Euronext RiskGuard – How the service works

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

01 APRIL 2026

V3.2

Table of contents

Preface

Purpose

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

This document describes how the service works for the 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 on the Euronext Connect Portal in 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 the 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:

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

  Derivatives desk email: EMSDerivatives@euronext.com

What's new?

VERSION NO.	DATE	AUTHOR	CHANGE DESCRIPTION
1.0	Nov 2022	Euronext	Initial version
2.0	Aug 2023	Euronext	Addition of the Daily Exposure Management (MEP)
3.0	Dec 2024	Euronext	Handling order movement between Logical Accesses (MEP)
3.1	Apr 2025	Euronext	Usage Guidelines for the Service and 'Kill Switch' Purpose
3.2	Apr 2026	Euronext	▪ OSL available at the Logical Access level and by EMM ▪ MEP available at the Logical Access level ▪ Clarification of the Current Exposure Position definition ▪ CEP Rule Update for commodities: ○ The computation of the Current Exposure Position (CEP) has been updated and no longer takes the lot multiplier into account. It is now expressed in number of lots.

1. Glossary and general definitions

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

NAME	GENERAL DEFINITION
ClientIdentificationShortCode	The short code of the Member's client. This 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
EMM	Euronext Market Model
ExecutionWithinFirmShortCode	The short code of the algorithm, the relevant individual, or the client that submitted the execution to the system. This definition is specific to Euronext Risk Management 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 that is 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** is 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 a licence 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 the Exchange's 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 is 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 is 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. Unlike the RiskGuard Clearer, a Self-Monitoring RiskGuard Member performs its activities solely for the scope of its particular Member Firm.

2. Introduction

The Euronext RiskGuard service for the 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 their firm's risk exposure in real time.

The following pre-trade risk controls are available for Euronext Derivatives Markets:

- **Suspend**, also called Kill Switch / **Unsuspend**
- **Order Size Limit** (**OSL**)
- **Block**, also called **Contract Restrictions** / **Unblock**

  Maximum Exposure Position (**MEP**)

2.1 RiskGuard user profiles

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:

- Within the organisation of a General Clearing Member (GCM), referred to in this document as a **RiskGuard Clearer**. RiskGuard Clearers can set or amend the risk controls of their Non-Clearing Members (NCMs) at a Member Code level (Optiq Firm ID) only.
- In the organisation of a Non-Clearing Member (NCM) or Individual Clearing Member (ICM), referred to in this document as a **RiskGuard Member**. RiskGuard Members can set or amend risk controls for their whole trading firm, i.e. at the Firm ID level, or for a subset of the Firm ID, i.e. at a Logical Access level, or at the level of the short code (ExecutionWithinFirmShortCode or ClientIdentificationShortCode).

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

The Risk Member (RiskGuard Clearer and RiskGuard Member) is identified by its Firm ID, an 8-character alphanumeric code.

Trading Members of Euronext that also have General Clearing status at the CCP may use the service both as a RiskGuard Member and as a RiskGuard Clearer through the same Member Code.

- Through the User Interface, Risk Managers can 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 are referred 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 within the organisation of a Euronext RiskGuard Clearer
  - A NCM Risk Manager is necessarily within the organisation of a Euronext RiskGuard Member

The term Risk Manager can also refer to Risk Agents in the Euronext Connect customer portal. Please refer to the RiskGuard User Access Guide for more details.

2.2 Subscription

A Risk Member can set risk controls only for pre-defined lists of contracts, which refer to the Risk Member's authorised **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**. All Euronext RiskGuard Participants 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'*
    - If a 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, whether 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 wishing to use the FIX API must order a dedicated RiskGuard Logical Access for EUA and Production (once conformance tests have been completed successfully).

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** whether the commands have been sent using the FIX API or through the MyEuronext RiskGuard User Interface.

1. A single RiskGuard command is always applicable to, at minimum, 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 Euronext 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 Euronext 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 authorised to submit orders.

a) A command submitted for a Firm ID will apply both to all associated Logical Accesses, and to 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 set up 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 Euronext 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 Euronext 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 Euronext Market Surveillance.

