Euronext RiskGuard – How the service works

Functional overview of Euronext Pre-Trade Risk Management on Derivatives markets

7 NOVEMBER 2022

EURONEXT

Table of contents

Preface

PURPOSE

Euronext RiskGuard is the Euronext pre-trade risk management service providing Risk Managers at Clearing or Trading Member firms of Euronext the ability to monitor their clients' or firm's risk exposure.

This document describes how to service works for Euronext Derivatives markets.

TARGET AUDIENCE

This document should be read by Risk Managers at General Clearing Members (GCMs) and Trading Members who use the Euronext RiskGuard service through either its web-based User Interface or FIX 5.0 API.

This document must be read in conjunction with the documents below. General information about the service can be found under the Trading Services section of the Euronext website here: RiskGuard.

ASSOCIATED DOCUMENTS

The following lists the associated documents, which either should be read in conjunction with this document or which provide other relevant information for the user. These documents can be found in the Euronext Connect Portal from the RiskGuard page

- Euronext Cash and Derivatives markets - OEG FIX 5.0 Messages - Interface Specifications
- Euronext RiskGuard - MyEuronext User Guide
- Euronext RiskGuard Access User Guide

CONTACTS

For further information about this document or RiskGuard service, please contact:

- Your Euronext Relationship Manager or the Operational Client Services (OCS) at clientsupport@euronext.com
- For access to the service, the Euronext Membership team at EuronextMembership@euronext.com and Customer Access Services team at cas@euronext.com
- For any queries related to the service in production, the Euronext Market Services (EMS) team

Available 06:30-22:30 CET
Telephone:

France: +33 1 8514 8585
The Netherlands: +31 20 721 9585
UK: +44 20 7660 8585
Belgium: +32 2 620 0585
Portugal: +351 2 1060 8585

Derivatives desk email:
ClientSupport@euronext.com

WHAT'S NEW?

VERSION NO.	DATE	AUTHOR	CHANGE DESCRIPTION
1.0	Nov 2022		Initial version

1. Glossary and general definitions

The table below lists the key terms of Euronext RiskGuard service. For each term is given a general definition.

NAME	GENERAL DEFINITION
ClientIdentificationShortCode	The short code of the Member's client. It can be the ID representing either the Legal Entity Identifier ("LEI") or the relevant individual.
Contract	A Futures or Options Derivatives contract whose value is based upon an underlying asset (e.g. a stock) or a basket of assets (e.g. an Index).
MyEuronext	The Euronext portal providing access to the RiskGuard User Interface
ExecutionWithinFirmShortCode	The short code of the algo, the relevant individual, or the client that submitted the execution to the system. This definition is specific to the RM Services and does not reflect the use and regulatory meaning of the term more generally.
Firm ID	The unique code used to identify a Euronext Trading Member of Euronext markets
FIX	Financial Information eXchange (FIX) electronic communication protocol
General Clearing Member (GCM)	A General Clearing Member (GCM) is an entity that has been approved by the clearing house for the clearing of principal transactions (transactions dealt on its own account) and client transactions on behalf of its clients (Non-Trading Members)
Individual Clearing Member (ICM)	An Individual Clearing Member (ICM) is an entity that has been approved by the clearing house for the clearing and the settlement of transactions dealt for its own account, or allocated to it
Logical Access	An Order Entry Gateway ("OEG") entry point, set up for clients to connect to a single Optiq Segment
Market Operations	The Euronext Market Surveillance team
Matching Engine	The Optiq Matching Engine, i.e. the software that manages the trading services for the Euronext markets on Optiq
Member	The entity that is involved in trading

Membership Segment	The list of instruments in relation to which a Risk Member monitors a Member. **Membership Segment ID** means the three letters comprising the identifying code for the Membership Segment. Within the scope of RiskGuard, it is also referred to as **Subscriptions**
Non-Clearing Member (NCM)	A trading member that is not a member of the clearing house and therefore does not have any license to clear its transactions. The NCM must have an agreement with a clearing member before being allowed to trade.
Optiq	Euronext's proprietary multi-market full trading chain technology platform
Optiq Segment	A universe of instruments sharing common trading properties
Order Entry Gateway (OEG)	The software that manages the access for Exchanges' clients, and acts as the private interface between the clients and the Optiq Matching Engine
RiskGuard Clearer	A clearing firm that is a participant in the Risk Management Services provided by Euronext and governed by the Risk Management Services Agreement
RiskGuard Member	A Member of Euronext that is a participant in the Risk Management Services provided by Euronext and governed by the Risk Management Services Agreement
Risk Manager	The person who occupies the risk management position at a Risk Member entity. One Risk Member can have multiple Risk Managers.
Risk Member	The entity that uses the RiskGuard service to monitor Members and clients for financial risk management purposes. Risk Members may be part of either a RiskGuard Clearer or a RiskGuard Member.
Self-Monitoring	Indicates the status of a RiskGuard Member in relation to the risk monitoring of trading activity on the Euronext markets. In contrast to the Riskguard Clearer, a Self-Monitoring RiskGuard Member performs their activities solely for the scope of their particular Member Firm.

