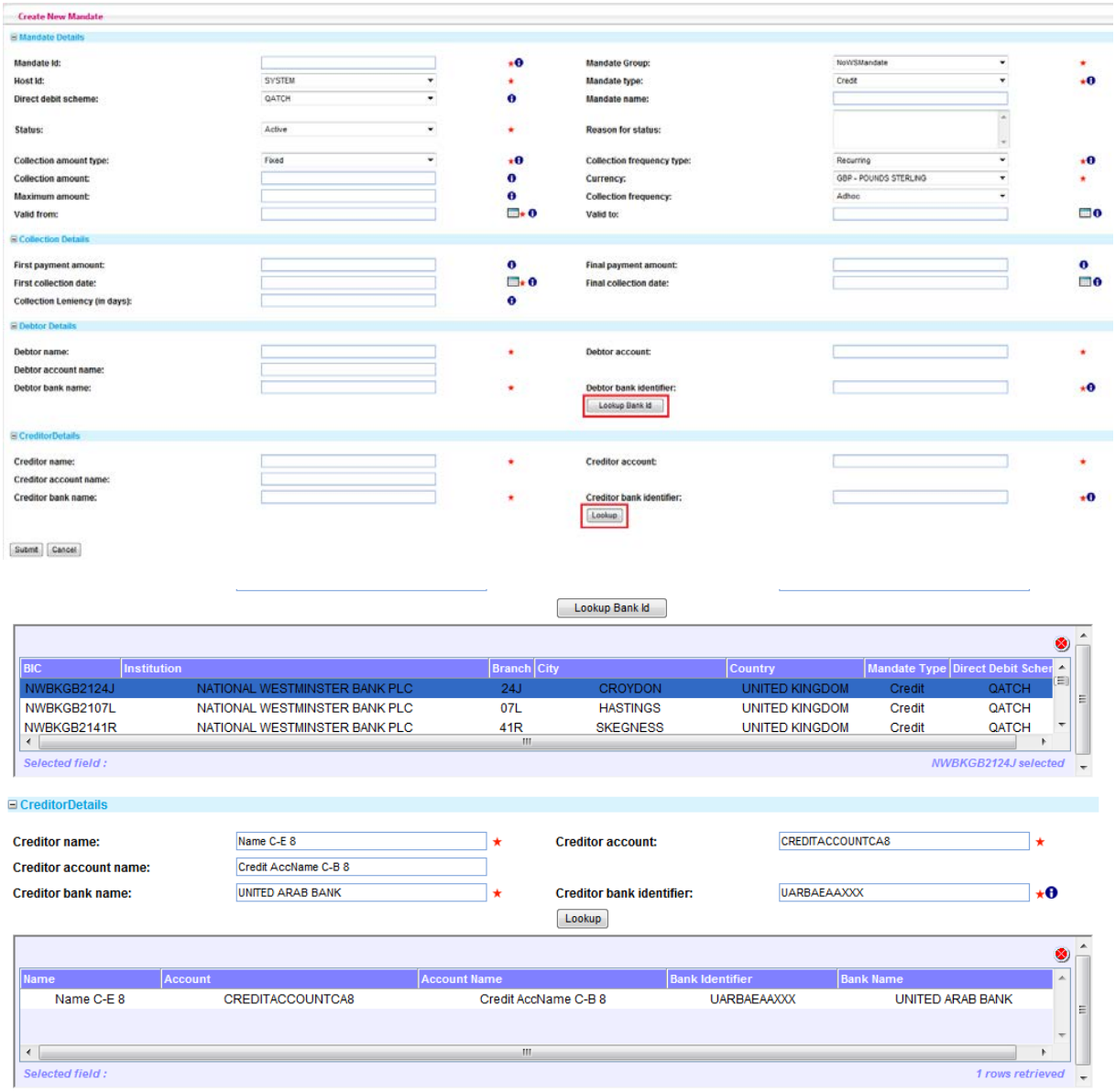
> Only QATCH and SEPA are available, Example, for QATCH, edit the **Clearing System Configuration** and add the implementing class in the **Bank Directory Search** field then tick **Enable Bank Directory Validation**.

6. Click **Submit** then **Done**.

To verify if the configuration was successful, go to **Administration > Mandates**, select Host Group and click **New Mandate**. At the Host Id field, select the Host that was used in step 4. Then select a Direct debit scheme.



The Lookup Bank Id and Lookup buttons should appear as in the screenshot below. The screen should look like the following.



For more information on how to use Lookup Bank Id and Lookup, please refer to *FusionBanking Payment Manager 5.1.1 User Guide*.

Configuring Clearing Systems

The Clearing Systems allows the administrator to add or modify clearing and settlement mechanisms (CSMs) where a payment is to be processed by a CSM. The CSM Extended Properties provides the administrator additional configuration properties to assign a property name and value to its default value.

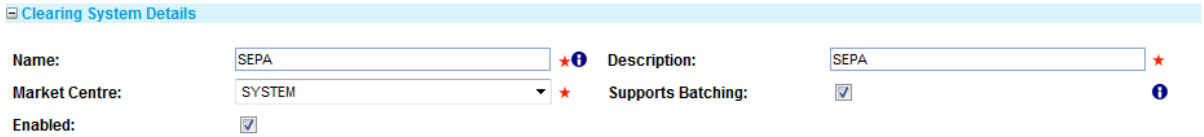
To enable this, first the following permissions must be added to a user or role:

- Create Clearing Systems
- Maintain Clearing Systems
- View Clearing Systems

To create a clearing system:

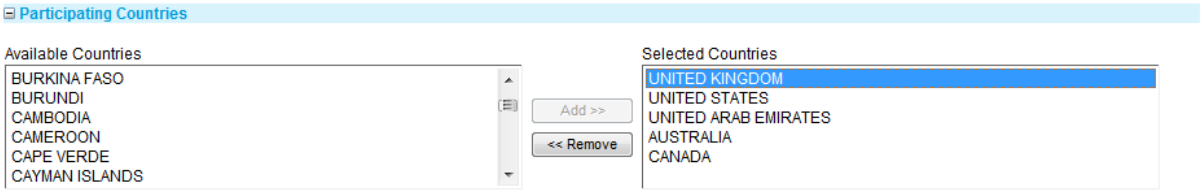
1. Go to Administration > Clearing Systems > Create Clearing Systems.

2. Enter the values for the following fields:
    a. Clearing System Details



Field	Description
Name	Name of the CSM
Market Centre	The market centre that will be used for the CSM
Description	Description of the CSM
Supports Batching	Tick this if the CSM will support batching of messages.
Enabled	Tick this to enable the CSM.

    b. Participating Countries



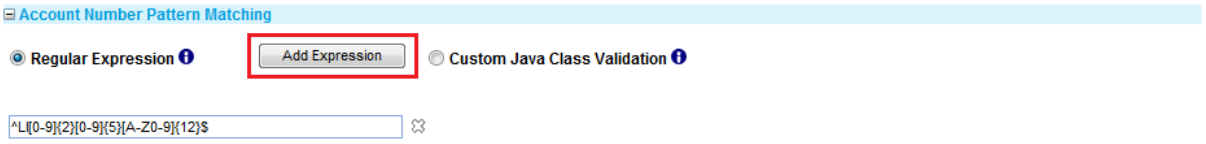
This allows the user to select counties where the CSM will be applied.

    c. Bank Directory Search

Field	Description
Bank Directory Search	Holds the value for the implementing class for the bank directory information for creditor/debtor mandate.
Enable Bank Directory Validation	Tick this to enable bank directory validation.

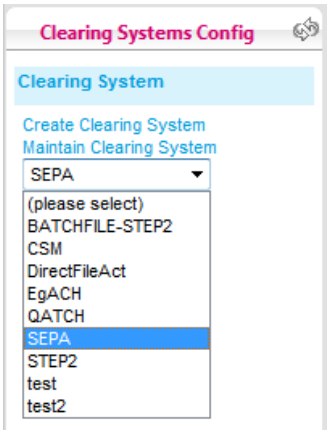
    d. Account Number Pattern Matching

    Users can either use Regular Expression or Custom Java Class Validation.



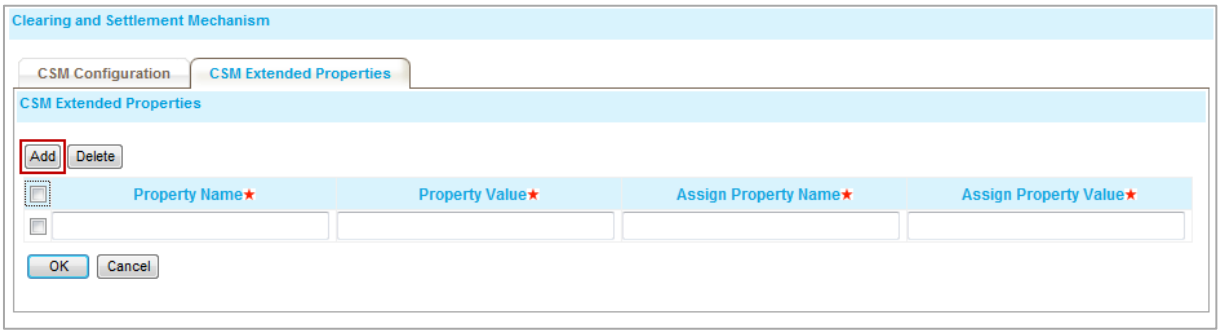
- Regular Expression – Click **Add Expression** then add the value format where the IBAN data will be validated against with.
- Custom Java Class Validation – A java class that can be used for data validation. This is normally configured during system implementation.
  Example: com.misys.meridian.runtime.filter.csm.validation.accountNumber.CSMIBANValidator

3. Click **Submit**.
4. The newly created CSM must appear in the **Maintain Clearing System** dropdown.

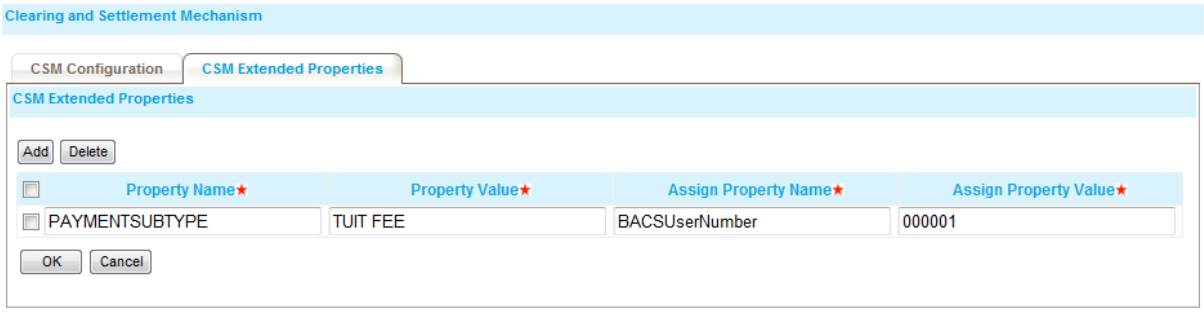


To configure CSM Extended Properties:

1. Go to Maintain Clearing System dropdown and choose one among the available CSMs.
2. Click the CSM Extended Properties tab.
3. Click add to insert a new field



