



User Guide

Enhanced Real-Time Rule Building

2022

Table of Contents

1. Introduction	1
2. Background	1
3. Rule Building – Fundamentals	1
4. Rule Administration – Navigation	2
5. Types of Rules	3
6. Rule Building – Primary Rule Screens	5
7. Basic Rule Building	7
8. Rule Advanced Settings	8
9. Basic Rule Building – Continued	9
10. Defining a Basic Rule	11
11. Creating New Filters or Match Groups	14
12. Defining Group Criteria	15
13. Enhanced Rule Functionality	18

1. Introduction

This document aims to provide guidance on how to create rules using the Enhanced Real Time (ERT) ruleset.

2. Background

The ERT ruleset is the rule set type that is available as a result of the new rule engine – that aims to be the single rule engine that runs all batch, manual entry and real time enquiries.

This means that the system has a single rule building experience, for Luminate FraudIQ Manager based rules, in order to make the user journey consistent for rule building.

As a direct result of the purpose for which the engine was built, the rule building journey is an amalgamation of the legacy batch and Real-time (RT) journeys.

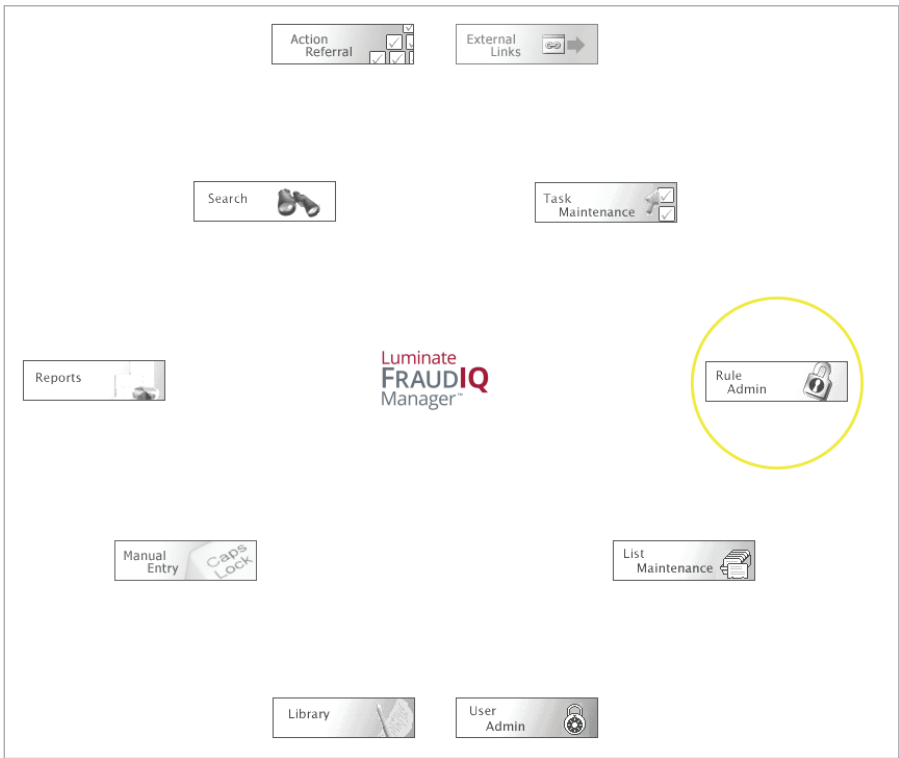
Similarly, with the existing rule engine, it hinges on data being consistent. If the data being sent to Luminate FraudIQ Manager to run against rules is inconsistent and poor quality, the performance of the rules will be impacted. There is the expectation that clients try to send the highest quality data into Luminate FraudIQ Manager to ensure that rules are as effective as possible and understand the impact of poor and inconsistent data on rule performance.

3. Rule Building – Fundamentals

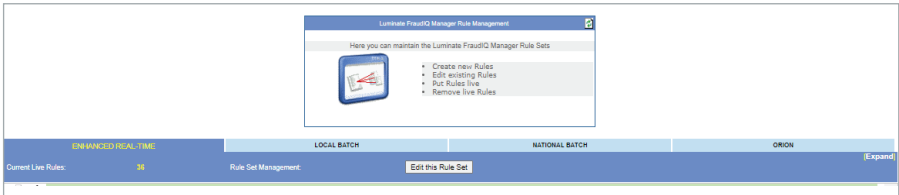
This section will aim to cover the basic prerequisite knowledge required prior to starting rule building. If you are comfortable as a user with how to build a rule already – skip to the enhanced functionality section for an overview of the new functionality that the ERT engine provides.

4. Rule Administration – Navigation

The rule administration page, which houses ERT rule tab, can be located from the clock face on the Luminate FraudIQ Manager home page.



The ERT rule set tab will then be available within the other rule sets configured for the domain:



This tab will display all the current live rules within the rule tab.