2. Introduction

The Euronext RiskGuard service for Euronext derivatives markets (Equity derivatives, Financial derivatives and Commodity derivatives) is designed to provide Risk Managers at Clearing and Trading Member firms the ability to set pre-trade risk controls in order to manage their customers' or firm' risk exposure in real-time.

The following pre-trade risk controls are available for Euronext derivatives markets :

- 'Suspend' or so-called "Kill Switch" / 'Unsuspend'

- Order Size Limit (OSL)

- 'Block' or so-called 'Contract Restrictions' / 'Unblock'

2.1 RiskGuard users' profile

Participants authorised to use the Euronext RiskGuard service are referred to as **Risk Members**.

The Risk Member corresponds to the firm that uses the Euronext RiskGuard service to monitor its customers' or firm's risk exposure. The Risk Member can be either:

- In the organisation of a General Clearing Member (GCM) or so-called **RiskGuard Clearer** in this document. RiskGuard Clearers can set or amend risk controls of their NCMs at a Member Code (Optiq Firm ID) level only.

- In the organisation of a Non Clearing Member (NCM) or Individual Clearing Member (ICM), or so-called **RiskGuard Member** in this document. RiskGuard Members can set or amend risk controls for their whole trading firm i.e. at the Firm ID, or for a subset of the Firm ID, i.e. at a Logical Access, or a short code (ExecutionWithinFirmShortCode or ClientIdentificationShortCode) level.

If the Risk Member is a NCM or ICM, the Risk Member is said to be *risk self-monitoring* as he is only allowed to monitor its firm's and client's exposure to Euronext derivatives markets.

The Risk Member (RiskGuard Clearer and RiskGuard Member) is identified by its Firm ID, a 8 alphanumerical code.

Trading members of Euronext also having a General Clearing status at the CCP level could use the service both as a RiskGuard Member and as a RiskGuard Clearer through the same Member Code.

- When using the User Interface, Risk Managers are provided the ability to select whether they want to access as a RiskGuard Clearer or as a RiskGuard Member. At any point of time, they can switch from one profile to the other. Please refer to the Access User Guide for more details.

- When using the Optiq OEG FIX 5.0 API, participants should pay attention to the format of the message as there is no dedicated Logical Access for RiskGuard Clearers or RiskGuard Members.

RiskGuard users within an authorised Risk Member refer to as **'Risk Managers'**.

- **Risk Manager**. The Risk Manager corresponds to a user of the Euronext RiskGuard service. A Risk Manager necessarily belongs to a Risk Member. A Risk Member can have several Risk Managers. The Risk Manager can set, amend, delete pre-trade risk controls available in the service.

  - A GCM Risk Manager is necessarily in the organisation of a Euronext RiskGuard Clearer

  - A NCM Risk Manager is necessarily in the organisation of a Euronext RiskGuard Member

Risk Managers also refer to Risk Agents in the Connect portal. Please refer to the RiskGuard User Access Guide for more details.

2.2 Subscription

A Risk Member is provided the ability to set risk controls only for pre-defined lists of contracts, that refer to the **Subscriptions**.

A Subscription corresponds to a list of contracts that are part of a Market segment that a Risk Member monitors for a customer or its firm. Risk controls within RiskGuard are always restricted to the subscriptions between the Risk Member and the risk-monitored entity, i.e.

- For a RiskGuard Clearer, the set of subscriptions correspond to the clearing agreement in place between the GCM and the NCM

- For a RiskGuard Member, the set of subscriptions correspond to all markets covered by the membership application of the trading member firm

2.3 How to access the Euronext RiskGuard Service

There are two ways to access to the Euronext RiskGuard Service:

1. Through the Optiq OEG FIX 5.0 API

2. Through the RiskGuard web-based User Interface, available from MyEuronext

In order to access the Euronext RiskGuard service:

- **Step 1**. Any Euronext RiskGuard Participant must sign a **'Risk Management Services Agreement'** with Euronext.

- **Step 2**. Clearing Members and Euronext Trading Members are also required to sign a **'Statement of Authority'** allowing the Risk Managers to access and use the Risk Management Services.

  - Euronext Trading Members who wish to make use of Euronext RiskGuard to self-monitor the risk of their firm must sign the *'Statement of Authority to be signed by a Member in respect of its business executed on the Euronext markets'*

  - Clearing Member (GCM) wishes to make use of Euronext RiskGuard in respect of a Member for which it provides clearing services, the Clearing Member and the Member are required to sign together a *'Statement of Authority to be signed by a Trading Member and its relevant Clearing Member on the Euronext Markets'*

- **Step 3.** Risk Members should sign the specific MyEuronext Terms & Conditions whatever they intend to use the User Interface or only connect through the FIX API.