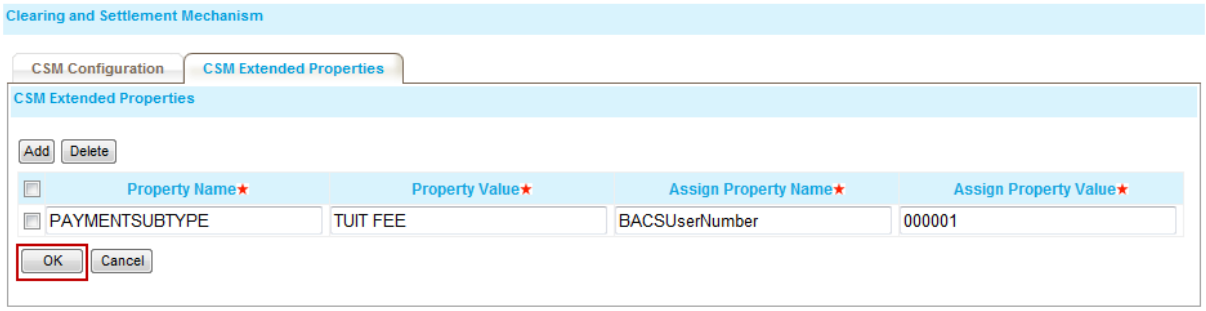
4. Enter the values for the following fields:
    a. CSM Extended Properties



Field	Description	Allowed Characters	Max Length
Property Name	Field found under the message's Credit Transfer Instruction Information Purpose Proprietary. Default value is "PAYMENTSUBTYPE".	Alphanumeric	100
Property Value	Value of the Property Name.	Alphanumeric including . , - (space)	200

Assign Property Name	User defined field that will be enriched in the batched message if matches the Property Value	Alphanumeric	100
Assign Property Value	Value of the User Defined field.	Alphanumeric including . , - (space)	200

5. Click OK.



Chapter 5 Configuring Compliance Watch List Processing

FusionBanking Payment Manager can be configured to interface to Fircosoft OFAC Integration Suite version 4.2, a comprehensive watch-list checking solution which works by checking that a pending payment is not destined for a party on a watch-list. Based on this feedback, the client application can automatically hold a potentially 'bad' payment, and alert a supervisor who can choose to make the payment anyway, over-ride the watch-list check, or cancel the payment. The workflow is used to control the flow of payments to Watch List Checking and subsequent manual decision-making processes within BFPM.

The components required to be set up in the BFPM project in order to implement Watch List Processing are described in the *FusionBanking Payment Manager Implementation Guide*.

Chapter 6 Configuring Target2 Processing

Background

FusionBanking Payment Manager will route payments via the Target2 Real-Time Gross Settlement system if the BankFusion Meridian project is set up such that the payments pass through a node on which the appropriate filter has been configured.

SWIFT will route a message via Target2 if it is an MT103 or an MT202, is in the Euro currency, and various fields are set on it. The filter sets these fields for Euro MT103s and MT202s.

Configuring the filter

As shipped in the core project, the filter's name is *Target2Filter*, which is of filter type *RTGSFilterType* (where "RTGS" is Real-Time Gross Settlement). However, if you are adding it to another project, the class name is *com.misys.meridian.runtime.filter.csm.target2.RTGSFilter*. The filter type and filter name can be anything, though we recommend using *RTGSFilterType* and *Target2Filter*, as above.

The following fields need to be set on the filter:

Field name	Meaning	Notes
RTGS Detector class name	A class which implements the *com.misys.meridian.userapi.csm.rtgs.RTGSDetector* interface	If not specified the class *com.misys.meridian. userapi. csm.target2.DefaultTarget2Detector* will be used.
RTGS Directory Lookup class name	A class which implements the *com.misys.meridian.userapi.csm.rtgs.RTGSDirectoryLookup* interface	
RTGS Mapper Factory class name	A class which implements the *com.misys.meridian.userapi.csm.rtgs.RTGSMapperFactory* interface.	

The switchable features

The following switchable features interact with this functionality. See the Switchable Features Guide for full details of the features.

- CORE000038: If enabled the Target2 priority for MT202s will be set to High (value = NYNN)
- CORE000044: process MT103 payments via Target2.
- CORE000045: process MT202 payments via Target2.
- CORE000047: applicable to domestic MT13 or MT202 for settling via Target2.
  - takes 2 optional parameters:
    - OPTIONALPARAMETER1 = List of country codes (comma separated)
    - OPTIONALPARAMETER2 = List of line of business (comma separated)
- CORE000048: if enabled payments from Equation will not be processed via Ratget2.
- CORE000065: Skip Field 57A of MT202s to determine the Target2 destination BIC

- CORE000080: if enabled the Target2 priority for MT103s will be set to High (Value = NYNN)

Appendix A - Parameters list for security complex permissions builder conditions

Permission	Left operand	Operator	Right operand
Originate message	Type	equals not Equals like not like starts with not starts with ends with not ends with	Field 1: Literal Value; OR Field 2: Dropdown selection of all Message types configured in the project
		In not in	Comma-separated range of values.
		between not between	Field 1: Literal value – start of range; and Field 2: Literal value – end of range
		Is blank Is not blank	n/a
Use template to modify a message	All message properties. See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*
Repair a message	All message properties. See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*
Modify a message	All message properties. See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*	See the *Payment Manager User Guide*
Define which messages are visible	All message properties. See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*
Send from BIC Address	BIC Institution Branch	equals not Equals like	Literal Value

Permission	Left operand	Operator	Right operand
	City Country	not like starts with not starts with ends with not ends with	
		In not in	Range of values separated with a comma
		between not between	Field 1: Literal value – start of range; and Field 2: Literal value – end of range
		Is blank Is not blank	n/a
Limit visibility for audit records	All audit properties. See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*	See the *FusionBanking Payment Manager User Guide*
Perform custom actions	Custom action	equals not Equals like not like starts with not starts with ends with not ends with	Literal Value
		In not in	Comma-separated range of values
		between not between	Field 1: Literal value – start of range; and Field 2: Literal value – end of range
		Is blank Is not blank	n/a
Select visible host groups for user	Host group	equals not Equals like not like starts with not starts with	Literal Value

Permission	Left operand	Operator	Right operand
		ends with not ends with	
		In not in	Comma-separated range of values
		between not between	Field 1: Literal value – start of range; and Field 2: Literal value – end of range
		Is blank Is not blank	n/a

Appendix B - Payments Netting

Overview

The payments netting functionality within FusionBanking Payment Manager allows users to combine a number of payment (MT202s, MT103s) and receive messages (MT210s) with similar settlement instructions to be netted together, producing a 'netted' set of messages which are then sent out to SWIFT. By default this functionality is switched off and 'invisible' within BFPM. To enable this functionality please contact your Account Manager.

This section covers all the aspects of the Payments Netting solution.

Netting Message Types

Two messages types, defined within the SWIFT system are the main drivers for the Netting functionality. Those message types are:

- CASHFLOWP (pay)
- CASHFLOWR (receive)

The CASHFLOWP message embodies a payment message and is similar to the standard SWIFT MT103 message. The CASHFLOWR message is similar to the 'Notice to Receive' message; the SWIFT MT210.

Both message types are given an InternalMessageType of 'N' to identify them as 'Netting Messages'. They share the same headers as other messages within the SWIFT system and as such can be persisted into the BFPM database and viewed via the FusionBanking Payment Manager GUI.

These two message types form the basis of the Payments Netting solution in that they are the source message types from which netted payment messages are produced. So, any external system feeding payments information into FusionBanking Payment Manager must utilise these two message types. This can be achieved using the FusionBanking Payment Manager Integration toolkit where bespoke Payments formats can be mapped to the CASHFLOWP or CASHFLOWR as required.

FusionBanking Payment Manager Workflow Components

The recommended Payments Netting workflow involves four nodes in the project, the names of which must be identified in the BFPM properties file (refer to Implementation Guide):

Netting Node – this MMDA node holds all the CASHFLOW messages that are available for netting. In certain cases it may be attached to the Deleted node to direct CASHFLOW messages that are manually deleted from the GUI (note that this requires the custom action "Delete" to be assigned to this queue).

Netted Node – this MMDA node holds all the CASHFLOW messages that have been netted. This means that once a set of CASHFLOW messages have been selected to be Netted in the FusionBanking Payment Manager GUI, they are sent to the Netted node to indicate that these messages have been Netted and that a Netted payment / receive has been produced. This node is assigned a default message status of "Sent".

Transmit Node – this node is where the resulting SWIFT messages are forwarded to. It is recommended that this node will have the ValidationFilter attached on the input side to allow the resulting SWIFT messages to be validated automatically. This is useful because it is possible that the SSI information selected for the Netted message may contain characters of invalid formats which would result in the message being Nacked by SWIFT.

The Transmit node also acts as a decision node to direct the message further into the workflow. The recommend set of routing decisions would be:

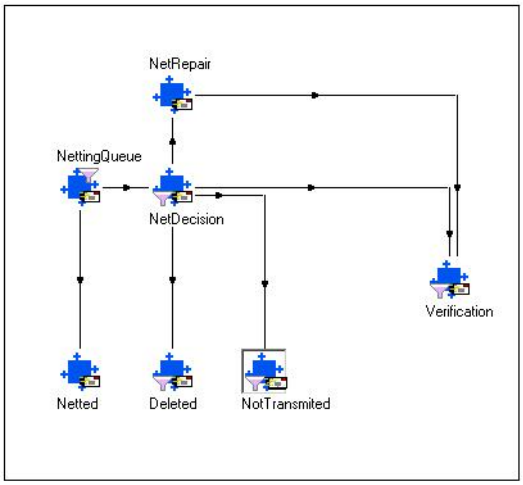
Valid messages are forwarded to the "Verification" node.

Invalid messages are sent to a Repair node.

All Netted messages with zero amount are sent to the NotTransmitted node (see diagram below).

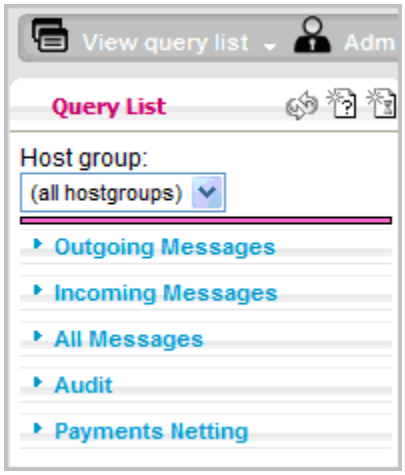
Repair Node – this node holds invalid SWIFT messages coming out of the Transmit Node. The user may build a query over this queue in order to repair the messages and get them transmitted to SWIFT. Repair functionality is covered separately within this document.

In the example workflow below, the "NettingQueue" is the Netting Node, "Netted" is the Netted Node, "NetDecision" is the Transmit Node and "NetRepair" is the Repair Node.