If the Luminate FraudIQ Manager system has multiple domains, the domain selector can be used to navigate to the domain's rule sets.

5. Types of Rules

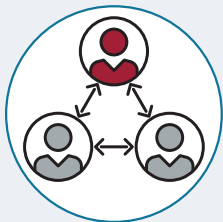
There are two types of rules that are available within the Luminate FraudIQ Manager system to be built.



Validation Rules

- Focus on information contained on the new enquiry **only**
- Does **not** compare against any existing enquiries
- Examines different elements of the enquiry in order to highlight characteristics which are aligned with suspicious profiles

Main Applicant has stated an income of \$80,000 and is only 18 years old



Match Rules

- Compares elements of the new enquiry with those of existing enquiries, looking to highlight similarities and/or differences
- Comparisons can be made against the local or National data sets

Main Applicant has the same first name, last name and DOB as an individual previously marked as fraud

When building rules, they are split into 3 main components; new, match and existing.

New – Defines the criteria and logic on the incoming application to be considered as part of the rule.

Match - Defines the data items and logic on which the rule will compare against the incoming and existing enquiry.

Existing – Defines the criteria and logic to refine the existing applications to be considered as part of the rule.

The rule build screen is split into these three sections. This will be explained in more detail further on in this guide.

Validation and **matching** rules can be recognized by their underlying logic and their iconography within the ruleset.

Validation rules *only* have filters in the 'New' column of the rule i.e. filtering on the incoming application. Matching rules *must* have some form of matching criteria in the 'Match' column. Filters in the 'New' and 'Existing' columns are optional.

When viewing a ruleset within rule administration – it is possible to quickly understand which rules are validation rules or match rules based on their iconography.



New	Match	Existing
<p>The left hand side of a rule focuses on the enquiry which has been submitted</p> <p>Only filter groups can be applied</p> <p>Acts as a sieve filtering high risk anomalies within the clients application</p> <p>Example: Main Applicant, age < 25, income > 40K</p>	Blank	Blank

New	Match	Existing
<p>The left hand side of a rule focuses on the enquiry which has been submitted and can be used to filter out unwanted data items or enquiries from the rule process</p> <p>Only filter groups can be applied</p> <p>Examples include "Party Type = Main Applicant" and "Address Type = Current Address"</p>	<p>The middle of a rule focuses on the criteria which will be used to compare new enquiries with those which already exist</p> <p>Only match groups can be applied</p> <p>Examples include "Same Person", "Different Address"</p>	<p>The right hand side of a rule focuses on the enquiries which already exist with the matching data set and can be used to filter out unwanted data items or enquiries from the rule process</p> <p>Only filter groups can be applied</p> <p>Examples include "Party Type = Main Applicant", "Action Status = Highly Suspect"</p>

6. Rule Building – Primary Rule Screens

Following the steps outlined in section 4 of this document will lead to the following screen, which displays the rule sets available for the domain. Clicking on each rule set tab will display the live rules for each rule set.

The page names below are referenced in the URL of the page, for example:

<https://fraudiqmanager.equifax.com/RTRuleSetDefinition.aspx>

RuleSetManagement

ENHANCED REAL-TIME		LOCAL BATCH		NATIONAL BATCH	
NATIONAL REAL TIME		ORION			
Current Live Rules: 0		Rule Set Management:		Edit this Rule Set	
			A_Test_Hoang_01	Score: 50	Same Person All Applicants
			A_TEST_HOANG_R01	Score: 0	A_TEST_HOANG_R01
			CIT01L	Score: 50	Same Person All Applicants
			CIT02L	Score: 50	Same Funding Account Applicants
			CIT03L	Score: 50	Same Cell Phone Applicants
			CIT04L	Score: 50	Same Telephone Number Applicants
			CIT05L	Score: 50	Same Telephone Number Employer
			CIT06L	Score: 50	Same Address Applicants
			CIT07L	Score: 50	Same Address Employer
			CIT08L	Score: 50	Same DOB and Postal Code Applicants
			CIT09L	Score: 0	Same Company Name Employer
			CIT10L	Score: 50	Same IP Address Applicants
			CIT11L	Score: 0	Same Passport Number Applicant
			CIT12L	Score: 50	Same DL Number Applicant
			CIT13L	Score: 50	Same Email Address Applicant
			CIT14L	Score: 50	Same SIN Applicant
			CIT25L	Score: 50	Recently Issued SIN 24 with Ontario Province Code
			CIT28L	Score: 50	Passport Check
			CIT29L	Score: 50	DL Algorithm Check

RTRuleSetDefinition

Clicking on the button 'Edit this Rule Set' leads to the RTRuleSetDefinition page.

This is the page where the rule creation process starts.