These duly signed documents must be returned to EuronextMembership@euronext.com.

Please note that access to the service will only be granted after the signature of these documents.

- **Step 4.** Risk Members willing to use the FIX API must order the dedicated RiskGuard Logical Access for EUA and Production (once conformance will be successfully completed).

2.4 Important general processing notes

The following provides important general notes related to the processing of RiskGuard actions in the Optiq Matching Engine.

These notes apply to all controls provided to clients under the RiskGuard service, **and** whatever the commands have been sent using the FIX API or through the MyEuronext RiskGuard User Interface.

1. A single RiskGuard command is always applicable, at minimum, to a Contract, and at maximum, to an Optiq segment.

2. Where several Risk Managers send the same command with the same granularity and referential scope, the system records all such commands, and takes into account the most restrictive setting that is in place at any given time. This means that all restrictions (Suspension / Block) from all Risk Managers need to be lifted in order to restore access.

3. Where both Market Operations, through the Kill Switch mechanism, and the Risk Manager, through RiskGuard (FIX API and / or MyEuronext User Interface), act for the same market participant, the system takes into account all such actions, and applies the most restrictive setting that is active at any given time. This means that both restrictions (Suspension / Block) from the Market Operations and the Risk Manager need to be lifted in order to restore access.

4. All actions submitted by the Risk Manager for a broader granularity (e.g. Firm ID or Logical Access) are automatically applied to the available narrower granularity (e.g. Logical Access or short code). E.g., Order Size Limit configured at Firm ID level is applicable to the orders submitted by the Member in any of the Logical Accesses on which it is authorized to submit orders.

   a) A command submitted for a Firm ID will apply to both all associated logical Accesses and short codes subject to the command. If the Firm ID that owns a Logical Access is suspended or blocked, any other Firm IDs that may be setup as executing for that Logical Access will also be suspended or blocked.

   b) A command submitted to a specific Logical Access will apply only to that Logical Access on that Optiq segment. If a Logical Access is suspended or blocked, all the Firm IDs that may be identified as entering or executing on that Logical Access will be subject to the suspension or block.

   c) A Firm ID may have multiple Logical Accesses; and a single short code may be present on multiple Logical Accesses of the same firm. A command submitted on an Optiq Segment to the Firm ID + short code will apply to all orders, on all Logical Accesses where this Firm has submitted orders with the identified short code.

5. In case of emergency, Risk Members can contact Market Surveillance to perform a RiskGuard command **on their behalf**. A dedicated *On Behalf* procedure will apply. Please note that a command can be set by a Risk Manager through the FIX API or the User Interface, and in case of emergency, lifted by Market Surveillance on behalf of the Risk Member. *Note that as per MiFID rules, Euronext Market Surveillance can perform a suspend. Such a command should be considered outside of the scope of RiskGuard and as a consequence can only be lifted by Market Surveillance.*

6. All commands are effective in real-time and remain persistent.

7. By default, no Block, neither OSL value are set, and Members have a Unsuspended status.

3. The Suspend / Unsuspend commands

The '**Suspend**' or so-called '*Kill Switch'* functionality provides Risk Managers the ability via a single command to halt trading activity on all subscriptions of an Optiq segment.

A Risk Manager belonging to a RiskGuard Clearer can only Suspend / Unsuspend at Member level *(Firm ID*) while a Risk Manager from a RiskGuard Member can Suspend / Unsuspend at Member, Logical Access, ExecutionWithinFirm and ClientIdentification short code level.

As the result of the Suspension:

- Risk-monitored traders are not logged off but further order and quote entry is rejected,

- Open orders including GTCs might be deleted (when option to Pull was selected),

- Impacted traders of the risk-monitored entity are notified through their trading interface that they have been suspended by their RiskGuard Clearer or their RiskGuard Member and may additionally receive specific pull notification messages.

The risk-monitored entity is excluded from trading until the Risk Manager explicitly reinstates it through the 'Unsuspend' functionality.

As the result of the Unsuspension:

- Impacted traders of the risk-monitored entity are notified of their Unsuspended status. They can then resubmit orders in all subscriptions of the Optiq segment.

The Suspend or Unsuspend command always applies to all Contracts of the Optiq segment, i.e.:

- When triggered by a RiskGuard Clearer: all subscriptions for which there is a clearing agreement between the GCM and the NCM, on a given Optiq segment

- When triggered by a RiskGuard Member: all trading subscriptions of the member's Firm ID(s) on a given Optiq segment.

The Suspend and Unsuspend commands can be triggered anytime during the day from when Optiq starts in the morning (before market opens) until session close at the end of the day.