CASHFLOW messages and the Criteria Builder

When the Payments Netting functionality is switched on, a new Query List category is added to hold all Payments Netting queries:

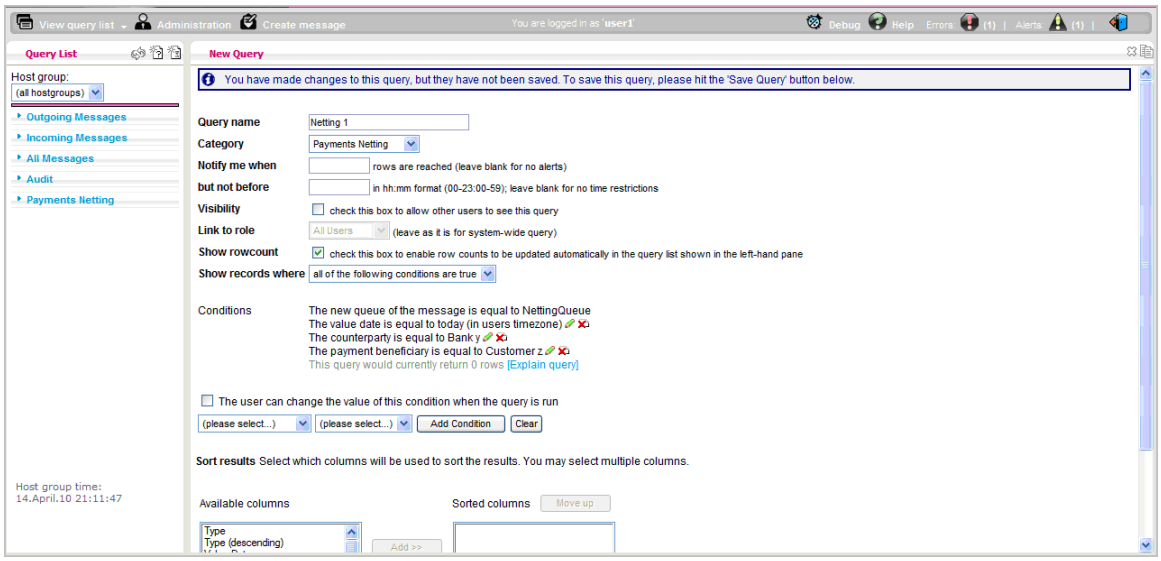


This Query List category is only available for 'Live' queries. It is not available on the End of Day or Archive query views.

This new category will only hold queries which return messages that are available on the **Netting** node (see above). By definition, messages on this node will be either "CASHFLOWP" for payment messages and "CASHFLOWR" for receipt messages. This is achieved through applying special conditions to any query created within the Payments Netting category.

Adding a Payments Netting Query

When the "New Query" icon is selected from the navigation pane, the usual query definition input form will be activated on the right hand pane. When a user selects 'Netting Messages' from the Category drop down, certain conditions are forced such that only messages on the NettingQueue are returned. There are some additional changes which are described in the table below.



Field	Description
Query Name	Field function unchanged.
Category	A new category; 'Netting Messages' has been added such that the following values are now provided in the dropdown: • Outgoing Messages • Incoming Messages • All Messages • Netting Messages
Notify me when	Field function unchanged.
Notify me but not before	Field function unchanged.
Visibility	Field function unchanged.
Show row counts	Field function unchanged.
Show records where	When Netting Messages is the selected Query Category, the dropdown will now be limited to "all of the following conditions are true". This is done to ensure that users cannot return messages which could not be Netted together. For example, this prevents a query being written that would return CASHFLOW messages that have different currencies or value dates.
Conditions	**Adding implied conditions:** If the selected Query Category is "Netting Messages, there is an implied condition that will be automatically added (ref. 8): All netting queries will run against a single queue (the Netting node as defined in the FusionBanking Payment Manager properties file) to ensure that only candidates for netting (CASHFLOW messages) are returned by the query.

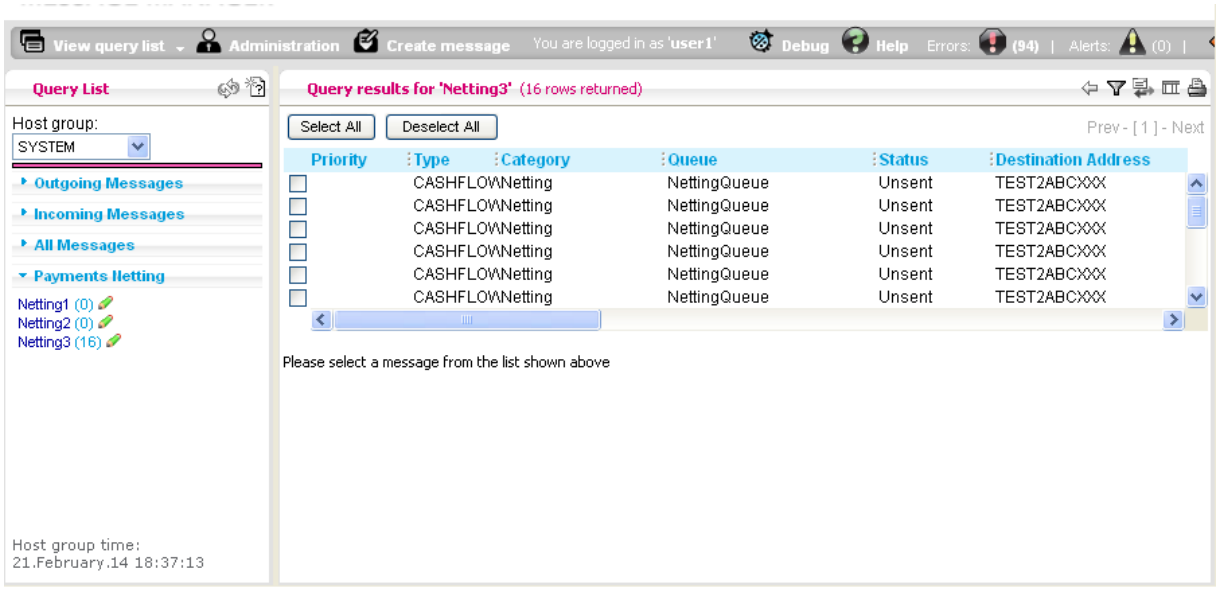
Field	Description
	When creating new netting queries, this condition will automatically be shown in the form and 'AND'ed to any other conditions that the user may add (e.g. ref. 9). You will notice that the implied condition cannot be amended nor deleted (i.e., icons are disabled). In addition this condition cannot be made promptable. **Defaulting the Value Date:** An 'inferred condition' will be applied to the Value Date. If the Value date has not been specified, it will be given a default value of "today" and will be added when the query is saved. In cases where a different date is required, the user can add the value date condition if not already present, or amend it otherwise. **Criteria restrictions:** Although the netting queries are built over the netting messages residing in the MESSAGES table, the criteria to use in ref. 13 will be reduced to allow the user to use only the properties that are relevant to netting: On the left-hand-side operand, the message properties dropdown will be limited to the following selections for the Netting Messages category: • Currency • Counterparty • Payment Beneficiary • Value Date • Message Type • Line of Business • Business Entity The only operator allowed is "equals" (=). The right-hand-side operand will remain unchanged (providing dropdowns or textbox as appropriate for the message property). For the new Counterparty property, the right-hand-side operand must show a dropdown of all party short names from the Counterparty table.
Explain Query	Field function unchanged.
Change Value checkbox	Field function unchanged.
Sort Results	To be able to sort Payments Netting query results returned, 'Counterparty' should be added to the Sort Results grid, allowing that users are able to sort results according to this field. Note that the other fields will remain in the list of sortable columns as they will still be allowed to be displayed in the query result pane, even though they are not to be used in the query conditions.
Save Query button	A few checks are done prior to persisting the query into the database: It is imperative that the Counterparty and the Currency criteria are present in the WHERE clause to ensure that the netting maintenance can select the appropriate SSIs for which these two properties play a key role. If any of these are not present, saving is not be allowed and appropriate error messages should be issued on the screen.
Cancel button	Function unchanged
Query name display	Function unchanged.
Delete Query icon	Function unchanged.

Field	Description
Create New Copy icon	Function unchanged.

Payments Netting Display & Maintenance

When a netting query is selected and run from the navigation pane, the top right hand panes will display the results of the query. The top pane will show the summary of CASHFLOW messages returned by the query. When CASHFLOW(S) are selected from the summary pane, the bottom pane will then show two tabs, the first is the Netting Maintenance tab and the other, the Message Details tab.

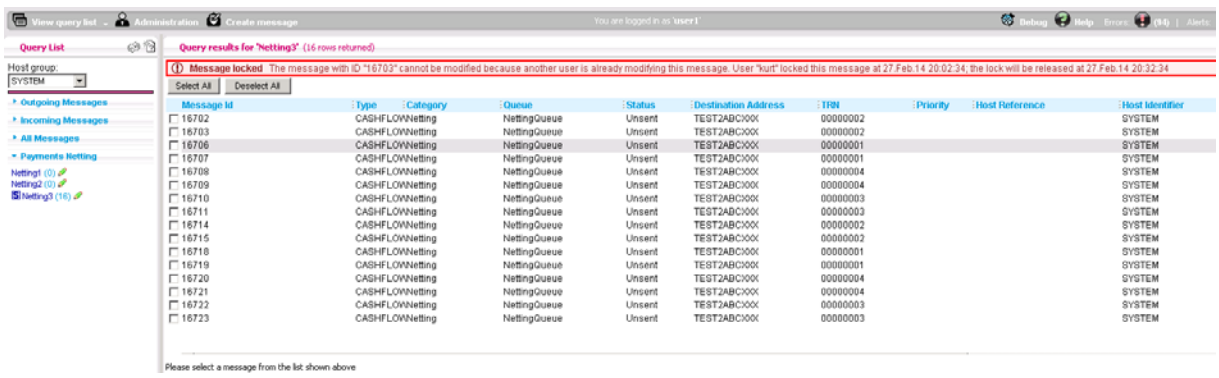
The Summary Pane



The Summary Pane is similar to the one displayed for conventional live messages queries. The differences are summarised below:

- The Filter icon on the toolbar is disabled.
- In conventional message query results, when one or more checkboxes are ticked on the results grid, the system waits for a user to perform a custom action on the selected rows (i.e., action is selected from Perform Action icon on the toolbar). For netting messages, this is replaced with an interactive display of the Netting SSI pane which will be discussed in more detail below.

To avoid selected messages from being processed by other users, a message locking mechanism has been applied. When a user tries to select a CASHFLOW message that has already been locked by another user, the selection box will not be checkable and a message will be shown as below:



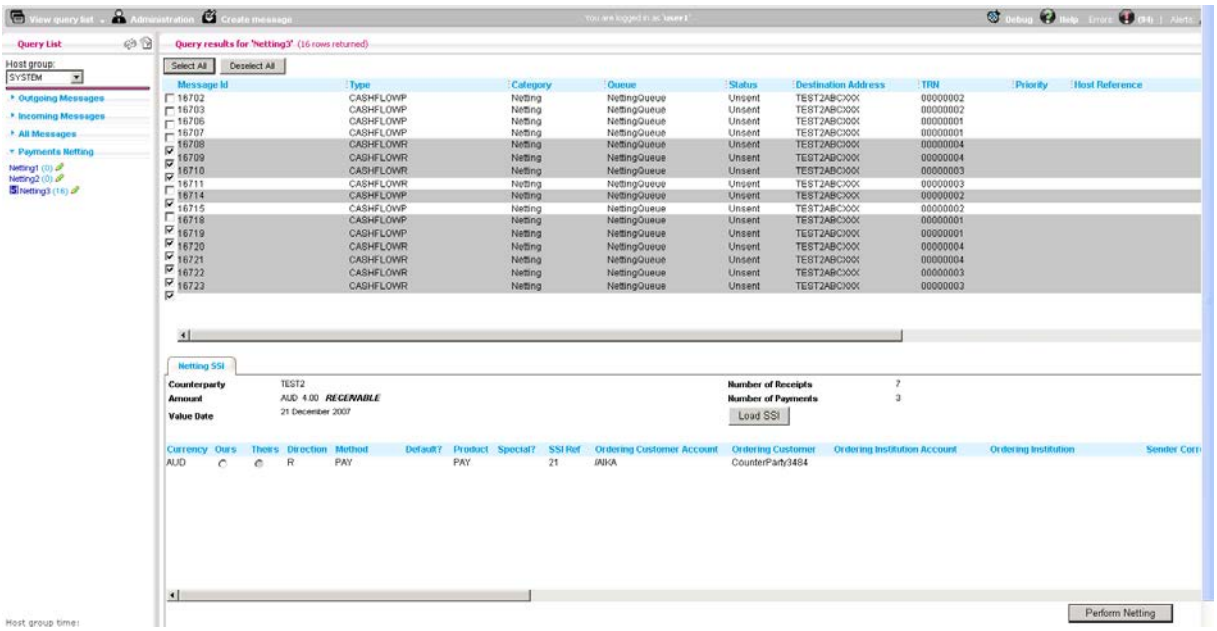
The user Id of the person locking that record is displayed on the screen. The lock on the message will be removed in any one of the following instances:

When the message locking timeout (defined in the **Administration > User Preferences**) has lapsed.