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

7. By default, no Block, OSL value, or MEP is set, and Members have Unsuspended status.

2.5 Usage guidelines

Any misuse of the RiskGuard Derivatives service for purposes other than risk management will be considered a violation of the service's intended use and will be subject to appropriate disciplinary actions. Such behaviour could negatively impact other users and the overall trading engine, potentially causing disruptions and compromising the integrity of the trading environment. It is imperative that all users adhere strictly to the guidelines and use the service solely for its designated risk management functions.

3. Suspend / Unsuspend commands

The '**Suspend**' functionality, also called the '*Kill Switch'*, allows Risk Managers to halt trading activity on all subscriptions of an Optiq segment via a single command.

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 the level of the Member, Logical Access, ExecutionWithinFirm or ClientIdentification short code.

As a result of a Suspension:

- Risk-monitored traders are not logged off but further order and quote entry is rejected;
- Open orders including GTCs may be deleted (if option to Pull is selected);
- Impacted traders at 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 a result of the Unsuspension:

- Impacted traders at 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 at any time during the day, from when Optiq starts in the morning (before market opens) until session close at the end of the day.

The *'Kill Switch'* is an **emergency command** and must be used solely for this purpose. Any abnormal behaviour related to its use will be analysed and subject to appropriate disciplinary actions.

3.1 Suspend (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 can also 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 permission 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 the levels of the Member, Logical Access, ExecutionWithinFirm and ClientIdentification short code.

As the Suspend is always effective at an Optiq Segment level, if a Risk Member wants to Suspend a Member completely on all the segments where they have trading or clearing authorisations, one Suspend command per Optiq segment must be sent. Through the User Interface, Risk Members can 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 can **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. This 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 authorisation 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 MyEuronext User Interface **and** the Optiq FIX API should note that when a Suspend command is triggered via the User Interface, **the notification message is sent not only 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 if the request is made at a level finer than the Firm ID) is notified via a dedicated message (User Notification (39) / FIX CB) 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 rejected orders 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 can only pull orders for the suspended Firm ID, Logical Access, and 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 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 authorisations, 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 authorisation 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 Unuspended 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. Order Size Limit (OSL)

The 'Order Size Limit' (OSL) allows Risk Managers to define a maximum number of lots that 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, Logical Access level and by Euronext Market Model (COB, RFC, Wholesale). **Finer granularity at the level of the ExecutionWithinFirmShortCode and the ClientIdentificationShortCode is not available.**

Risk Managers can set Order Size Limits at Contract Level for orders from a Member for which there is a Membership Segment authorisation 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 or disabled at any time during the day, from when Optiq starts in the morning (before market opens) until session close at the end of the day.

4.1.1 Activation of the Order Size Limit

The Order Size Limit (OSL) for a Contract can be set or 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 also have the ability to set the OSL. Through the User Interface, the Risk Manager can set the same OSL value at one time for multiple Contracts 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 being rejected in the Contract.

Upon receipt of this command, the Matching Engine will check that the Risk Member has the authorisation 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 means that **all** orders, order revisions and quotes are checked against the Order Size Limit, whether or not a value has been set 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 is 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 limit.

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

4.1.2 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 entity, 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.

4.1.3 Order size limit for expiries

All expiries in a 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 De-activation of the Order Size Limit

Risk Managers can disable an 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 can also de-activate (delete) an OSL. The User Interface allows the Risk Manager to delete the OSL value at one time for multiple Contracts belonging to the same subscription. The Matching Engine will still process one command per Contract.

An Order Size Limit can be disabled at the Firm ID level and Logical Access 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. Block / Unblock commands

5.1 Block command

The 'Block' functionality, also called the 'Contract Restriction' functionality, gives 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 have permission to trade a specific financial instrument.

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

As a 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 by the risk-monitored Member is not impacted,
- If the Block command includes a pull action, relevant orders and quotes are deleted and impacted traders at 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 the Contract through the 'Unblock' functionality.

As a result of the Unblock:

- Impacted traders at 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 at any time 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 can also trigger the Block command. Through the User Interface the Risk Manager can set the command at one time for multiple Contracts 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 the levels of the Member, Logical Access, ExecutionWithinFirm and ClientIdentification short code.