3.1 The Suspend (i.e. 'kill switch') command

The Suspend ('Kill Switch') functionality can be triggered through the OEG FIX API using the ERGCommand (U68) message with the fields *ERGActionType (tag: 21097)* set to '1' (Suspend). Risk Managers also have the ability to trigger the Suspend command in the User Interface via a dedicated window. Access to the Kill Switch command in the User Interface is limited to specific Risk Managers

that have been previously granted to perform the command (please refer to the User Guide for further details).

The Suspend command can be triggered at different levels:

- Suspension of the Member at the Firm ID level for a given Optiq segment *(TargetFirmID (tag: 21098*) in the Optiq FIX API)

- Suspension of the Member for a given Logical Access on a given Optiq segment (*TargetLogicalAccessID (tag: 21099)* in the Optiq FIX API)

- Suspension of the Member for a given ExecutionWithinFirmShortCode level on a given Optiq segment (*TargetPartyID (tag: 21095)* in the Optiq FIX API)

- Suspension of the Member for a given client identified using its short code on a given Optiq segment (*TargetClientShortCode (tag 21108)* in the Optiq FIX API)

Note that a Risk Manager belonging to a RiskGuard Clearer can only suspend at Member level while a Risk Manager from a RiskGuard Member can suspend at Member, Logical Access, ExecutionWithinFirm and ClientIdentification short code levels.

As the Suspend is always effective at an Optiq Segment level, if a Risk Member wants to completely Suspend a Member on all the segments where they have trading or clearing authorizations, one Suspend command per Optiq segment must be sent. Through the User Interface, Risk Members are provided the ability to view and select all the active Optiq segments of the risk monitored entity, and therefore submit only one single request; the Matching Engine nevertheless manages one request per segment.

Risk Members have the ability to **optionally pull orders** when triggering a Suspend command through the API or the User Interface (the *Purge (tag: 21100)* must be set to 'Y' (True) when using the Optiq FIX API).

When a Risk Manager suspends a Member, the suspension is restricted to the subscriptions that are common between the Risk Member and the Member, that means:

- When triggered by a RiskGuard Clearer: all subscriptions for which there is a clearing agreement between the GCM and the NCM, on a given Optiq segment

- When triggered by a RiskGuard Member: all trading subscriptions of the member's Firm ID (s) on a given Optiq segment.

Upon receipt of this command, the Matching Engine will check that the Risk Member has the authorization to submit the Suspend command for the target Member.

Following a Suspend Command a message (ERGCommandAck (U69) through the API) is sent back to notify the Risk Managers about the success or failure of the operation. Risk Managers using the User Interface are also notified through a dedicated alert.

Clients accessing the service through the MyEueronext User Interface **and** the Optiq FIX API should note that when a Suspend command is triggered via the User Interface, **the notification message is not only sent to the user who triggered the operation through the User Interface but also to the Risk Member's RiskGuard Logical Accesses.**

The suspension results in the following:

- The Suspended Member (fully or partially when the request is done at a finer level than the Firm ID) is notified via a dedicated message (User Notification (39) / FIX CB) message with a dedicated User Status. The User Status varies depending on the level at which the Suspend command applies, i.e. Member Firm ID, Logical Access, ExecutionWithinFirmCode, ClientIdentificationShortCode.

- All subsequent orders are rejected. The scope of orders being rejected depends on the level of the submitted Suspend command, i.e. if a Suspend command is at a Logical Access level, only orders from the suspended Logical Access will be rejected. The Member can continue to submit orders through the other Logical Accesses. .

- The Suspended Member only has the ability to pull orders for the suspended Firm ID, Logical Access, short codes.

If the Risk Manager selected the option to pull orders, all active orders, including GTC (Good Till Cancel), wholesale trades awaiting validation and RFCs are pulled. The scope of the orders pulled depends on the level of the Suspend command.

- For a Suspend at Firm ID level, all orders submitted by the Member on the target Optiq segment are pulled

- For a Suspend at Logical Access level, all orders submitted by the Member via the target Logical access are pulled

- For a Suspend at the ExecutionWithinFirmShortCode level, all orders submitted by the Member with the target short code are pulled

- For a Suspend at the ClientIdentificationShortCode level, all orders submitted by the Member for the target client short code are pulled.

The Member is explicitly notified that orders have been pulled as a result of an action from its Risk Manager.

The Member is not logged off as a result of a successful Suspend Command and may continue trading on other segments, sessions or short codes not in the scope of the command.

The Suspend status is final and a Member stays so suspended until a Risk Manager unsuspends it. The Suspend status is persistent across trading sessions and trading days until an explicit Unsuspend command is submitted.