1. When the message has been manually unlocked from the Message Lock facility under the Administration dropdown.
2. When the row is deselected from the summary grid
3. When the user has decided to abandon the exercise.
4. When the netting has been completed.

Points (1) and (2) represent functionality applied for all messages, not just CASHFLOWS.

The Payments Netting Maintenance Screen



When one or more checkboxes are ticked in the summary grid, the bottom pane will show the Netting SSI tab. It is possible for the user to select only one CASHFLOW message for netting. When only one CASHFLOW message is selected, the user will go on to pick the appropriate SSI for the message in the same manner as done when netting several CASHFLOW messages. The only difference is, the resulting net message will retain its own TRN, i.e., it will not be system-generated.

This tab displays two distinct groups of information:

The Header Details

The Header information shows a summary of the netting details taken from the selected messages:

Field Name	Data Description
Counterparty	The counterparty of the selected messages.
Amount	The currency and the net amount are displayed, as well as an indication of whether it will be paid or received, depending on the selected netting messages. The net amount is calculated by finding the difference between the sum of all the payments (message type = CASHFLOWP) and the sum of all the receipts (message type = CASHFLOWR). If the calculation results in a payment, the text "**PAYABLE**" is displayed, otherwise, "**RECEIVABLE**" is displayed.

	If the calculation results in a zero amount, then the text "**PAYABLE**" is displayed.
Number of Receipts	The number of CASHFLOWR messages selected in the summary pane.
Number of Payments	The number of CASHFLOWP messages selected in the summary pane.

The Amount, Number of Receipts and Number of Payments are changed interactively as rows are selected or deselected from the summary pane.

The SSI Grid

The SSI grid below the header information shows the applicable settlement instructions for the selected CASHFLOW messages. You must click **Load SSI** in order to populate the grid. If you change the selection of messages from the Summary pane, you will need to click this button again.

SSI records are displayed in the grid according to the following rules:

- Records must have the same Counterparty, Currency and Host Group as that displayed in the header information.
- The SSI Netting flag must be set to 'Y', i.e., if 'N', the record must not be selected. This rule however will be ignored if the counterparty's record in the PARTIES table has the ISCOUNTERPARTY flag set to 'Y'.
- If the net amount is Receivable, the result will be further narrowed down by showing only those with Type = "Ours" and a Direction of 'R' (Receive) or 'B' (Both). If it is Payable, the type is not considered but the Direction will be 'P' (Pay) or 'B' (Both).
- Records must have an Effective Date that is on or before the Value Date and also an Expiry Date that is after the Value Date (Effective Date <= Value Date < Expiry Date)
- The order of output in the grid will be as follows (in ascending order unless specified): Their SSIs, Our SSIs, Default (descending, i.e. those with 'Y's first), Product Type and Method.
- The columns from the SSI table will be displayed in the following order:

Field	Data
Column Label	Data (from SSI table)
Column Label	Data (from SSI table)
Currency	The netting currency
Our	Radio button. Enabled if type of SSI is "Ours". Only one row can be selected within this column.
Their	Radio button. Enabled if type is "Theirs". Only one row can be selected within this column.
Method	SSI Method
Default	SSI Default
Product Type	SSI Product Type
Special	SSI IsSpecial
SSI Ref	SSI numeric reference
SSI Description	SSI Description

Field	Data
Ordering Cust A/c	Ordering customer account line
Ordering Customer	Ordering customer short name
Ordering Inst A/c	Ordering Institution account line
Ordering Institution	Ordering Institution short name
Sender's Corr A/c	Sender's Correspondent account line
Sender's Correspondent	Sender's Correspondent short name
Receiver's Corr A/c	Receiver's Correspondent account line
Receiver's Correspondent	Receiver's Correspondent short name
Third Reimbursement Inst A/c	Third Reimbursement Institution account line
Third Reimbursement Institution	Third Reimbursement Institution short name
Intermediary A/c	Intermediary account line
Intermediary	Intermediary short name
Account With Inst A/c	Account with institution account line
Account With Institution	Account with institution short name
Beneficiary A/c	Beneficiary account line
Beneficiary	Beneficiary short name
Remittance Info	Remittance information (first line only)
Details of Charges	Details of charges ("OUR", "BEN", "SHA")
Sender to Receiver Info	Sender to receiver info (first line only)
Remarks	Remarks (all 4 lines)

The user can scroll horizontally to view the rest of the columns. The column widths are adjustable as is the case for the Message Query Results grid.

Other Details

The Maximise icon will be made available at the toolbar which will expand the bottom pane to a larger portion of the screen. Once maximised, it will be replaced by a Minimise icon which will shrink it back to its default size.

A "Perform Net" button is available under the SSI grid. Clicking this button (when appropriate) will create the net SWIFT message. When **Perform Net** is clicked, the following checks are carried out to ensure that the required information to populate the payment/receipt SWIFT message is available:

- For a net payable, one OUR row and one THEIR row must have been selected.
- For a net receivable, one OUR row must have been selected

Any other combination of choices is disallowed and an error message is displayed on the Netting pane. Netting is still possible when the resulting amount is zero. The resulting message will have a

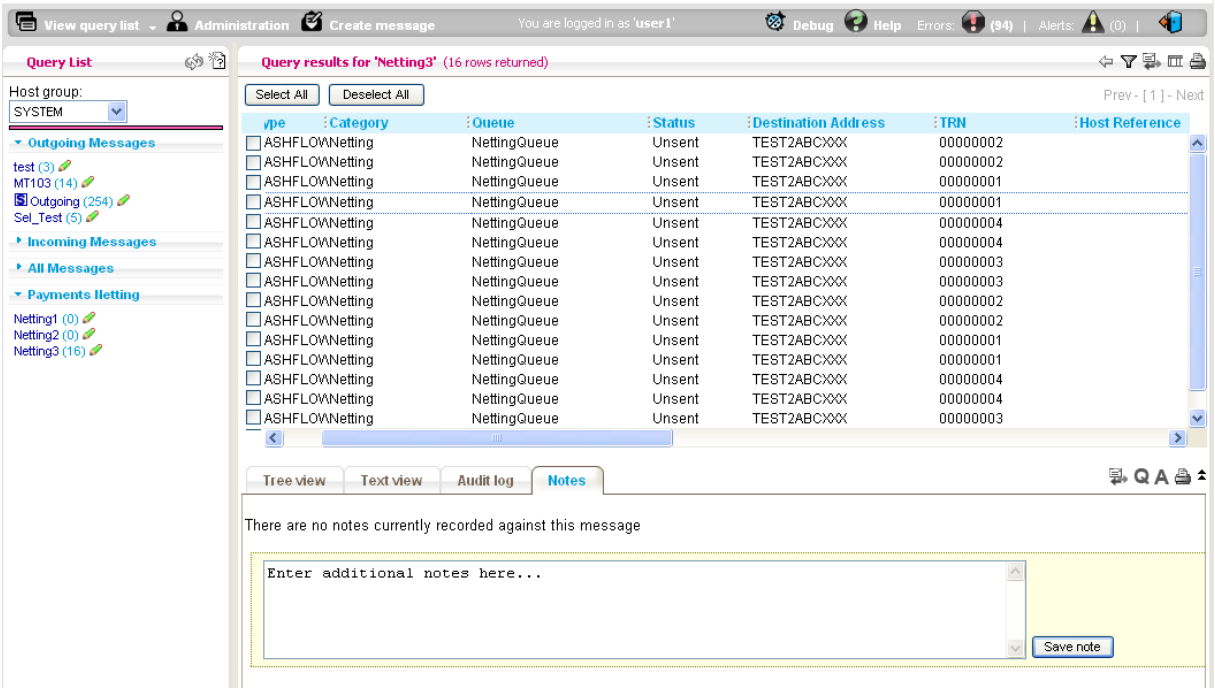
zero amount and, providing the recommended workflow is implemented, will be directed to the "Deleted" queue in the Project.

The Netting Action Result pane

If the netting action is successful, the bottom pane will be replaced with the "Netting action result" pane, with a message detailing the message IDs of the netted messages and the message type and message ID of the resulting SWIFT message.

Adding Notes to a Net Message

In the same Netting Action Result pane, the "Notes" tab provides a means for the user to add some notes about the created net message.



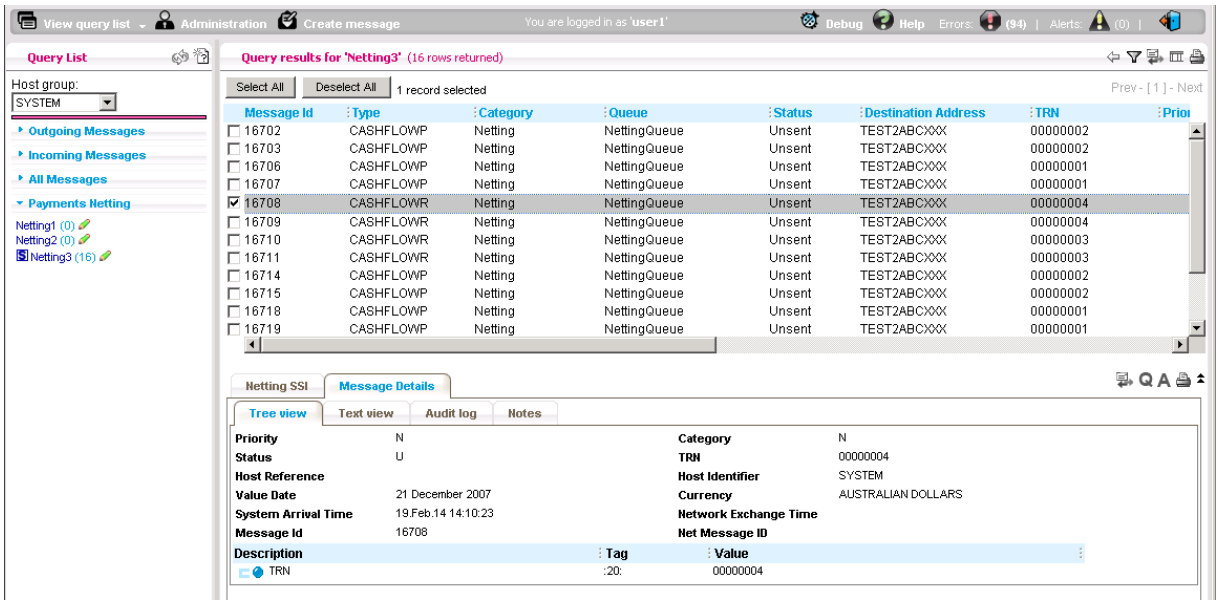
When the net message is queried using a conventional Outgoing Messages query, this note can be viewed on the Notes tab in the Message Details pane.