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 can **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 authorisation to set such a control for the target Member.

Following a Block command, a message 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 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 blocked on the target contract until a Risk Manager unsuspends the Member.

5.2 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 can also trigger the Unblock command. Through the User Interface the Risk Manager can set the command at one time for multiple Contracts 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 the levels of the Member, Logical Access, ExecutionWithinFirm and ClientIdentification short code.

It is not necessary that the same Risk Manager unblocks a Member it has 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 corresponding Risk Member has the authorisation 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 the Member cannot resume full trading in the target Contract until all restrictions have been lifted.

6. Daily Exposure Management (Maximum Exposure Position)

6.1 General principles of the Maximum Exposure Position (MEP)

The Maximum Exposure Position functionality, also called the MEP functionality, allows Risk Managers to prevent the risk-monitored entity from trading beyond a financial limit. The Exposure is valid for the day, and must be set in terms of **Quantity** (standard contracts or, for equity derivatives, underlying shares) **at a Contract level** (*TargetFirmID (tag: 21098)* in the Optiq FIX API). The Exposure is computed considering open orders and quotes (where applicable), as well as executed trades during the current trading day. It also takes into account wholesale transactions.

The 'MEP' is available to RiskGuard Members and RiskGuard Clearers, but by design is more targeted to clearing members to monitor their NCMs.

Important note: Please be aware that Sponsored Access is out of scope as it is not offered on Euronext Derivatives markets.

- When triggered by a RiskGuard Clearer: the MEP can be set for any Contract (*TargetPartyID* (*tag: 21095*) in the Optiq FIX API) within the subscriptions included in the clearing agreement between the GCM and the NCM,

- When triggered by a RiskGuard Member: the MEP can be set for any Contract (*TargetPartyID* (*tag: 21095*) in the Optiq FIX API) within the member's trading subscriptions.

In the case of multiple Risk Managers setting limits for the same FirmID and/or Logical Access and on the same Contract, the most restrictive limit will apply. The MEP can be set for the member at Firm ID level and Logical Access level. No finer granularity is available to Risk Managers (ExecutionWithinFirm and ClientIdentification levels are not available).

The MEP has been designed so that Risk Managers can set different actions per member. Therefore, when setting the MEP:

1- Risk Managers must specify at Contract level the **Long Exposure** (referred to in this document as **MEP Long** and the Optiq FIX API as *MaximumLongExposure*) and the **Short Exposure** (referred to in this document as **MEP Short** and in the Optiq FIX API as *MaximumShortExposure*). This refers to as the **MEP Limit,** i.e. the maximum Long and / or Short acceptable value set by the Risk Manager. The MEP Limit can be set asymmetrically for the Long and Short Exposure, meaning that the MEP Short can have a value that is different from the MEP Long. Both limits must be expressed as a positive integer.

2- Risk Managers may optionally specify up to three (3) **MEP Thresholds**, referred to in the Optiq FIX API as *ThresholdValue*, expressed as a percentage of the MEP Limit (must always be below 100%).

3- Risk Managers must configure specific actions to be triggered in the case of a breach of each of pre-configured MEP Limits and MEP Thresholds.

This flexibility allows General Clearing Members to fine-tune the exposure of each of their NCMs based on their exact and specific risk profile.

The MEP parameters are persistent across trading sessions and trading days, until they are deactivated by the Risk Manager.

6.2 Current Exposure Position (CEP)

The Current Exposure Position (CEP) refers to the current value of the net position of the risk-monitored entity as calculated by RiskGuard in real time during a trading day. It is therefore not persistent, but is initialised at start of day based on the active GTC / GTD orders for each contract for which the MEP has been set by the Risk Manager.

The CEP is dynamic and is updated continuously in real time, reflecting ongoing changes in the position. It is constantly compared against the MEP to ensure that the real-time exposure remains within the defined limits.