Development Area

Finish - Rules to go Live

Checked

The following rules have been successfully tested, but have not yet been promoted to go Live

[expand]

Type	Rule Name
No Checked rules	

Development

The following rules have been created but not yet successfully tested

[expand]

Type	Rule Name
NEW	[No name set]

Create a New Rule

This page has two main areas:

- **Development** – This area is where any new and untested rules will reside
- **Checked** – This area is where any rules that have been successfully tested will reside

Rules that have a status of 'working' will be in the development area of the screen, those with the status of 'tested' will be in the 'Checked' area of the screen. Splitting this screen into development and checked allows the user to quickly see which rules are ready to be promoted to live.

Clicking the tab at the top 'Finish – Rules to go Live' will navigate the user to the RRuleSetDefinitionPending page.

If the user has the relevant permission, there will be a link to the 'Rule Loading Priorities' page.

[Go to Rule Loading Priorities](#)

This page allows the users to map the rules to specific RT workflows.

Rules																			
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This allows fully control of each workflow's rule strategy, enabling configurability at each call to the Luminate FraudIQ Manager system.

RRuleSetDefinitionPending

This page will display the current live rule set. Here it is possible to copy live rules to the working area in order to be edited and promoted, in order to replace the live rule. It is also possible to remove the rules from the live rule set.

Development Area

Finish - Rules to go Live

Rules to go Live

The following Real-Time rules have been set to go Live with this collection, they will replace what is currently live

Type	Promoted By	Rule Name	
-	[Inherited]	CITA_ERT_DLRule_Test - CITA_ERT_DLRule_Test	»
-	[Inherited]	CITA01L_ERT_MIG - Same Person Match to HS,S,GS,LS	»
-	[Inherited]	CITA01L_ERT_MIG - Same Person Match to HS,S,GS,LS	»
-	[Inherited]	CITA01N_ERT_MIG - Same Person Match to HS, S, GS	»
-	[Inherited]	CITA01T_ERT_MIG - Same Person_Telco	»
-	[Inherited]	CITA01T_ERT_MIG - Same Person_Telco	»
-	[Inherited]	CITA02L_ERT_MIG - Same Address Match to HS,S,GS,LS	»
-	[Inherited]	CITA02N_ERT_MIG - Same Address Match to HS,S,GS	»
-	[Inherited]	CITA02T_ERT_MIG - Same Address_Telco	»
-	[Inherited]	CITA03L_ERT_MIG - Same SIN Match to HS,S,GS,LS	»
-	[Inherited]	CITA03N_ERT_MIG - Same SIN Match to HS,S,GS	»
-	[Inherited]	CITA03T_ERT_MIG - Same Sin_Telco	»
-	[Inherited]	CITA04L_ERT_MIG - Same DL Match to HS,S,GS,LS	»
-	[Inherited]	CITA04N_ERT_MIG - Same DL Match to HS,S,GS	»
-	[Inherited]	CITA04T_ERT_MIG - Same DL_Telco	»
-	[Inherited]	CITA05L_ERT_MIG - Same IP Match to HS,S,GS,LS	»
-	[Inherited]	CITA05N_ERT_MIG - Same IP Match to HS,S,GS	»
-	[Inherited]	CITA05T_ERT_MIG - SAME IP_Telco	»
-	[Inherited]	CITA06L_ERT_MIG - Same Email Match to HS,S,GS,LS	»
-	[Inherited]	CITA06N_ERT_MIG - Same Email Match to HS,S,GS	»
-	[Inherited]	CITA06T_ERT_MIG - Same Email_Telco	»
-	[Inherited]	CITA07L_ERT_MIG - Same Email , Different Name	»
-	[Inherited]	CITA07N_ERT_MIG - Same Email , Different Name	»
-	[Inherited]	CITA07T_ERT_MIG - Same Email , Different Name_Telco	»
-	[Inherited]	CITA08L_ERT_MIG - Same DOB & Address, Different Person	»
-	[Inherited]	CITA08N_ERT_MIG - Same DOB & Address, Different Person	»
-	[Inherited]	CITA08T_ERT_MIG - Same DOB & Address, Different Person_Telco	»
-	[Inherited]	CITA09L_ERT_MIG - Same Person, Different Address	»
-	[Inherited]	CITA09N_ERT_MIG - Same Person, Different Address	»
-	[Inherited]	CITA09T_ERT_MIG - Same Person, Different Address_Telco	»
-	[Inherited]	CITAL_ERT_SameAddress_TestRule - CITAL_ERT_SameAddress_TestRule	»
-	[Inherited]	MB_SameDL_Local - Same DL	»
-	[Inherited]	MB-Same All DL_05092022 - Same Address	»
-	[Inherited]	MB-SameIP05092022 - Same IP	»
-	[Inherited]	TFST1.001 - Testinn	»

I want these Real-Time rules to replace the current Live collection

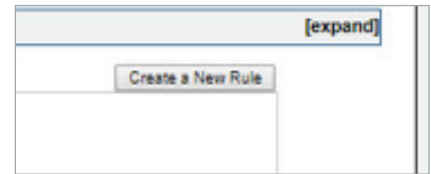
Set this Real-Time collection Live...