*Please note that **all** orders, order revisions and quotes from all market participants are being checked against the Suspended status.*

3.2 The Unsuspend command

The Unsuspend functionality can be triggered through the OEG FIX API using the ERGCommand (U68) message with the field *ERGActionType (tag: 21097)* set to '2' (Unsuspend). Risk Managers also have the ability to trigger the Unsuspend command through the MyEuronext User Interface via a dedicated window. Access to the Unsuspend command in the User Interface is limited to specific Risk Managers that have been previously granted to perform the command (please refer to the RiskGuard Access User Guide for further details).

An Unsuspend command can be triggered at different levels:

- Unsuspension of the Member at the Firm ID level for a given Optiq Segment (*TargetFirmID (tag: 21098)* in the Optiq FIX API)

- Unsuspension of the Member for a given Logical Access on a given Optiq Segment (*TargetLogicalAccessID (tag: 21099)* in the Optiq FIX API)

- ExecutionWithinFirmShortCode level on a given Optiq Segment (*TargetPartyID (tag: 21095)* in the Optiq FIX API)

- Unsuspension of the Member for a given client identified using its short code for a given Optiq segment (*TargetClientShortCode (tag: 21108)* in the Optiq FIX API)

As the Unsuspend is always effective at an Optiq Segment level, if a Risk Member wants to completely Unsuspend a Member on all the segments where they have trading or clearing authorizations, one **Unsuspend** command per Optiq segment must be sent. Through the User Interface, Risk Members are provided the ability to view and select all Optiq segments on which the risk monitored entity is Suspended, and therefore submit only one single request; the Matching Engine nevertheless manages one request per segment.

Important note: Note that the Matching Engine takes into account the most restrictive setting. If a risk monitored entity has therefore been suspended at several levels by its RiskGuard Member, it is possible that a Member cannot resume full trading until all restrictions have been lifted.

When a Risk Manager Unsuspends a Member, the suspension is restricted to the Membership Segments that are in common between the Risk Member and the Member, that means:

- When triggered by a RiskGuard Clearer: all subscriptions for which there is a clearing agreement between the GCM and the NCM, on a given Optiq segment

- When triggered by a RiskGuard Member: all trading subscriptions of the member's Firm ID(s) on a given Optiq segment.

It is not required that the same Risk Manager unsuspends a Member they have previously suspended. Any Risk Manager belonging to the same Risk Member can unsuspend a Member that another Risk Manager has suspended. This applies whatever the suspension was performed through the FIX API or through MyEuronext User Interface.

Upon receipt of the relevant command, the Matching Engine checks that the Risk Member has the authorization to submit the Unsuspend command for the target Member.

Following a Unsuspend Command a message (ERGCommandAck (U69) through the Optiq FIX API) is sent back to the Risk Manager to confirm the success or failure of the operation. Risk Managers using the MyEuronext User Interface are also notified through a dedicated alert.
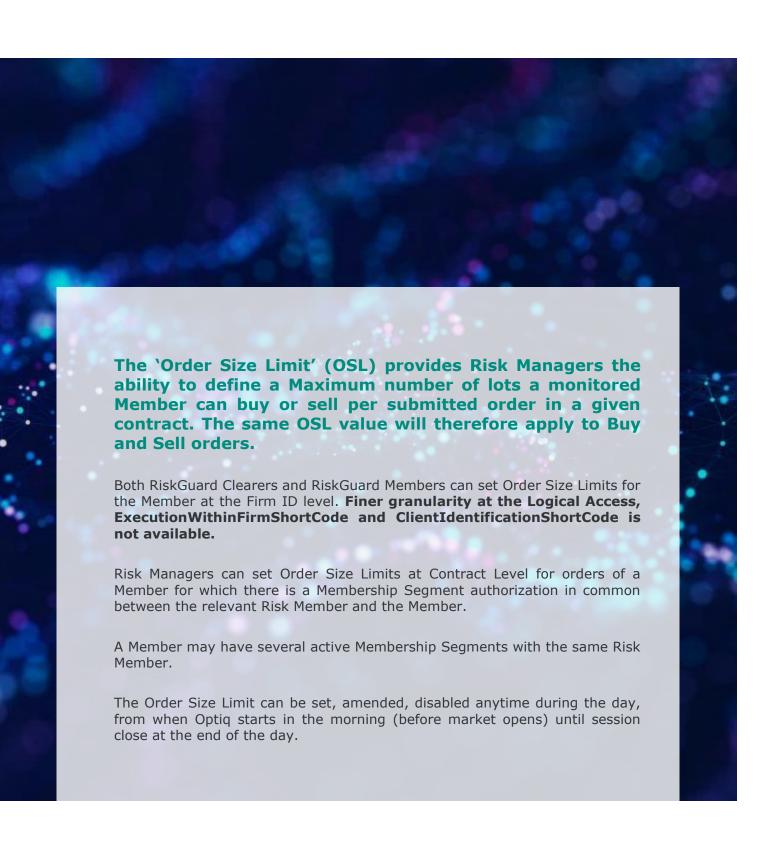
The unsuspension results in the following:

- The Unsuspended Member is notified via a User Notification (39) / FIX (CB) message with a dedicated User Status. The User Status varies depending on the level at which the Unsuspend command applies, i.e. Member Firm ID, Logical Access, ExecutionWithinFirmCode, ClientIdentificationShortCode

When a Member is unsuspended, it can resume normal trading on the contracts constituting the Membership Segment. Please note that orders pulled due to a previous suspension are never restored.