The CEP is calculated at the level of the contract, and takes into consideration the value of all open orders as well as of all executed trades for the relevant Contracts. It is therefore equal to:

$$CEP\ Long = \left(\sum_{\substack{i=\ buy\\ trades\\ in\ the\ day}} quantity_i - \sum_{\substack{i=\ sell\\ trades\\ inthe\ day}} quantity_i \right) + \left(\sum_{\substack{i=\ open\\ buy\\ orders}} quantity_i \right)$$

$$CEP\ Short = \left(\sum_{\substack{i=\ sell\\ trades\\ in\ the\ day}} quantity_i - \sum_{\substack{i=\ buy\\ trades\\ inthe\ day}} quantity_i \right) + \left(\sum_{\substack{i=\ open\\ sell\\ orders}} quantity_i \right)$$

where the quantity parameter is defined as:

- for Index Derivatives and Commodities: the number of standard lots of the transaction or open order;
- for Equity Derivatives: the number of standard lots multiplied by the lot size (i.e. the trading unit) of the respective instrument. This means that the CEP is expressed in number of underlying instruments for the contract.

Throughout the trading day, the value of the Current Exposure is checked against the MEP Limits and MEP Thresholds set by the Risk Manager. An action is triggered in case any of the MEP Thresholds or Limits have been breached i.e.

CEP <= MEP Short or any related MEP Threshold

or

CEP >= MEP Long MEP or any related MEP Threshold

In the case of a breach, one of the configurable actions described in the paragraph 6.3 will be triggered.

6.2.1 Orders and trades included in the Current Exposure calculation

At the start of day, the Current Exposure that is not carried between trading days includes only GTC / GTD orders.

Then, during the trading day, the Current Exposure Position (CEP) is calculated in real time, in Quantity, including all open orders including quotes, and trades across different EMMs. This includes:

- **Orders and quotes under *EMM = '1'*** (Central Order Book)
- **Executed trades on *'EMM = 1'*** (Central Order Book)
- **Wholesale transactions taking place on *'EMM = 4'*** (Wholesale). Please note that unexecuted wholesale transactions are not included. For Commodities, please note that "Against Actuals" are not included in the CEP.
- **RFC transactions taking place on *'EMM = '7'*** (Request For Cross). Please note that unexecuted RFCs are not included.
- **Strategies (both orders and executed trades)**. For delta neutral strategies, the future leg as well as the ratio is counted, however the cash leg is not. To avoid double counting, please note that implied orders are not included (as the original order is already considered).
- **Temporary TRF trades**. For Total Return Futures (TRFs) traded under the TAIC model, only temporary trades are included in the CEP (since the CEP is calculated in quantity, and no additional info would be added by considering the updated trade price determined at the index close).

6.2.2 Current Exposure calculation based on Risk Managers Authorisation

The calculation of the Current Exposure, as the set-up of the MEP, has been implemented to be restricted to:

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

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

Example:

- Firm A is defined as a GCM for Firm B on Subscription "J12"
- Firm E is defined as a Trading member on Subscription "X34" AND on Subscription "J12"
- Firm B is defined as:
  - A Trading Member on Subscription 'J12' AND Subscription "X34"
  - A GCM for Firm E on Subscription "X34"

Since Firm A is a GCM for Firm B only on the contracts belonging to Subscription "J12", the Current Exposure of Firm B is computed only by considering the trading activity of Firm B on the contracts linked to Subscription "J12".

Since Firm B is a GCM for Firm E only on the contracts belonging to Subscription "X34", the Current Exposure of Firm E is computed only by considering the trading activity of Firm E on the contracts linked to Subscription "X34".

6.3 How to set and amend the MEP Limits and Thresholds

6.3.1 Activate the MEP Limits and Thresholds

The MEP for a Contract can be set (activated) through the FIX API using the ERGCommand (U68) messages with the field *ERGActionType (tag: 21097)* set to '7' (Maximum Exposure Position) and the *MEPFlag (tag: 21811)* set to 'Y'.

The following fields are available in the ERGCommand (U68) message to set the MEP Limit and Thresholds.