The Message Details Tab

When a row is clicked on within the summary grid, the Message Details tab is shown in the bottom pane, which will display the usual information and features available on the Message Details pane for conventional live message queries. The only notable difference is the new location and availability of the icons on the toolbar. For netting messages, only the Delete and Print icons will be enabled.

When the Message Details tab is selected whilst in the Netting SSI tab view, the last row selected in the summary grid will be shown.

Refer to the *FusionBanking Payment Manager User Guide* for full information on the functionality offered on the Message Detailed pane.



Tracking CASHFLOW Messages to Net Messages

FusionBanking Payment Manager provides a means to link netted CASHFLOW messages to the associated net message and vice-versa.

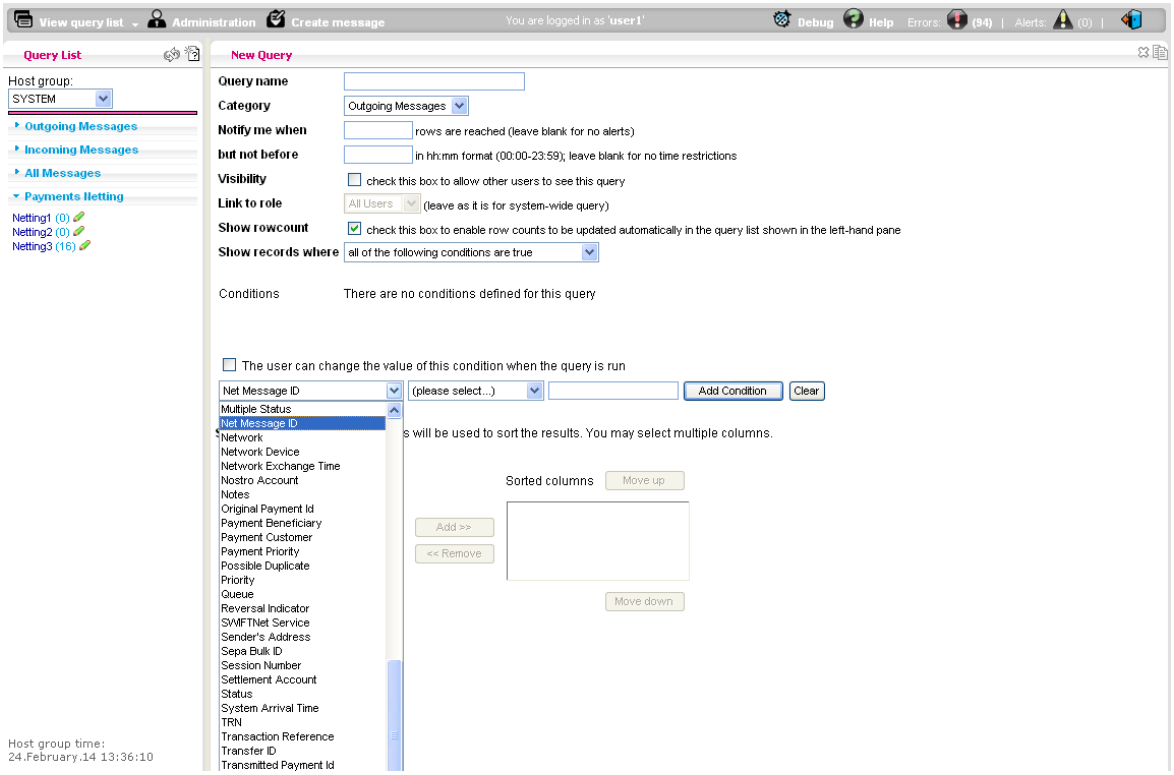
Tracking the Net Message for a Given CASHFLOW Message

When viewing CASHFLOW messages that have already been netted (via an ordinary Outgoing Messages query), an icon will be shown on the Detailed Message Pane toolbar which, when clicked, will display the associated net message on the same pane (overriding the display of the cashflow message). The 'View Net Message' icon will only be activated for messages that have an associated Net Message ID.

Tracking the CASHFLOW Messages for a Given Net Message

To track all cashflow messages that belong to a net message, an ordinary Outgoing Message query can be defined by the user to return all messages with a particular Net Message ID.

To make querying of the Net Message ID possible, the Query Builder has been changed to include the Net Message ID as one of the message properties in the dropdown for setting up Query conditions:

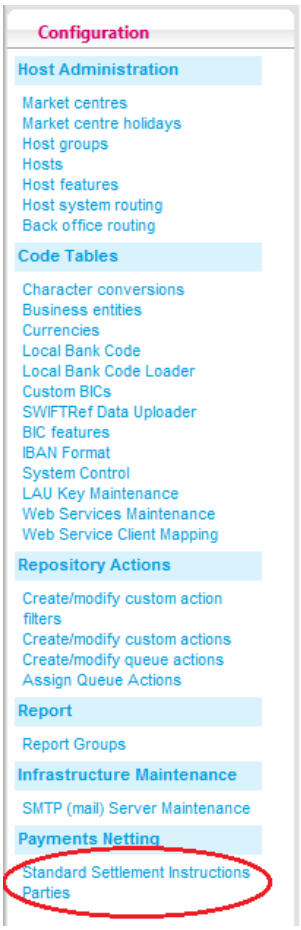


Standard Settlement Instruction (SSI) Maintenance

Within the Administration > Configuration suite of functions there is an additional section called "Payments Netting". Under this category two new tables can be maintained:

Standard Settlement Instructions (SSIs)

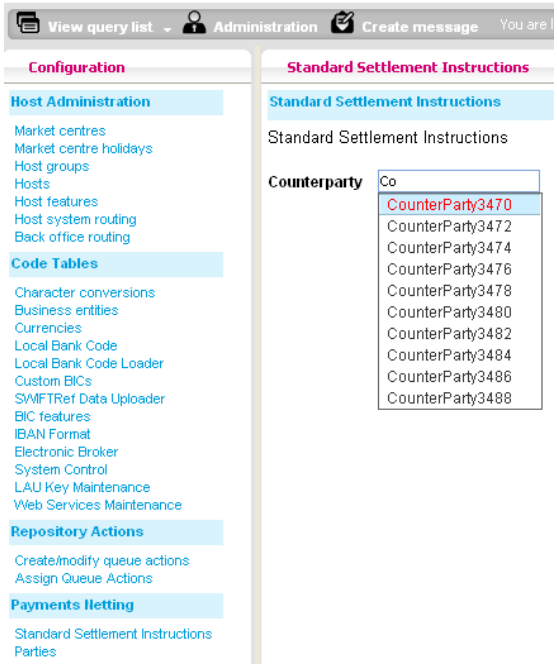
Parties



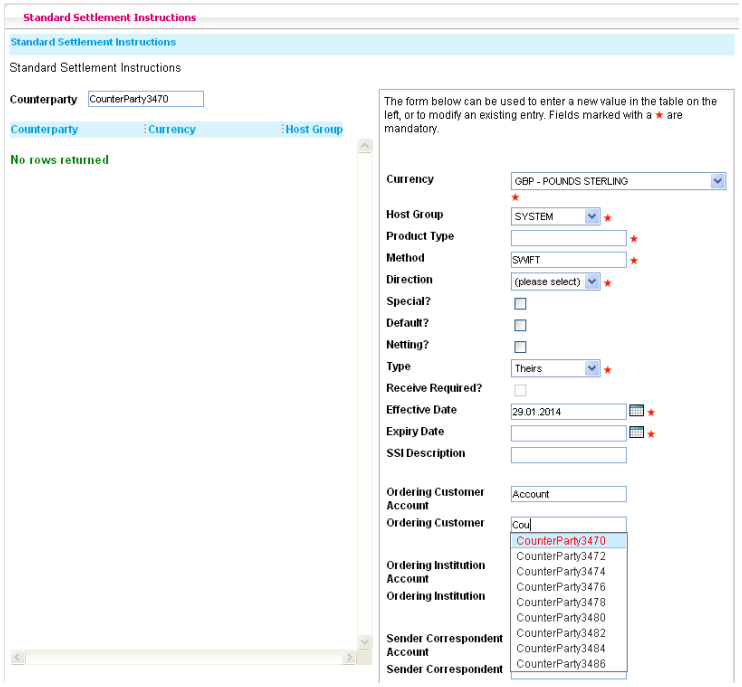
The Standard Settlement Instructions Maintenance Function

This function enables users to maintain the settlement instructions that will be attached to messages created as the result of a Net. As such it includes settlement fields that are used in MT103, MT202 and MT210.

When this option is clicked on from the navigation pane, a selection screen will be displayed in the right hand pane allowing the user to enter and select the name of a particular counterparty of interest.



The user must enter a partial or full counterparty short name in the text entry field. As the user types, a drop-down list of up to twenty counterparty short names that start with the entered character sequence are displayed as a filtering mechanism. The first entry in the list is highlighted in red and can be selected by pressing enter. Other entries in the list can be selected by typing more of the name, or by using the mouse or keyboard navigation keys. On entry or selection of counterparty, the SSI grid and SSI input form will be displayed as follows:



The SSI grid displays all existing settlement instructions associated with a particular counterparty.

In order to improve the application response time during search, the number of rows that can be returned in the search is limited to a figure that can be defined in the FusionBanking Payment Manager Properties file by your Application Administrators. The counterparty text entry field is also included in this pane to allow the user to reference the settlement instructions associated with another counterparty without having to go back to the previous screen. When a new counterparty is selected, the SSI grid is dynamically updated.

The input form on the right hand side of the grid is designed to display existing settlement instructions and allow the capture of new settlement instructions for the current counterparty. Please note that the fields will not be validated according to SWIFT rules.

The following details can be captured and maintained by FusionBanking Payment Manager:

Mandatory fields are appended with a red star on the input screen. All checkboxes that are regarded as mandatory are not tagged with a red star as an unchecked box signifies an entry of 'N'.