4. The Order Size Limit (OSL)

The 'Order Size Limit' (OSL) provides Risk Managers the ability to define a Maximum number of lots a monitored Member can buy or sell per submitted order in a given contract. The same OSL value will therefore apply to Buy and Sell orders.

Both RiskGuard Clearers and RiskGuard Members can set Order Size Limits for the Member at the Firm ID level. **Finer granularity at the Logical Access, ExecutionWithinFirmShortCode and ClientIdentificationShortCode is not available.**

Risk Managers can set Order Size Limits at Contract Level for orders of a Member for which there is a Membership Segment authorization in common between the relevant Risk Member and the Member.

A Member may have several active Membership Segments with the same Risk Member.

The Order Size Limit can be set, amended, disabled anytime during the day, from when Optiq starts in the morning (before market opens) until session close at the end of the day.

4.1 The activation of the Order Size Limit

The Order Size Limit (OSL) for a Contract can be set / amended through the FIX API using the ERGCommand (U68) messages with the field *ERGActionType (tag: 21097)* set to '5' (Order Size Limit). A dedicated field *OSLFlag (tag: 21101)* must be set to 'Y' (True) to activate or amend the Order Size Limit. One FIX message per Contract must be sent.

Risk Managers using the MyEuronext User Interface are also provided the ability to set OSL. Through the User Interface is given the ability to the Risk Manager to set the same OSL value for multiple Contracts at once, i.e. belonging to the same subscription (please refer to the MyEuronext User Guide for further details).

Important note: An Order Size Limit equal to 0 will result in all orders to be rejected in the Contract.

Upon receipt of this command, the Matching Engine will check that the Risk Member has the authorization to set / amend OSL parameters for the target Member.

Following the submission of the command a message is sent back to the Risk Manager to confirm the success or failure of the operation. The Member is notified via a User Notification (39) / FIX (CB) message with a dedicated User Status. The notification includes the value of the OSL Limit. Risk Managers using the MyEuronext User Interface are also notified through dedicated alerts.

Once an Order Size Limit has been set, each time an order is submitted or revised by the risk monitored Member, the Matching Engine checks the order quantity against any OSL value set for the Member in the Contract. Otherwise no OSL control is applied.

The Order Size Limit applies to new orders and order revisions as well as quotes. Delta-neutral trades, RFCs, and wholesales trades are excluded.

*This implies that **all** orders, order revisions and quotes are being checked against the Order Size Limit, whatever a value has been set or not by the Risk Manager. This therefore guarantees fairness between all trading participants.*

Orders or quotes exceeding the Order Size Limit are rejected and the Member notified of this rejection.

A Member can be subject to only **one** OSL per Contract and per type of Risk Manager. However, a Member can be subject to a limit set by the RiskGuard Clearer's Risk Manager as well as a different limit set by its RiskGuard Member's Risk Manager. When submitting an order, the Matching Engine will validate the two limits and will reject the order based on the lowest, i.e. the most restrictive one.

Important note: The OSL values remain persistent across trading days.

4.1.1 ORDER SIZE LIMIT FOR STRATEGIES

The Order Size Limit is set for outright Contracts.

Risk Managers do not have the ability to set a different value of OSL for strategies.

When a strategy order is submitted by a risk monitored order, the order is checked at the level of the head of the strategy.

Orders on delta-neutral strategies are not checked against the Order Size Limit defined for the underlying Contract of the strategy.

4.1.2 ORDER SIZE LIMIT FOR EXPIRIES

All expiries of the Contract are subject to the same Order Size Limit. Risk Managers do not have the ability to set a different value for the Front Month.

4.2 The de-activation of the Order Size Limit

Risk Managers can disable the OSL that has previously been set using the ERGCommand (U68) message with the field *ERGActionType (tag: 21097)* set to '5' (Order Size Limit) and the field *OSLFlag (tag: 21101)* set to 'N' (False). One message per Contract must be sent.

Risk Managers using the MyEuronext User Interface are also provided the ability to de-activate (delete) OSL. Through the User Interface is given the ability to the Risk Manager to delete the OSL value for multiple Contracts at once, i.e. belonging to the same subscription. The Matching Engine will still process one command per Contract.

An Order Size Limit can only be disabled at the Firm ID level.