Changes are not committed to the system until the 'Set this Real-Time collection Live' button is pressed.

7. Basic Rule Building

Following the steps above, navigate to the RTRuleSetDefinition page and click the 'Edit this Rule Set'.

Then click the 'Create a New Rule' button.



+*You will then be presented with the below screen:

A screenshot of the RTRuleSetDefinition page. The 'Rule Definition' section on the left contains fields for Name (1), Display Name (2), Description (3), Score (4), and Original Rule Key (5). The 'Domain Group' dropdown (6) is set to 'National Real-time Group'. The 'Rule Criteria' section on the right is split into three columns: 'New', 'Match', and 'Existing'. The 'New' column contains a single item 'Any Party Type Groups' (8). The 'Match' column contains a list of filter groups (7) including 'Applicants', 'Main Applicant', 'Current Address', 'Highly Suspect', and 'Suspicious Referral Source'. The 'Existing' column is empty.

- Name** – This box should be populated with the name of the rule. Generally, it is advised to have this as a short form e.g. MRT001, CC001. These names can then be used to group rules together, and will help with MI & reporting.
- Display Name** – This should be populated with a description of the rule's behaviour. For example, 'Same person as Highly Suspect', 'Same telephone number, different address within 90 days'.
- Description** – This can be a more detailed overview of what the rule is doing, and isn't displayed anywhere else within the system. Usually this is populated with the display name of the rule for completeness.
- Rule Score** – This is the score attributed to the rule, generally, the higher the score the higher priority the rule hit is deemed to be. This score can then be used to drive referral priority within tasks.
 - It is recommended instead to use the Dynamic Rule Score functionality, provided as part of the core Luminate FraudIQ Manager solution – so that the rule score is changed automatically based on the fraud propensity of the rule. This means that the rule score associated with a rule doesn't have to be manually changed every time. Luminate FraudIQ Manager learns the performance of the rules and automatically adjusts the score over time.
- View/Hide further settings** – This section expands to allow for additional settings and configuration to be made. This will be explained in more detail below.
- Domain setup** – These options can be added and removed from the selection in order to define which pots of data the rule will fire against e.g. Local data or National Luminate FraudIQ Manager data.
- Preset Filter Groups** – These options are available from the drop-down lists as predefined filters which can be selected and dragged to the 'New' and 'Existing' parts of the rule.
- Rule configuration sections** – This part of the screen is split into three columns, 'New', 'Match' and 'Existing', which is where the filter and match groups are created or dragged onto to build up the rule.

8. Rule Advanced Settings

Upon pressing the 'View/Hide Further Settings' button the below will be displayed on the screen.

abc_ View/Hide Further Settings

Check the Validity of this Rule

- 1. Where applicable, match to at least Existing Entries
- 2. Where applicable, match to a maximum Existing Entries
- 3. Only interested in Existing Entries from the last day(s) to
- 4. A recommendation to the operator if an Entry hits this rule

This allows the user to further refine the rule to behave more specifically depending on how it's been set up.

1. **Where applicable, match to at least x existing entries** – Leaving this value at 1, means that the rule will fire if the incoming application matches to at least 1 existing enquiry. Changing the number to, say 3, will mean that the incoming application has to match to at least 3 distinct existing enquiries before firing. This is particularly useful for detecting multiple enquiries over a time period such as '3 or more applications from the same device within 30 days'.
2. **Where applicable, match to a maximum x existing entries** – This value defaults to 1000 to protect the system, when opening RHS matches, from performance issues. As having to load potentially thousands of matches could cause a significant performance degradation for the Luminate FraudIQ Manager system.
3. **Only interested in Existing Entries from the last x day(s) to x** – These values define the age range of the matching enquiries. This can be particularly useful when optimizing rules in order to define the recency of the matching enquiries.
 - a. The first box defines how far into the **future** the system should look i.e. enquiries with application dates in the future. For example, a policy could be incepted into the system with a policy start date (which is used as application date) in the future. **This value should be prefixed with a '-' e.g. -120 will look at dates 120 days into the future from the incoming application's date.**
 - b. The second box defines how far into the past the system should look i.e. enquiries with an application date in the past. **This value should be just a number. e.g. 30 for 30 days**
4. **Recommendation** – This allows for a small description to be entered that should be used to guide the investigator on how to treat the rule hit e.g. 'possible ID fraud, refer for additional ID checks'.

9. Basic Rule Building – Continued

When creating a new rule, it is useful to bear in mind the following structure when creating and interpreting a rule:

Any incoming application that ...