FIELD NAME & TAG	DESCRIPTION	CONDITION
MaximumLongExposure (tag: 21812)	Indicates the Maximum Long Exposure limit	Conditional
MaximumShortExposure (tag: 21813)	Indicates the Maximum Short Exposure limit	Conditional
MEPBreachAction (tag: 21814)	This field indicates the type of action that will be triggered when the MEP Limit (Long and Short) is breached	Conditional
NoThresholds (tag: 21815)	Indicates the Number of repeating sections	Conditional
ThresholdValue (tag: 21817)	Defines the percentage of the MEP at which an action might be triggered. *The value to be provided is an integer, meaning, in case the Threshold is to be set at 65%, Risk Manager should populate the field with 65.*	Conditional

ThresholdBreachAction (tag: 21816)	This field indicates the type of action that will be triggered when a given threshold is breached	Conditional

When setting the MEP for a Contract, Risk Managers are provided with the ability to:

- Set the MEP Long limits, i.e. *MaximumLongExposure (tag: 21812)* and MEP Short limits, i.e. *MaximumShortExposure (tag: 21813)*, expressed as absolute values, i.e. in number of standard lots (for Index Derivatives and Commodities) and in number of underlying instruments for the contract (for Equity Derivatives). Note that the values should be >0, otherwise the message will be rejected.

  Important note: Different values for the MEP Long and MEP Short can be set.

- Optionally, configure up to three (3) MEP Thresholds, expressed as a percentage of the MEP Limits using the repeating section in the ERGCommand (U68) message. Please note that the MEP Thresholds are symmetrical for the long and short sides. The percentage must be represented as an integer number. While the MEP Limits must necessarily be defined when the MEP control is activated, the MEP intermediate thresholds are optional, i.e. the MEP Limits can be set without any intermediate threshold.

- Define an action to be automatically triggered on breach:
  1. Of the MEP Long and MEP Short limits using the *MEPBreachAction (tag: 21814)* field
  2. Optionally, for each MEP Threshold using the *ThresholdBreachAction (tag: 21816)* field

More information about Breach Actions is provided in the following chapter.

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

Following the submission of the command, an ERGCommandAck (U69) message is sent back to the Risk Manager to confirm the success or failure of the operation:

- Acknowledged: *AckStatus (tag: 5711)* set to '0' (Accept);
- Rejected: *AckStatus (tag: 5711)* set to '1' (Reject) in the case of a functional rejection. For a technical rejection, a Reject (3) message with an error code is provided.

Once the MEP parameters have been set, each order will be checked against the MEP Limit and Thresholds based on the updated Current Exposure.

*Please note that across participants, **all** orders, order revisions and quotes (where applicable) are being checked against the MEP, whatever a value has been set or not by the Risk Manager. This therefore guarantees fairness between all trading participants.*

In the case of multiple Risk Managers setting MEP limits for the same FirmID and the same Contract, the most restrictive one will apply.

Important note: The MEP parameters remain persistent across trading days.

6.3.2 How to de-activate the MEP Limit and Thresholds

Risk Managers can disable the MEP that has previously been set using the ERGCommand (U68) message with the field *ERGActionType (tag: 21097)* set to '7' (Maximum Exposure Position) and the field *MEPFlag (tag: 21101)* set to 'N' (False). One message per Contract must be sent.

The MEP can only be disabled at the Firm ID level and Logical Access 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 de-activation of the MEP will remove both the MEP Long and / or MEP Short as well as any previously configured MEP Thresholds.

6.3.3 How to amend the MEP Limit and Thresholds

Risk Managers can amend the previously configured MEP Limits, MEP Thresholds and Breach Actions using the ERGCommand (U68) message with the field *ERGActionType (tag: 21097)* set to '7' (Maximum Exposure Position) and the field *MEPFlag (tag: 21101)* set to 'Y' (True).

Risk Managers are strongly recommended through the API to only populate the limits and / or actions that should be amended.

Example: A Risk Manager wants to amend the MEP Long and MEP Short values without amending the levels of the thresholds. The threshold repeating section must not be populated (or populated with the values and actions previously set).

6.3.4 the User Notification (39) / FIX CB)

Once MEP parameters have been set (i.e. activated) for a Member and Contract, each time a Breach Action is triggered, Risk Managers are notified through a ERGMEPBreachAlert (U76).

The Risk-monitored entity is notified through UserNotification 39 / FIX (CB) message once one or more limits are breached simultaneously, either the Long or Short MEP Limit or one/multiple of the individual thresholds. The only exception is in the case where the breach action is "alert only".