Following the submission of the command a notification message is sent back to the Risk Manager to confirm the success or failure of the operation. The Member is notified via a User Notification message with a dedicated User Status. Risk Managers using the User Interface are also notified through dedicated alerts.

5. The Block / Unblock commands

5.1 The Block command

The 'Block' or so-called 'Contract Restriction' functionality provides Risk Managers the ability via a single command to prevent the risk monitored trading entity from submitting orders in a specific contract when the Risk Manager is aware that the 'trader does not permission to trade a specific financial instrument'.

Risk Managers optionally have the option to pull resting orders in the Contract.

As the result of the Block command:

- Risk-monitored traders are not logged off but further order and quote entry in the contract is rejected,

- Trading in other Contracts of the risk monitored Member is not impacted,

- In the event that the block command includes a pull action, relevant orders and quotes are deleted and impacted traders of the risk monitored entity receive specific pull notification messages and are notified through their trading interface that they have been 'Blocked by their 'RiskGuard Clearer' or their 'RiskGuard Member'.

The risk-monitored entity is excluded from trading in the Contract until the Risk Manager explicitly reinstates it through the 'Unblock' functionality.

As the result of the Unblock:

- Impacted traders of the risk-monitored entity are notified of their Unblocked status. They can then resubmit orders in the contract.

Both RiskGuard Clearers and RiskGuard Members can set Block commands for the members they are monitoring, i.e.

- When triggered by a RiskGuard Clearer: any contract within the subscriptions included in the clearing agreement between the GCM and the NCM,

- When triggered by a RiskGuard Member: any contract within the member's trading subscriptions.

The Block and Unblock commands can be triggered anytime during the day from when Optiq starts in the morning (before market opens) until session close at the end of the day.

The Block command can be triggered through the OEG FIX API using the ERGCommand (U68) message with the fields *ERGActionType (tag: 21097)* set to '3' (Block).

Risk Managers using the User Interface are also provided the ability to trigger the Block command. Through the User Interface is given the ability to the Risk Manager to set the command for multiple Contracts at once, i.e. belonging to the same subscription. The Matching Engine will still process one command per Contract.

A Block command can be triggered at different levels:

- Block the whole Member at the Firm ID level in the target Contract (*TargetFirmID (tag: 21098)* in the Optiq FIX API)

- Block the Member for a given Logical Access in the target Contract (*TargetLogicalAccessID (tag: 21099)* in the Optiq FIX API)

- Block the Member for a given Logical Access in the target Contract (*TargetPartyID (tag: 21095)* in the Optiq FIX API)

- Block the Member for a given Logical Access in the target Contract (*TargetClientShortCode (tag 21108)* in the Optiq FIX API)

Note that a Risk Manager belonging to a RiskGuard Clearer can only set the control at Member level while a Risk Manager from a RiskGuard Member can set the control at Member, Logical Access, ExecutionWithinFirm and ClientIdentification short code levels.

The Block control can only be set for a given Contract of an Optiq Segment, meaning that if a Risk Member using the API wants to block a Member from submitting orders in multiple contracts, multiple ERGCommand messages per Contract and per Optiq segment must be sent.

Risk Members have the ability to **optionally pull orders** when setting a Block control through the FIX API or the User Interface (the *Purge* (tag: 21100) must be set to 'Y' (True) when using the Optiq FIX API).

Upon receipt of this command, the Matching Engine checks that the Risk Member has the authorization to set such a control for the target Member.

Following a Block Command a message is sent back to the Risk Manager confirm the success or failure of the operation. Risk Managers using the MyEuronext User Interface are also notified through dedicated alerts.

The block command results in the following:

- The Member is notified via a User Notification (39) / FIX CB) message with a dedicated User Status. The User Status varies depending on the level at which the Block command applies, i.e. Member Firm ID, Logical Access, ExecutionWithinFirmCode, ClientIdentificationShortCode.

- All subsequent orders in the given Contract are rejected. The scope of orders being rejected in the target Contract depends on the level of the Block control i.e. if Block control has been set for a Logical Access, only orders in the given Contract from the target Logical Access will be rejected. The Member can continue to submit orders on the Contract using its other Logical Accesses.

If the Risk Manager selected the option to pull orders, all active orders in the target Contract, including GTC (Good Till Cancel), wholesale trades awaiting validation and RFC are pulled. The scope of the orders pulled depends on the level of the Block control.

- For a Block control at Firm ID level, all orders submitted by the Member on the target Contract are pulled.

- For a Block control at Logical Access level, all orders submitted by the Member on the target Contract from the target Logical access are pulled.

- For a Block control at the ExecutionWithinFirmShortCode level, all orders submitted by the Member on the target Contract submitted with the target short code are pulled.

- For a Block control at the ClientIdentificationShortCode level, all orders submitted by the Member on the target Contract for the target client short code are pulled.