- ✓ *Meets all the LHS filter criteria defined*
- ✓ *and matches based on ... the matching criteria defined*
- ✓ *Where any existing application meets the ... RHS filter criteria that are defined*

If all the above conditions are met, the rule will fire

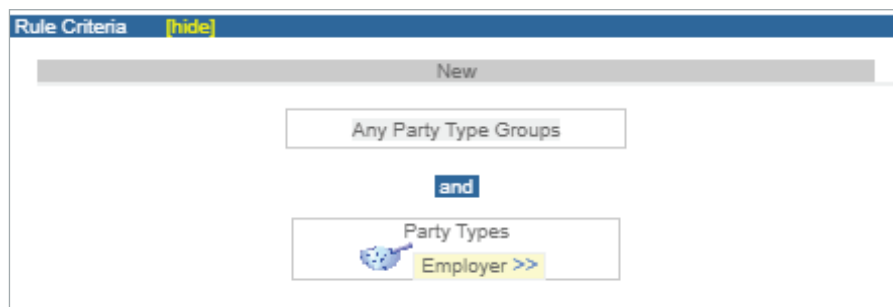
Using the preset filter groups, seen below, you can select system defined filter groups. These are generic and are configured the same for all Luminate FraudIQ Manager systems.

The screenshot shows a table with four columns: Filter, Match, New Group, and Add Level. The 'Filter' column contains a list of filter groups, each with a filter icon (a blue circle with a white 'X'). The 'Match' column contains a dropdown menu for each filter group. The 'New Group' column contains a dropdown menu for each filter group. The 'Add Level' column contains an 'Add' button for each filter group. The filter groups are: Party Type Groups (Applicants), Party Types (Main Applicant, Joint Applicant, Employer, Co-Applicant Employer), Party Sub Types (Highly Suspect), Action Status (Suspicious Referral Source), Reason (Suspicious Referral Source), and Advanced Filter Groups ([Select a Filter Group]).

By clicking and dragging the filter icon, highlighted in the image above, it is possible to create the filters within the rule by dragging the icon onto the LHS or RHS of the rule. When the screen displays a yellow highlight, it means the user can let go of the click and the filter will drop onto the screen.

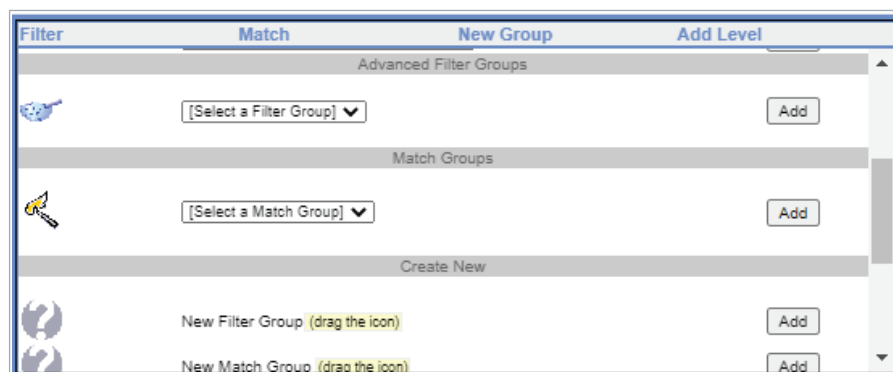
The screenshot shows a rule building interface with a yellow background. It displays a rule structure: 'Any Party Type Groups' followed by 'and' followed by 'Party Types' followed by 'Main Applicant >>'. A filter icon is highlighted on the right side of the screen, indicating it can be dragged onto the rule.

Once the icon is dropped it will be displayed in the column:



The screenshot shows a 'Rule Criteria' panel with a '[hide]' button. Below the header, there is a 'New' button. The main area contains a rule structure: a box labeled 'Any Party Type Groups' followed by an 'and' connector, and then a box labeled 'Party Types' which contains a sub-item 'Employer >>'.

Scrolling down in the Filter and Match group selection area of the page will present the user with an 'Advanced Filter Groups' and 'Match Groups' section:



The screenshot shows a section with four tabs: 'Filter', 'Match', 'New Group', and 'Add Level'. The 'Filter' tab is active, showing a list of 'Advanced Filter Groups'. Each group has a filter icon, a dropdown menu to 'Select a Filter Group', and an 'Add' button. Below this is a 'Match Groups' section with a match icon, a dropdown menu to 'Select a Match Group', and an 'Add' button. At the bottom, there is a 'Create New' section with two options: 'New Filter Group (drag the icon)' and 'New Match Group (drag the icon)', each with an 'Add' button.

These filters and match groups are those that have been configured by Luminate FraudIQ Manager users to serve a specific purpose. Furthermore, they will have been purposefully chosen to be reusable across multiple rules, this means that if a group is used commonly it doesn't have to be created repeatedly across multiple rules.

These groups are sometimes referred to as 'global filters' or 'global match groups'.