Important note: Please note that in the case of **successive breaches of individual thresholds,** no message is sent to clear the previous breached threshold, but only a message to indicate the new, i.e. **last** applicable threshold in place, is sent.

When the Current Exposure value decreases to level(s) below the pre-defined threshold(s), i.e. thresholds are cleared, (the CE is no longer breaching the threshold(s)):

- If only the current threshold is cleared, but lower ones were set, the ERGMEPBreachAlert (U76) and UserNotification 39 / FIX (CB) messages will indicate the new threshold and breach action activated. Note that no message is sent in the case the Breach Action is "alert only".

- If the Current Exposure calculation leads to "no longer threshold being active, the ERGMEPBreachAlert (U76) and UserNotification 39 / FIX (CB) messages will indicate that no threshold neither action is activated.

6.4 MEP Limits and MEP Thresholds Breach Actions

6.4.1 Breach Actions available

The following Breach Actions can be set by Risk Managers both for the MEP Limits (Long and Short) **and** the MEP Thresholds.

- The Breach Action applying to the MEP Long and the MEP Short must be set in *the MEPBreachAction (tag: 21814)* field

- The Breach Action applying to the MEP Thresholds must be set in *the ThresholdBreachAction (tag: 21816)* field

Important note: Breach actions are implemented **with increasing restrictiveness**. Risk Managers are strongly recommended to pay attention to the rules detailed below.

Please note that a given action stays in place for as long as the position is between a given threshold and the next one (the action that was in place previously, if any, at the moment the breach was triggered, is overridden).

- **0 = No Action, Alert Only**: An alert is sent to the Risk Manager indicating that a given limit – MEP Limit and/or MEP Thresholds – has just been reached. This specific action does not impact the new inbound messages coming from the risk-monitored entity, nor the orders already in the book. It means that if a MEP Threshold is breached, orders are still accepted and only an alert is sent. In this case, as no action is triggered, no notification is sent to the risk-monitored entity, but only to the Risk Manager. No other restrictive action is triggered.

- **1 = Accept Actions that Decrease Position Only:** An alert is sent to the Risk Manager and to the risk-monitored entity indicating that a given limit – MEP Limit and/or MEP Thresholds – was breached and the Breach Action has been triggered. This specific action has an impact on the acceptance / rejection of the new inbound messages coming from the risk-monitored entity, however there is no impact on the resting orders. Only inbound messages that will result in a decrease of the Exposure will be accepted.

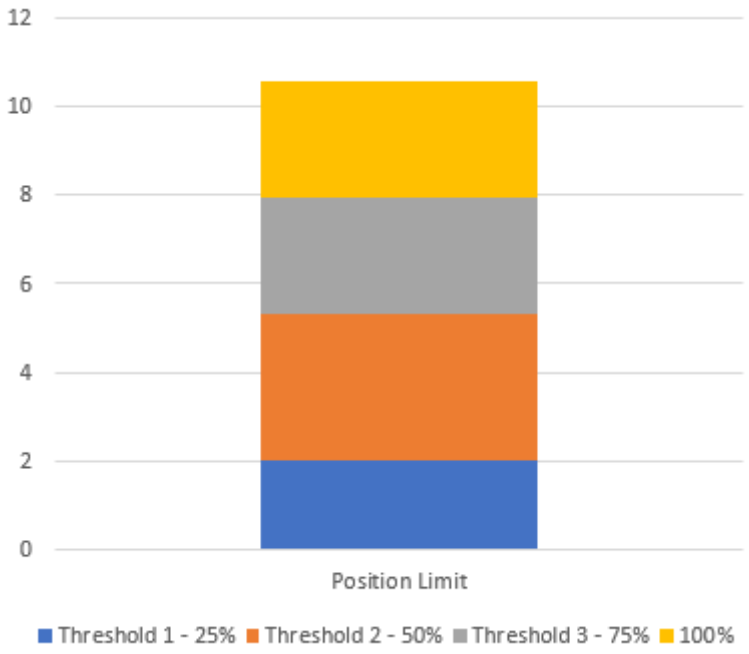
- **2 = Block Only**: An alert is sent to the Risk Manager and to the risk-monitored entity indicating that a given limit – MEP Limit and/or MEP Thresholds – was breached and the Breach Action has been triggered. This specific action has an impact on the acceptance / rejection of the new inbound messages coming from the risk-monitored entity, however there is no impact on the resting orders. No inbound messages on the impacted Contract will be accepted by Optiq except "Mass Cancellation" messages. An action is required by the Risk Manager to allow the risk-monitored entity to restart its trading activity.