The Member is explicitly notified that orders have been pulled as a result of the action from its Risk Manager.

The Member is not logged off and may continue trading on other Contracts or other sessions or short codes not in the scope.

The Block control is persistent so the Member remains so blocked in the target contract until a Risk Manager unsuspends it.

5.2 The Unblock command

The Block control can be lifted through the OEG FIX API using the ERGCommand (U68) message with the field *ERGActionType* (tag: 21101) set to '4' (Unblock).

Risk Managers using the User Interface are also provided the ability to trigger the Unblock command. Through the User Interface is given the ability to the Risk Manager to set the command for multiple Contracts at once, i.e. belonging to the same subscription. The Matching Engine will still process one command per Contract. An Unblock control can be triggered at different levels:

- Unblock the whole Member at Firm ID level in the target Contract (*TargetFirmID* (tag: 21098) in the Optiq FIX API)

- Unblock the Member for a given Logical Access in the target Contract (*TargetFirmID* (tag: 21098) in the Optiq FIX API)

- Unblock the Member for a given ExecutionWithinFirmShortCode level for the target Contract (*TargetPartyID* (tag: 21095) in the Optiq FIX API)

- Unblock the Member's client (identified via its short code) for the target Contract (*TargetClientShortCode* (tag: 21108) in the Optiq FIX API)

The Block control can only be lifted for a given Contract of an Optiq Segment, meaning that if a Risk Member wants to lift block restrictions in multiple Contracts, multiple ERGCommand messages must be sent.

Both RiskGuard Clearers and RiskGuard Members can lift block restrictions for members they are monitoring.

Note that a Risk Manager belonging to a RiskGuard Clearer can only lift Block controls at Member level while a Risk Manager from a RiskGuard Member can lift Block controls at Member, Logical Access, ExecutionWithinFirm and ClientIdentification short code levels.

It is not required that the same Risk Manager unblock a Member they have previously blocked. Any Risk Manager belonging to the same Risk Member can lift block restrictions for a Member that another Risk Manager has blocked.

Upon receipt of the relevant command, the Matching Engine will check that the Risk Member corresponding has the authorization to unblock the target Member.

Following an Unblock command a message is sent back to the Risk Manager to confirm the success or failure of the operation. Risk Managers using the User Interface are also notified through dedicated alerts.

The Unblock results in the following:

- The unblocked Member is notified via a User Notification message with a dedicated User Status. The User Status varies depending on the level at which the Unblock command applies, i.e. Member Firm ID, Logical Access, ExecutionWithinFirmCode, ClientIdentificationShortCode

When a Member is unblocked, it can resume normal trading in the target Contract.

Note that because the Matching Engine takes into account the most restrictive setting, it is possible that a Member cannot resume full trading in the target Contract until all restrictions have been lifted.

6. Additional features

6.1 Get RiskGuard status of risk-monitored entities

Risk Managers can at any time through the FIX API request the status of Members they are risk monitoring in order to obtain the exhaustive list of controls set using the GetRiskControls (U70) message.

The command can be sent requesting settings set at different levels:

- Firm ID *(through TargetFirmID (tag: 21098) field)*

- Logical Access (through *TargetLogicalAccessID (tag: 21099)* field)

- ExecutionWithinFirmShortCode (through *TargetPartyID (tag: 21095)* field)

- ClientIdentificationShortCode (through *TargetClientShortCode (tag : 21108)* field

A dedicated field within the message provides the Risk Manager with the ability to request settings for one specific risk control i.e. Block, Suspend, Order Size Limit, or globally for all submitted controls.

In response the Risk Manager receives a single RiskControlDetails (U71) message, containing all the settings currently set for the level submitted in the request, i.e. Member Firm ID, Logical Access, ExecutionWithinFirmCode, ClientIdentificationShortCode.

Through the MyEuronext User Interface, Risk Managers are always provided with the latest status of the risk monitored entity. Any changes to the status is updated in real-time.

6.2 Email alerts

This function is only available for Risk Managers using the MyEuronext User Interface.

Risk Managers are provided with the ability to define some email recipients to which automatic emails will be sent in case some RiskGuard controls are triggered, e.g. Suspend, Unsuspend, Block, Unblock.

RiskGuard Clearers are given the opportunity to set email recipients for their NCMs as well.

For more details, please refer to the User Guide.

6.3 Short Code management

This function is only available for Risk Managers using the MyEuronext User Interface.

Through the MyEuronext User Interface, Risk Managers can declare the specific ExecutionWithinFirm and ClientIdentification short codes that they want to use in the context of RiskGuard. This is the responsibility of the Risk Manager to make sure that the short codes declared in the User Interface are the same as the ones declared in the SLC Manager and used at the order entry level. No consistency check with the SLC Manager is done.

For more details, please refer to the User Guide.

euronext.com