10. Defining a Basic Rule

Putting all the aspects of the above section together, putting together a basic rule is simple.

For example, trying to create a rule such as ‘Same Person as Highly Suspect’, across National, would look like this:

The screenshot displays the 'Rule Definition' and 'Rule Criteria' sections of a software interface. The 'Rule Definition' section on the left includes fields for Name, Display Name, Description, Score, and Original Rule Key. The 'Rule Criteria' section on the right shows a visual representation of the rule logic, organized into three columns: New, Match, and Existing. The logic is as follows: 'Any Party Type Groups' (New) AND 'Same Person' (Match) AND 'Any Party Type' (Existing) AND 'Any Party Sub Type' (Existing) AND 'Party Action Status' (Existing) AND 'Highly Suspect' (Existing) AND 'Any Reason' (Existing).

Using the format outlined above ...

Any incoming application that ...

- ✓ Looks at any Party Type/Groups
- ✓ and matches based on ... Same Person
- ✓ Where any existing application meets the ... Action Status of Fraud

If all the above conditions are met, the rule will fire

Building upon this further, if the enquiry in question had multiple Party Types/Groups on the incoming application (left most column) – adding an additional filter to target specific Parties to look like:

Any incoming application that ...

- ✓ Looks at Main Applicant only
- ✓ and matches based on ... Same Person
- ✓ Where any existing application meets the ... Action Status of Highly Suspect

If all the above conditions are met, the rule will fire

This level of configurability allows the rules to be defined to target specific party types or sub party types which is particularly useful when trying to refine rulesets and referral rates.

Further building upon this concept, adding additional criteria to the match group and 'Existing' column (right hand side) can further increase the complexity of the rule.

Any incoming application that ...

- ✓ Looks at Main Applicant only
- ✓ and matches based on ... Same Person AND Different Address AND same IP Address
- ✓ Where any existing application meets the ... Action Status of Highly Suspect AND Reason code is Residential Address Issues

If all the above conditions are met, the rule will fire

To further refine the rule, it may be worth reviewing the options available in the 'Further Settings' section. For example, if the rule should only look at existing enquiries that have a date within 1 year of the incoming enquiries' when evaluating whether to fire the rule:

- Where applicable, match to at least Existing Entries
- Where applicable, match to a maximum Existing Entries
- Only interested in Existing Entries from the last day(s) to
- A recommendation to the operator if an Entry hits this rule

To finalize the rule, ensuring that the rule only targets National data using the domain groups is required. This is done via the 'Domain Group' selector at the top of the Rule Definition block.

Domain Group:

Add Group | Remove Group...

Clicking 'Add Group' provides a drop down of other domains that are available for selection when creating the rule. This list will provide all the available options for the domain that are available for the Luminate FraudIQ Manager system. This will include other local domains (if a multi-domain client) and separate domains within National. By default, these are 'National Luminate FraudIQ Manager – Finance' and 'National Luminate FraudIQ Manager – Insurance', but can also include other data sets, if the system is configured to match those data sets.

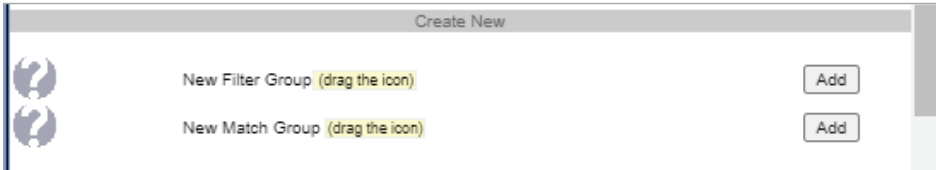
Domain Group:

Address is an Institution
 Address is an Institution
 Death Notice Warning
 Identity Lost or Stolen
 Local group for Equifax Canada
 Lost or Stolen SIN
 Possible Identity Fraud

11. Creating New Filters or Match Groups

If a filter group or match group isn't available as part of the predefined lists – it may be necessary to define them as part of the rule building process. Whilst Equifax Canada sets up a standard list of criteria, this flexibility allows users to create unique filters and match groups in order to fully optimize their rule sets.

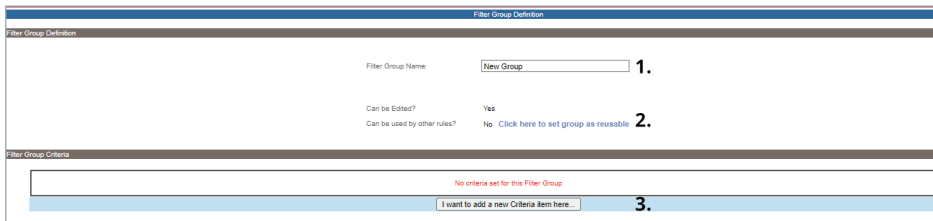
In order to do this – scroll down in the top right-hand setting box in the Rule Definition (top half) of a new rule to see the below:



Clicking and dragging the icon (the question mark symbol) into the required section of the rule i.e. 'New', 'Match' or 'Existing'.