Item	Mandatory?	Description
Counterparty	Y	Dropdown of the short names of all the parties available in the Parties table that are financial institutions
Currency	Y	Dropdown of all currencies (ISO Code + description) from the Currencies table
Host Group	Y	Dropdown of all available host groups from the Host Groups table
Product Type	Y	Free format text of up to 50 characters.
Method	Y	Free format text of up to 20 characters. This would typically contain the payment settlement method such as "SWIFT", "RTGS", "CHAPS", "CHIPS", etc.
Direction	Y	Dropdown: Pay, Receive, Both. A combination of Type=Their and Direction=Receive is disallowed
Type	Y	Dropdown: Ours or Theirs
Effective Date		With Date Picker, is displayed in Data-Entry format (from User Preference).
Expiry Date		With Date Picker, is displayed in Data-Entry format (from User Preference). Entry must be later than Effective Date.
Default		Checkbox. Validation ensures that there is only one default per set of SSI records with the same key. The key comprises of the following: • Host group • Counterparty • Currency • Type • Product Type • Method • Direction
Special?		Checkbox. This indicates special processing or routing will be done for net messages using this SSI.
Receive Required?		Checkbox, signifying that this Counterparty wants to receive MT210 messages. It is only activated when type = "OURS".
Netting SSI		Checkbox. This indicates the SSI is available for netting

Item	Mandatory?	Description
SSI Description		Free format text of up to 50 characters.
Source		This information cannot be captured. It is given a default value that will be taken from a properties file.
Ordering Customer Account Line		Free format text using SWIFT X-character set.
Ordering Customer		Entry must be a valid Party short name that exists in the PARTIES table that is NOT a financial institution
Ordering Institution Account Line		Free format text using SWIFT X-character set.
Ordering Institution		Entry must be a valid Party short name that exists in the PARTIES table that is a financial institution.
Sender's Correspondent Account Line		Free format text using SWIFT X-character set.
Sender's Correspondent		Entry must be a valid Party short name that exists in the PARTIES table that is a financial institution..
Cover Required		Check box. Should be clickable only if the Sender's Correspondent is present.
Receiver's Correspondent Account Line		Free format text using SWIFT X-character set.
Receiver's Correspondent		Entry must be a valid Party short name that exists in the PARTIES table that is a financial institution.
Third Reimbursement Institution Account Line		Free format text using SWIFT X-character set.
Third Reimbursement Institution		Entry must be a valid Party short name that exists in the PARTIES table that is a financial institution..
Intermediary Account Line		Free format text using SWIFT X-character set.
Intermediary		Entry must be a valid Party short name that exists in the PARTIES table that is a financial institution.
Account with Institution Account Line		Free format text using SWIFT X-character set.
Account with Institution		Entry must be a valid Party short name that exists in the PARTIES table that is a financial institution.
Beneficiary Account Line		Free format text using SWIFT X-character set.
Beneficiary		Entry must be a valid Party short name that exists in the PARTIES table.

Item	Mandatory?	Description
Remittance Information lines 1-4		Up to 4 lines of free format text using SWIFT X-character set. Entry on each line cannot exceed 35 characters.
Details of Charges		Dropdown: BEN, OUR, SHA. Defaulted to OUR.
Sender to Receiver Information lines 1-6		Up to 6 lines of free format text using SWIFT X-character set. Entry on each line cannot exceed 35 characters.
Remarks 1-4		Free format text.

Entry on all account lines is optional (except for Ordering Customer) and should start with a forward slash '/'.

For Ordering Customer Account line, entry is optional and if entered, one of the these two formats must be followed (otherwise an invalid Net SWIFT message may result):

/34x - a forward slash followed by up to 34 character text from SWIFT X-character set,

CCCC/ - (SWIFT 2007) a four-character codeword followed by a forward slash. The codeword will not be validated against SWIFT allowable codes until the Net message is passed through the SWIFT FIN Validation filter.

Security Permissions

New permissions have been added to the FusionBanking Payment Manager Security function to control users who are allowed to maintain SSI records:

Maintain SSI (administration.MaintainSSI)

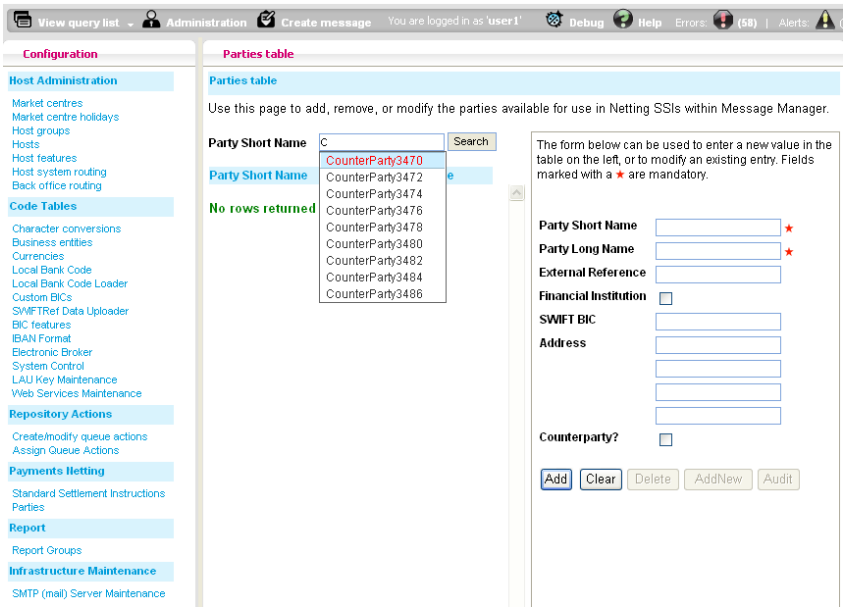
Normally, the standard permission "Configure System Tables" will allow the user to view/maintain the tables under the Administration > Configuration suite of code tables. This new permission will need to be granted along with the "Configure System Tables" to be able to insert or edit SSI records.

If this new permission is not granted, a user can only use the function in view mode when the Netting function is enabled.

The Parties Maintenance Function

This maintenance function allows FusionBanking Payment Manager users to maintain parties and counterparties for whom Standard Settlement Instructions can be created.

When this option is clicked on from the navigation pane, a search screen is displayed in the right hand pane, which will narrow down the results that will be displayed in the grid displayed in the next screen.

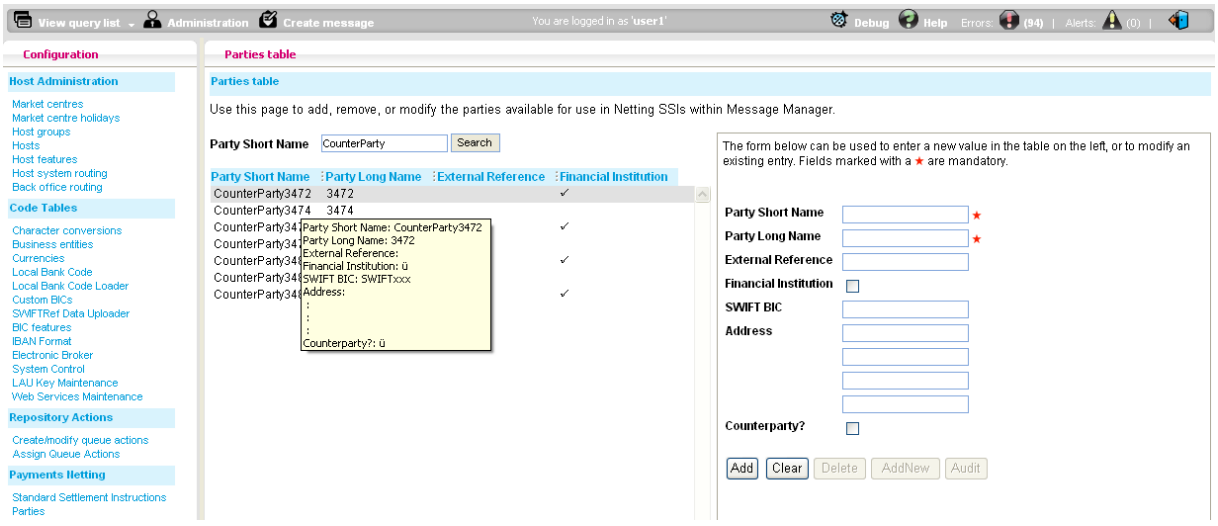


The user can enter either a partial or full Party short name in the associated text entry field. As the user types an entry, a drop-down list of up to ten counterparty short names that start with the entered character sequence is displayed. The first entry in the list is highlighted in red and can be selected by pressing Enter. Other entries in the list can be selected by typing more of the name, or by using the mouse or keyboard navigation keys.

If a partial Party short name is entered when the 'Search' button is selected, the party grid will be populated with the details of all the parties whose party short names start with the entered text. When a new Party is selected, the Party grid is dynamically updated.

If a full Party short name is entered on search, the party grid will be populated with the details of a single party that matches the entered text.

When a row in the party grid is selected, the party input form is populated with the details of the party, as displayed in the following screen shot:



The party input form allows for the modification of the details of existing parties and the addition of new parties. In order to improve the application response time during search, the number of rows that can be returned in the search is limited to a figure that is defined in the FusionBanking Payment Manager properties file. If the user did not enter any values in the previous search screen, the grid will have blank rows displayed. The search fields are also included in this pane to allow the user to do another search without having to go back to the previous screen.

The following details will be captured:

Item	Mandatory?	Description
Short Name	Y	Short version of the party's name. Entry should not be longer than 20 characters.
Long Name	Y	Long version of the party's name. Entry should not be longer than 100 characters.
External Reference		External version of the party's name. Entry should not be longer than 50 characters.
Financial Institution flag		Checkbox, signifying whether the party is a financial institution or not. This value influences the type of message to be produced (MT103 or MT202) when the netting exercise results in a payment.
BIC		Enter the SWIFT BIC for this party if available. Entry should not be longer than 11 characters. Note that either the BIC or the Address must be entered.
Address		Enter up to 4 lines of the party's name and address. This is primarily used to output option K, D or blank option of a party field in the SWIFT message. Note that either the BIC or the Address must be entered
Counterparty flag		Checkbox, signifying that the party is used as a counterparty in payments netting.

Security Permissions

New permissions have been added to FusionBanking Payment Manager Security to allow control over the users who are allowed to add or view only SSI records:

Maintain Parties (administration.MaintainParties)

Normally, the standard permission "Configure System Tables" will allow the user to view/maintain the tables under the **Administration > Configuration** suite of code tables. This new permission will need to be granted along with Configure System Tables to be able to insert or edit Party records.

Appendix C - Switchable Features

Reference	Name	Location	Description
CORE000007	Using TRAM	MPMFlow	If this feature is switched on, copies of the message types mentioned below will be sent to the TRAMMBX node from where they will be picked up by the MidasPlus to TRAM interface: MT300, MT320, MT321, MT330,MT340, MT341, MT350, MT392 This node has no endpoint set up by default. If this feature is to be turned on, the flat file adaptor and connector must be configured and the project re-deployed.
CORE000019	Allow Production of Multiple Messages	Filter – MPMFlow	This is the main controlling feature for the production of multiple messages. It must be enabled for hosts whose messages are to be pooled into multiples via the Configuration, Host Features page of the Administration suite of functions. This feature produces MT203s and multiple MT210s from individual MT202s and MT210s respectively. If CSW031 is switched on, it will also produce MT102s from individual MT103s.
CORE000020	Verify by Line of Business	MPMFlow	This feature allows messages to be sent to the Verification queue based on the Midas Plus module that indicates the source of the message. The list of Midas Plus modules (2 character module IDs) to be included when the feature is turned on must be specified in the optional parameter for the feature (OtionalParameter2).
CORE000024	Enable Midas Plus Functionality	Midas_Stub	This feature tells FusionBanking Payment Manager that Midas Plus is running, as opposed to Midas R4. It must be turned on for all standard Midas Plus Payment Manager installations.
CORE000025	Bypass Verification for all Statements	MPMFlow	This feature allows statement messages to be sent straight out to SWIFT instead of being sent to the Verification queue for manual release.
CORE000027	Consider Urgent Messages as Candidates for Multiples	Filter – MPMFlow	This feature must be switched on for hosts which require their urgent messages to be included in the production of multiple messages. As with CORE000019, this is also enabled on a host by host basis via the Host Features functionality. This feature will only become effective if CORE000019 is also enabled for the same host.
CORE000028	Add Tag 108: into the SWIFT Header	MPMFlow	If this feature is on, field 108: (Message User Reference / MUR) will be added to the block 3. The value will be the Transaction Reference (Midas Plus Deal Reference).