For example, dragging the 'New Filter Group' icon, will present the following screen to the user:

N.b. the screen for a new match group is the same but the terminology is different i.e. 'Match Group Definition'



- 1. Define the Filter/Match Group Name** – This is the display name for the group that will be displayed as part of the rule build. If the rule is set to be shared, then this is the name that will be displayed in the drop-down lists. Best practice is to ensure that the group name is indicative of what the group is doing so that anyone that builds rules can easily understand what the group is doing – without having to drill into the group.
- 2. Can be used by other rules?** – This option dictates whether the group is available as a shared group so that it can be used by other users when creating other rules. Whilst it is possible to create the groups individually each time, usually groups may be reused across multiple rules – this function allows the system to make groups available for reuse. Once the rule has been set to be shared for use in other rules, it can no longer be edited within this screen.
- 3. I want to add a new Criteria Item here** – This button opens up the options to begin building the group criteria, this will be described in more detail below.

12. Defining Group Criteria

After selecting the 'I want to add a new Criteria Item here' button the user will be presented with the below screen:

Filter Group Criteria

No criteria set for this Filter Group

Validation Detail Type: 1.

Field A: 2.

Type of Comparison: 3.

Add | Cancel 4.

1. **Validation Detail Type** – This has two options, for a normal rule build this will remain as 'Single Item'. The other option that may be available depending on the Luminate FraudIQ Manager set up is 'Dual Item' which is used for advanced rule building using transpositions etc. (this will not be detailed in this user guide)
2. **Field A** – This dropdown allows the user to select the data item that will have a comparison performed on it i.e. an item of data the group should be looking at specifically
3. **Type of Comparison** – Depending on the data type of the field that has been selected, such as an Integer or text, the type of comparison options will be reflected accordingly so that the user can define the comparison to undertake on the data item.

String Comparisons

The available list of operators that can be used against string i.e. text data items are shown below:

=
Greater than (a number)
IN (separate values with commas)
IS NOT NULL
IS NULL
Less than (a number)
NOT IN (separate values with commas)

Examples

Postal Code *BEGINS WITH* M5V

Filter Group Criteria

No criteria set for this Filter Group

Validation Detail Type:

Field A:

Type of Comparison:

The value that I am comparing against is:

Add | Cancel

LHS Only : Postal Code BEGINS WITH M5V

Employment Status IN Not Working – No Income, Not Working – Disability Benefit

No criteria set for this Filter Group

Validation Detail Type:

Field A:

Type of Comparison:

The value that I am comparing against is:

Add | Cancel

Employment Status IN (separate values with commas) Not Working – No Income, Not Working – Disability Benefit

IP Address BEGINS WITH 192.168

No criteria set for this Filter Group

Validation Detail Type:

Field A:

Type of Comparison:

The value that I am comparing against is:

Add | Cancel

IP Address BEGINS WITH 192.168

Numeric Comparisons

The available list of operators that can be used against numeric data i.e. numbers are shown below:

<>

<>

=

Greater than (a number)

IN (separate values with commas)

IS NOT NULL

IS NULL

Less than (a number)

NOT IN (separate values with commas)

Examples

Income Greater than (a number) 31,000

No criteria set for this Filter Group

Validation Detail Type:

Field A:

Type of Comparison:

The value that I am comparing against is:

Add | Cancel

LHS Only : Income Greater than (a number) 31000

Term of Loan less than (a number) 30

Validation Detail Type:

Field A:

Type of Comparison:

The value that I am comparing against is:

Add | Cancel

LHS Only: Term Less than (a number) 30

For some data items, the values that are going to be used in the filter are made available in a dropdown list for selection.

The value that I am comparing against is:

1

x

<

Highly Suspect

[Add](#) | [Cancel](#)

Gender = Male

Action Status IN Highly Suspect, Suspect

Validation Detail Type:	Single Item ▾		
Field A:	Action Status ▾		
Type of Comparison:	IN ▾		
The value that I am comparing against is:	1,13	x	< ▾ Suspect
Add Cancel			
Action Status IN Highly Suspect,Suspect			

13. Enhanced Rule Functionality

The ERT engine provides additional functionality that is available for users to create more complex and refined rules in accordance with their organizational risk strategy.

Does Not Match or Not Present (match groups)

In order for a successful match to be generated, information has to be available on both the incoming and existing enquiry. Data has to be present.

ERT can now treat data not being present on either the incoming or existing enquiry as a 'do not match' argument. This helps remove gaps in data matching where data quality may be an issue.