Reference	Name	Location	Description
CORE000031	Allow all non SWIFT messages	Filter – MPMFlow	If this feature is on, non SWIFT messages will not be suppressed by Payment Manager (in the CancellationFilter filter). Instead they will be routed by default to the NotSentToSwift queue in Payment Manager.
CORE000032	Disable Sending of Incoming Messages to Midas	MPMFlow	If this feature is on, incoming messages (outgoing from SWIFT) will not be sent to Midas. Instead the final destination of these messages will be the NotSentToMidas queue in Payment Manager.
CORE000051	Use Canonical	MPMFlow	Use canonical payment for payment messages.
CORE000052	Treasury STP Awaiting Match Functionality	MPMFlow	
CORE000053	Enable Currency	MPMFlow	If this feature is switched on, a check will be made on the settlement currency to verify that it is a working day in the country aligned with the payment currency.
CORE000054	Automatic Release Date Update	MPMFlow	If this feature is switched on, a payment which fails a non-working day check will have its release date reset. If this is not on, the payment will be queued.
CORE000055	Process Late	MPMFlow	If this feature is switched on, late payments will skip cycle checks and will be allowed through.
CORE000056	Release Payment on non-working day	MPMFlow	If this feature is switched on, future dated payments will be sent even if the value date is a non-working day, otherwise payments are routed to the repair queue.
CORE000057	Release Payment with Insufficient Notice Days	MPMFlow	If this feature is switched on, payments can be released without applying the full number of notice days.
CORE000058	Raise IBAN format validation error for non-STP messages	MPMFlow	If this feature is switched on, messages not undergoing STP with incorrect IBAN formats will have an error raised.
CORE000059	Bypass BIC-IBAN combination validation	MPMFlow	If this feature is switched on, validation for the combination of BIC and IBAN will be bypassed.
CORE000069	Enable validation of local bank code and SWIFT BIC matching.	MPMFlow	If this feature is switched on, the following will take place, where relevant: validation of a local bank code identification of a local bank code from a received SWIFT BIC checking that a received SWIFT BIC/local bank code pair matches correctly
CORE000088	Use CSM Calendar	MPMFlow	If this feature is switched on, the market center that will be used will be from the CSM

Reference	Name	Location	Description
			Configuration Tab in the Clearing Systems Config page.
CSW028	Release Confirmations Without Verification	MPMFlow	If this feature is on then all confirmation messages pass through MMM without need for verification.
CSW029	Release All Messages Without Verification	MPMFlow	If this feature is on then all messages pass through MMM without need for verification.
CSW031	Generate MT102's in Payment Manager	Filter – MPMFlow	If this feature is on, it allows the production of MT102s from individual MT103s. It must be switched on, on a BIC by BIC basis, via the BIC Features functionality. When MT103 messages are received by Payment Manager from host applications, the MT103 sender and destination BIC addresses are used to lookup their corresponding CSW031 records in the BIC features table. If both are found and are enabled, then the MT103 is eligible for multiple message processing. This feature will only become effective if CORE000019 is also enabled for the MT103 host.
CSW032	Suppress Field :22F: from Sequence B	Midas_Stub	If this feature is on, field:22F: (TTCO) in Sequence B of Trade generated MT540, MT541, MT542, MT543 messages will be suppressed.
TESTMODE	Use Test and Training Mode	MPMFlow	If this feature is on, all messages produced in Midas Plus Payment Manager will have their destination address set to the training address that must be entered into Optional Parameter 1.

Appendix D - Automated Cancellation Processing

The ArrivalServer adaptor is a component that performs cancellation processing for financial messages. In a typical workflow, the ArrivalServer adaptor is attached to the first node that receives financial messages from the host interface. Cancellation processing takes account of cancellation semantics for each of the supported network/formats.

SWIFT

Three SWIFT cancellation processing models are implemented; the **codeword model** used for category 3 messages (Treasury Markets Foreign Exchange, Money Markets & Derivatives), the **ISO15022** model used for ISO15022 Securities messages and the **MTn92** model, used for other message types, including pay and receive messages.

Codeword model

Reference	State of previous messages	Result
New transaction	New transaction, so no existing confirmations.	New confirmation generated with 'new' codeword (NEWT).
Amend transaction	No existing confirmations for this transaction (either because the transaction was entered before FusionBanking Payment Manager was in use, or because old messages have been dropped).	New confirmation generated with 'amend' codeword (AMND). Assumption is that previous messages were sent, even if they are no longer available to the cancellation process.
	Existing unsent confirmation. No confirmation has ever been sent for this transaction.	Existing unsent confirmation logically deleted. New confirmation generated with 'new' codeword (NEWT).
	Existing unsent confirmation, but previous confirmations for this transaction were sent.	Existing unsent confirmation logically deleted. New confirmation generated with 'amend' codeword (AMND).
	No unsent confirmations, but at least one confirmation already sent.	New confirmation generated with 'amend' codeword (AMND).
Cancel transaction	No existing confirmations for this transaction (either because the transaction was entered before FusionBanking Payment Manager was in use, or because old messages have been dropped).	New confirmation generated with 'cancel' codeword (CANC). Assumption is that previous messages were sent, even if they are no longer available to the cancellation process.
	Existing unsent confirmation. No confirmation has ever been sent for this transaction.	Existing unsent confirmation logically deleted. No new confirmation is generated.
	Existing unsent confirmation, but previous confirmations for this transaction were sent.	Existing unsent confirmation logically deleted. New confirmation generated with 'cancel' codeword (CANC).

Reference	State of previous messages	Result
	No unsent confirmations, but at least one confirmation already sent.	New confirmation generated with 'cancel' codeword (CANC).

ISO15022 model

Action	State of previous messages	Result
New transaction	New transaction, so no existing messages	New message generated
Amend transaction	No existing messages for this transaction.	New message generated. Cannot generate cancellation if previous message cannot be found.
	Existing unsent message	Existing unsent message logically deleted. New message generated.
	Existing sent message.	MT5nn cancellation generated to cancel previous message. New message generated.
Cancel transaction	No existing messages for this transaction.	No message generated
	Existing unsent message	Existing unsent message logically deleted.
	Existing sent message	MT5nn cancellation generated to cancel previous message.

ISO15022 cancellation messages are of the same type as the message being cancelled (i.e. an MT541 is cancelled by a second MT541). The cancellation is identified by the codeword **CANC** in field **23G Function of the Message.** The message being cancelled is referenced in the **Linkages** subsequence, fields **16R LINK – 16S LINK**.

MTn92 model

Action	State of previous messages	Result
New transaction	New transaction, so no existing messages	New message generated
Amend transaction	No existing messages for this transaction.	New message generated. Cannot generate MTn92 if previous message cannot be found.
	Existing unsent message	Existing unsent message logically deleted. New message generated.
	Existing sent message.	MTn92 generated to cancel previous message. New message generated.
Cancel transaction	No existing messages for this transaction.	No message generated

Action	State of previous messages	Result
	Existing unsent message	Existing unsent message logically deleted.
	Existing sent message	MTn92 generated to cancel previous message.

Cancellation prerequisites

Cancellation processing depends on a number of fields in the message's SWIFT header. These fields allow the ArrivalServer adaptor to correctly identify the action (Insert, Amend or Delete) associated with each message, and to identify related messages. The mandatory fields for cancellation processing are:

Field	Content	Comment
HostType	The type of host system (Equation Midas, Opics, …)	
HostID	A string that uniquely identifies an instance of a host system (e.g. Equation unit mnemonic, Midas system prefix, …)	
DealReference	A unique reference to the transaction	Used on deletion to find all messages for the transaction
HostReference	A unique reference to a transaction and the event in the life of that transaction for which the message was generated.	Used by amend process to find messages for this event (for example if details for one settlement amongst many have changed, this field will be used to identify and cancel/delete only those messages related to the changed details)
InternalMessageType	A code representing the function of the message: P=Payment; R=notice to Receive; C=Confirmation; I=ISO15022; S=Statement, M=Cash Management.	Used on amend to ensure that, for example, only payment messages are cancelled if only pay-side details have changed.
Action	I=Insert; A=Amend; C=Cancel	

Appendix E - Multiple Message Processing

Overview

Multiple messages are a feature of the SWIFT FIN standard. It is possible to group together a number of similar transactions for transmission as a single message – saving on the cost of message delivery. For example, a SWIFT General Financial Institution Transfer (MT202) may be sent as part of a Multiple General Financial Institution Transfer (MT203). Other multiple message types include MT102 (multiple MT103) and MT210 (multiple MT210). To be eligible for inclusion in a multiple, individual messages must share some common data or **match criteria**. In the case of an MT203 payment message, for example, all parts must have the same sender, destination, currency and value date.

FusionBanking Payment Manager includes a feature that allows individual messages to be consolidated into multiple messages automatically. The FusionBanking Payment Manager Message Broker workflow is used to route eligible single messages to a special queue (normally **MultipleHold**) that implements the message consolidation logic. Messages arriving at this queue are held; pending the arrival of other messages with identical match criteria (FusionBanking Payment Manager adds some standard match criteria of its own to ensure that multiple messages belong to a single business entity). If an optimal multiple message – one that is as large as the standard permits - can be assembled from the component messages on the queue it is sent immediately, and the components are marked as having been sent as a multiple. A user may opt to send a non-optimal multiple or single message component from the multiple hold queue at any time prior to automatic release using FusionBanking Payment Manager Explorer. Component messages are automatically sent as non-optimal multiples or single messages on their value date, at a time determined by a setting on FusionBanking Payment Manager Currency Details table, to ensure that payments are not missed if an optimal multiple cannot be created.

Enabling the Multiple Message Functionality

The production of multiple messages is controlled by the following switchable features:

Field ID	Description
CORE000019	"Allow production of multiple messages" This is the main controlling feature for the production of multiple messages. It must be enabled for hosts whose messages are to be pooled into multiples via the Configuration, Host Features page of the Administration suite of functions. This feature produces MT203s and multiple MT210s from individual MT202s and MT210s respectively. If CSW031 is switched on, it will also produce MT102s from individual MT103s.
CORE000027	"Allow urgent messages to become eligible for the production of multiple messages." This feature must be switched on for hosts which require their urgent messages to be included in the production of multiple messages. As with CORE000019, this is also enabled on a host by host basis via the Configuration, Host Features page of the Administration suite of functions. This feature will only become effective if CORE000019 is also enabled for the same host.
CSW031	"Allow the production of MT102s" This feature allows the production of MT102s from individual MT103s. It must be switched on a BIC by BIC basis via the Configuration, BIC Features page of the Administration suite of functions. When an MT103 messages is received, the MT103 sender and destination BIC addresses are used to lookup their corresponding CSW031 records on the BIC features table. If both are found and

Field ID	Description
	are enabled, then the MT103 is eligible for multiple message processing. This feature will only become effective if CORE000019 is also enabled for the MT103 host.

Identifying Potential Components

When an MT210, MT202, MT103 is sent from a host to FusionBanking Payment Manager, a number of rules need to be met, before deciding if the message can become a potential component of a multiple message:

- The feature CORE000019 is switched on for sending host.
- The message amount does not exceed the cut off amount for the related currency.
- If the feature CORE000027 is not switched on for the sending host, the message priority cannot be 'U' – Urgent.
- If the message type is MT103, it can only be sent as part of multiple MT102 if the feature CSW031 is switched on for both sender and receiver BIC address

The cut off amount is stored is stored in the Currencies table without decimal points. The amount from either 32B for an MT210, or 32A for an MT103 and MT202 will be checked if less than or equal to the Cut Off amount.

If all the above criteria are met, then the message will be populated with the relevant data to satisfy eligibility for a component of a multiple message. This data will be in the form of a matching key which will be created by concatenating an order of the message type, destination address, value date and currency code into one field. This is because to be eligible for grouping, messages must have the same message type and share the same destination, value date and currency details. Further criteria are also required for each message type, which follows below.

The message will also contain a multiple message status field that will be populated with the value 'P' - potential message. Once flagged, all potential component messages will be held in a common queue (normally the **MultipleHold** queue) for a period of time, before being released as either an individual message or as a component of a multiple. Only messages with the multiple message status flagged as 'P' will be held in this queue.

MT210 Multiple message criteria

The multiple match key for an MT210, will be made up of the following criteria:

- Message type
- Block 3 Message User Reference
- Block 3 Banking Priority
- Block 3 Address Information
- :32B: Currency Code
- Sender Address
- Host ID
- Destination Address
- :30: Value Date
- Account ID

The multiple message match key will look similar to:

```
MT210@null@null@null@USD@PTSAGBPPAXXX@A1@CHASUS33AXXX@190605@null
```

MT102 Multiple message criteria

The multiple match key for an MT103, will be made up of the following criteria:

- Message type
- Block 3 Validation code
- Block 3 Message User Reference
- Block 3 Banking Priority
- Block 3 Addressee Information
- :32B: Currency Code
- Sender Address
- Host ID
- Destination Address
- :30: Value Date
- :23: Bank Operation Code
- :51A: Sending Institution
- :53a: Sender Correspondent either A
- :54a: Receiver Correspondent A
- :71A: Details of Charges
- :72: Sender to Receiver Information

Senders Correspondent, Sending Institution, Receivers Correspondent and **Ordering Institution** are optional and therefore may not appear in the multiple message key. 50K contains an optional account no, with an address, this field must match all other fields of other components, so the account must be the same.

The multiple message match key may look similar to the following:

```
MT103@null@null@null@null@USD@PTSAGBPPAXXX@A1@PASOBEB0AXXX@190605@CRED@null
@null@null@OUR@null
```

Please note there is further criteria for a 102, see the SWIFT user manual.

MT203 Multiple message criteria

The multiple match key for an MT202 will be made up of the following criteria:

- Message type
- Block 3 Message User Reference
- Block 3 Addressee Information
- :32A: Currency Code
- Sender Address
- Host ID
- Destination Address
- :32A: Value Date
- :53a: Sender Correspondent either A, B or D
- :54a: Receiver Correspondent A, B or D
- :52a: Ordering Institution A or D

Senders Correspondent, Receivers Correspondent and **Ordering Institution** are optional and therefore may not appear in the multiple message match key.

The multiple message match key may look similar to:

```
MT202@null@null@ USD@PSTAGBPPAXXX@A1@PASOBEB0AXXX@190605@null@null@null
```

Generating Multiple Messages

A background process called the Multiple Message Service monitors the collection of potential component messages held on the Multiple Hold queue. The process is triggered on a configurable polling interval (usually set at 5 to 30 minutes) defined in the project multiple message service profile. The process will trigger a number of operations for releasing potential messages either as components of multiple messages or as individual messages:

Creating multiple messages when the maximum components are available

The process will monitor the number of component messages for a matching key. The maximum number of components for each multiple message type is configured in the project multiple message service profile. When the number of component messages is available, they will be released as part of a multiple message.

Creating multiple messages when the maximum size is reached

For all multiple message types, as defined in the Swift standards, a maximum number of characters is enforced for a message. A process will be required to monitor the collected size of characters for each set of matching potential component messages. When the maximum size is reached, the messages will be grouped together and released as a multiple message. The maximum number of characters for the related multiple messages are:

- MT210, MT203 – 2,000 characters
- M103 – 10,000 characters

The maximum characters can be configured to be less than the above recommendations by changing the defaulted values in the project multiple message service profile.

Releasing messages at cut off time

A user configurable **cut off time** field is provided in the Currencies table to allow an administrator to set up a time to release messages for a given currency. The following points describe the behaviour of batching up multiple messages around the cut off time:

- Prior to the cut time, only multiple messages that reach the maximum components and size limits will be released. Non-optimal multiples (i.e. matching messages that do not reach the limits) and unmatched potential messages remain in the MultipleHold queue.
- When the cut off time is reached, all potential component messages for that currency will be released as either components of multiple messages (whether optimal or non-optimal) or, if no matching messages are available, as individual messages. The creation of multiple messages and individual messages are discussed below.

From this time on up to midnight, all qualified messages with value date prior or equal to today are sent as individuals, whilst those with value date of greater than today will be pooled and sent as normal (i.e. as per processing prior to cut off time).

Message States

The following table describes the messages states:

Field ID	Type	Description
P	Potential (component)	A message of this type is defined as being eligible for becoming a part of a multiple message
C	Component	A message becomes a component once it has been incorporated into a multiple message
M	Multiple	A message is defined as multiple if it contains two or more component messages
I	Individual	A message is an individual if it is released from the holding place and has no potential for being a component of a multiple.

Individual messages

Individual messages will be transmitted to the next point in the workflow, this is likely be the SwiftTransmit node.

At this point the MultipleMessageStatus field will be changed to 'I' – Individual. This change will exclude any conflicts with matching potential component messages and provide flexibility for the user when creating custom queries.

If the message is a MT210, then the message count monitor, for the multiple match key will be corrected.

Component messages

All potential component messages will have their message status set to 'C' – Component. The component messages will then be moved to a **'Sent as Multiple'** node. Here, the component messages will remain until archived.

When the Multiple message status is set to 'C', it will help to exclude any conflicts with matching potential component messages and provide flexibility for the user when creating custom queries. It will also be used for reference by the multiple message for display purposes. The multiple message match key will also be included in the component message this will be used to reference the multiple message.

Multiple messages

Multiple messages will be transmitted to the next point in the workflow, which is likely to be the SwiftTransmit node.

At this point the MultipleMessageStatus field will be changed to 'M' – Multiple. This change will exclude any conflicts with matching potential component messages and provide flexibility for the user when creating custom explorer queries.

The creation of multiple messages will use the same generic behaviour for all actions described in the above processes. The structure of the different multiple message types vary, for more information see the SWIFT documentation.

When created, the multiple message will have a unique key generated (Multiple Message ID). The key will be added to all component messages. This key may be used on query conditions to reference the multiple message on the View Query List option (see the *FusionBanking Payment Manager User Guide*).

The MT102 multiple message requires the total sum of the amounts for all of the components, in field 23A to be calculated and added to field 19. The sum of receivers charges (71G) also needs calculating.

The MT203 multiple message requires the total sum of the amounts for all of the components, in field 23A to be calculated and added to field 19.

During the process of creating a multiple message, prior to adding a matching potential message, the size of the multiple message should be calculated with the new potential message. If the multiple message would exceed the maximum size with the new potential, the multiple message should be released without the potential message.

Configuration Options

Currencies Table

The following fields in the currencies table are used specifically for the multiple message processing:

Multiple Message Cut Off Time – the time of the day when all component messages will be pooled into multiples regardless of whether the maximum components or size is reached. See Releasing Messages at cut off time.

Next Multiple Message Run – this is the date at which the cut off time processing will be made effective. This date is automatically advanced to the next day after the cut off processing.

Market Centre – this is used to express the time zone at which the cut off time is be expressed in. This is to qualify the cut off time against the server time when all payment and receive messages will be sent. As an example, if the cutoff time for USD is 17:00 and the server is in London, setting the Market Centre in New York will have the cut off time processing for USD be processed at 22:00 London time (a difference of 5 hours).

Cut Off Amount – Potential messages with amounts greater than specified on this field will not be pooled into the multiple message. If a value is not defined, then no amount checking will be performed. When the Cut off Amount is re-set any time during the day, the new value will be used immediately.

Multiple Message Service Profile

The background process that collects the potential messages into multiples is controlled by a number of configurable fields kept in the project Multiple Message Service Profile. Some of these fields are listed below:

- **Polling Interval** – This field defines the time interval (in milliseconds) between activation of the background process. This is usually set at 300,000 to 1,800,000 milliseconds (5 to 30 minutes).
- **Input Node** – The node/queue which contains messages which will be combined (usually the **MultipleHold** queue)
- **Transmit Node** – The node/queue where completed multiples or individuals that cannot be combined, will be sent (e.g., the **SwiftDecision** node)
- **Sent As Multiple Node** – The node/queue where copies of the individual messages which have been combined will be placed (usually the **SentAsMultiple** node).
- **Maximum Size MT102** – The maximum number of characters a generated MT102 multiple message. As mandated by SWIFT, this should not exceed 10,000.
- **Maximum Size MT203** – The maximum number of characters of a generated MT203 multiple message. As mandated by SWIFT, this should not exceed 2,000.
- **Maximum Size MT210** – The maximum number of characters of a generated MT210 multiple message. As mandated by SWIFT, this should not exceed 2,000.

- **Maximum Components MT102** – The maximum number of component messages to create in an MT102 multiple message.
- **Maximum Components MT203** – The maximum number of component messages to create in an MT203 multiple message. As mandated by SWIFT, this should not exceed 10.
- **Maximum Components MT210** – The maximum number of component messages to create in an MT210 multiple message. As mandated by SWIFT, this should not exceed 10.

Manual Routing Actions for Potential Multiple Messages

FusionBanking Payment Manager allows a user, on an ad hoc basis, to manually select potential components and route them forward in the workflow. This is particularly useful when the background service is in waiting mode or when isolated potential components need to be sent out ahead of the cut off time.

To do this:

1. Create a query to display all potential components being held.
2. Select a potential component from view
3. Click **Custom Action** icon from the toolbar and perform one of two actions from the dropdown: Route as Individual and Route As Part of Multiple

Route as Individual

When the RouteIndividual action is selected, the chosen message will have its state change to 'I' – Individual and will be released on its own.

Route as Part of a Multiple

When the RouteMultiple action is selected, a process will gather a list of messages with the same multiple match key as the selected potential component message and the resulting multiple message will be released. If no other messages are found with the same key, the potential component will be released as an Individual, performing the same functions described above.

The minimum amount of messages required for a multiple message is two. If two or more matching potential component messages are found, a multiple message will be created out of these. The selected message and all other related components will have their state changed to 'C' – component. The multiple message will be created using the same procedure as described in Multiple Messages. Component messages are detailed in Component Messages.

Multiple Message Display Facilities

When viewing component messages in the FusionBanking Payment Manager Explorer, an option is available to view the corresponding multiple message by selecting the View Multiple icon from the Detailed Message Pane toolbar. The multiple message will then be displayed in the Detailed Message Pane.

All multiple messages are created with a unique key called the Multiple Message ID. To generate a query for displaying the associated component messages of a selected multiple message, create query conditions based on selecting components with the same Multiple Message ID, located in the SentAsMultiple queue.

Glossary

Booked	A booked payment instruction is one where debit / credit accounting entries have been applied. Un-booked instructions are the opposite – the relevant account has not been debited or credited.
Release Date	Date on which a payment is scheduled for release.
Release Time	The time on Release Date at which a payment can be released into the workflow
Settlement Cut-Off Time	The latest time of day at which the Business wishes to release a payment. This time is used to define when "proximity" alerts should be raised, and to alert users when a payment is being released after its settlement cut-off time.
Settlement Date	The inter-bank settlement date for a payment. Settlement date is applied according to date at the payment destination.