The screenshot shows the 'Match Group Criteria' interface. At the top, a message states 'No criteria set for this Match Group'. Below this, the 'Match Detail Type' is set to 'Single Item'. The 'New Field' is 'Bank account number'. The 'Type of Comparison' dropdown menu is open, showing options: 'Does Not Match' (selected), 'Does Not Match or Not Present', 'Match', 'Both match or both blank', and 'MATCH IF PRESENT'. The preview area at the bottom shows 'Bank account number Does Not Match'.

Date Tolerances (match groups)

Being able to match enquiries that are within a certain time frame adds an additional layer of refinement above and beyond those available within the advanced settings of the rule build. This functionality can be applied to any date data if requested.

There are four options provided when using date tolerances:

1. Greater than +X Days
2. Less than +X Days
3. Greater than -X Days
4. Less than -X Days

This allows the user to create a single timeframe ...

For example, *claim date is less than 10 days from policy inception date*

.... or use them in combination to define a specific time period ...

For example, *claim date is less than 31 days and greater than 19 days (between 20 – 30 days) from policy inception date*

The screenshot shows the 'Match Group Criteria' interface. At the top, a message states 'No criteria set for this Match Group'. Below this, the 'Match Detail Type' is set to 'Single Item'. The 'New Field' is 'Enquiry Date/Time Tolerance'. The 'Type of Comparison' dropdown menu is open, showing options: 'Greater Than +x Days' (selected), 'Less Than +x Days', 'Greater Than -x Days', and 'Less Than -x Days'. The 'X Value' is set to '19'. The preview area at the bottom shows 'Enquiry Date/Time Tolerance Greater Than +x Days (where X = 19)'.

Postal code wildcard (match groups)

The previous rule engine could support exact matching on postal codes only. The ERT engine allows for matching on postal codes using wildcards to refine the matching criteria accordingly. This is particularly useful when matching on postal code areas as opposed to specific postal codes. This functionality can be applied to any string data item if requested.

There is one option to select from for this comparison:

- All but last X characters match

Where X is the number of characters that should be ignored when doing the matching, shown in the example below.

For example:

Same person and postal code where all but last 2 characters of the postal code match

The screenshot shows the 'Match Group Criteria' form. At the top, it says 'No criteria set for this Match Group'. Below this, the 'Match Detail Type' is set to 'Single Item'. The 'New Field' is 'Postal Code Wildcard'. The 'Type of Comparison' is 'All but last X characters match'. The 'X Value' is set to '2'. At the bottom, there is a summary bar that reads 'Postal Code Wildcard All but last X characters match (where X = 2)'.

Numeric Tolerance (match group)

This function operates in a similar way to the date tolerance match groups. It is possible to compare the incoming enquiry to a matching enquiry and calculate the difference between a number, usually salary/income etc. This is particularly useful when trying to detect income manipulation across products/services or across enquiries as they're updated. This functionality can be made available for use against any number data item if requested.

There are four options to select from when doing numeric tolerance difference:

1. Greater than +X%
2. Less than +X%
3. Greater than -X%
4. Less than -X%

The four options can be used individually or in combination with each other in order to form boundaries, as some tolerance between a salary, for example, may be acceptable.

The screenshot shows the 'Match Group Criteria' form. At the top, it says 'No criteria set for this Match Group'. Below this, the 'Match Detail Type' is set to 'Single Item'. The 'New Field' is 'Salary Tolerance'. The 'Type of Comparison' is 'Greater Than +x%'. The 'X Value' is set to '10'. At the bottom, there is a summary bar that reads 'Salary Tolerance Greater Than +x% (where X = 10)'.

Fuzzy Matching (match groups)

ERT now supports fuzzy matching capabilities in order to help improve match rates across data. Currently the data items that support fuzzy matching are forename and surname. Equifax Canada will continue to review additional data items to see if there would be value to add fuzzy matching to other data items such as company name.

Fuzzy Surname (dbl_metaphone)
Fuzzy Surname (metaphone)
Fuzzy Surname (nysiis)
Fuzzy Surname (refinedsoundex)
Fuzzy Surname (soundex)

It is possible to select multiple or single phonetic functions in order to create the match criteria. This allows for further refinement of the rule to only match using certain matching functions.

Rules can be built using these criteria in the same manner as you would a normal match group.

Application Age

It is possible to create a filter in order to define the age of application at the point of inception.

For example:

Same person as clear within 1 hour, matching to at least 3 enquiries

Validation Detail Type:	Single Item
Field A:	Application Age (Hours)
Type of Comparison:	Less than (a number)
The value that I am comparing against is:	1
Add Cancel	
Application Age (Hours) Less than (a number) 1	

1.855.233.9226 • consumer.equifax.ca/business

© Equifax Canada Co., 2021. All rights reserved. This User Guide is provided for informational purposes only to you as a Customer of Equifax Canada. This User Guide should not be shared, distributed, or reproduced, nor should it be interpreted as business or legal advice. Users of this informational User Guide should contact their own legal representatives for legal advice. Please note that the contents of this User Guide may be subject to change without notice.