- **3 = Block and Pull All Orders:** An alert is sent to the Risk Manager and to the risk-monitored entity indicating that a given limit – MEP Limit and/or MEP Thresholds – was breached and the Breach Action has been triggered. This specific action has an impact on any new inbound messages, **as well as on the orders already on the book, regardless of the side of the breach**. When this action is triggered, any new incoming message from the risk-monitored entity is rejected except for the "Mass Cancel" message, and all open orders are deleted.

Please note that a given action stays in place for as long as the position is between a given threshold and the next one (the action that was in place previously, if any, at the moment the breach was triggered, is overridden).

If the current position breaches the control just set, because of orders and/or trades that have already taken place, then alerts / actions should be triggered immediately after the MEP Command is accepted and acknowledged. The drawing below illustrates the different thresholds that can be configured.

Breach Action Thresholds



Important note: Mass cancellation messages are always accepted, irrespective of the MEP Breach Action in place.

6.4.2 Example of increasing restrictiveness of Breach Actions

A Risk Manager defines an MEP Long of 10,000 lots on Contract XYZ, and two MEP Thresholds at 50% (5,000 lots) and 80% (8,000 lots).

In the event that the Risk Manager decides to associate Breach Action "1 – Accept Actions that Decrease position only" to the 50% Threshold, the Risk Manager will not be allowed to associate action "0 – No action, Alert only" to the 80% Threshold or to the MEP Long. An acceptable sequence of actions would be:

- 50% threshold: "1 – Accept actions that decrease position only"
- 80% threshold: "2 – Block only"
- MEP Long: "3 – Pull All Orders and Block"

Please note that:

- The **same** Breach Action (for example Breach Action ”0 – No action, alert only” can be associated to more than one (1) consecutive MEP Thresholds;

- Breach Actions “2 – Block Only “ and “3 – Pull All Orders and Block“ are considered to have the same level of restrictiveness, so they can be freely associated across consecutive MEP Thresholds and MEP Limits.

Risk Managers must be aware that, if actions “2 – Block only” or “3 – Pull all orders and Block” are triggered, the Block action will also persist if the Exposure returns below the corresponding threshold. A manual action from the Risk Manager will be required to Unblock the risk-monitored entity:

- In this scenario, sending the ERGCommand (U68) with *ERGActionType (tag: 21097) set to ‘4’* (Unblock) will not have any impact. This command will **not** remove the Block triggered by the MEP breach.

  In order to remove the Block triggered by a MEP breach, the Risk Manager is required to re-set the MEP command via the ERGCommand (U68), eventually modifying the MEP Limits, the MEP Thresholds and/or their related Breach Action(s). This command gives the Risk Manager the flexibility to re-evaluate the appropriate risk limits to be applied to the risk-monitored entity, following its previous breach. Note that alternatively, the Risk Manager can deactivate the MEP using the ERGCommand (U68) message, with the *MEPFlag (tag: 21811)* equal to “N” (False).

6.5 Order handling and processing

This chapter provides a high-level overview of how orders are handled when MEP parameters are set, and breach actions can be triggered. It also provides a list of functional events that can impact the Current Exposure.

6.5.1 Upon receipt of an order

The order is accepted or not depending on the action in place at the moment of the submission *(i.e. the system does not take into account the potential impact of that order for the future exposure).*

- If the order is accepted and there is no counterpart, the exposure is recalculated and checked against the configured thresholds and limits. This may or may not lead to the triggering of a Breach Action.

- If the order is accepted and matched, the current exposure is checked against the configured thresholds and limits. This may or may not lead to the triggering of a new Breach Action, **only** at the end of the full processing of the incoming message.

- If the order is rejected, the exposure is not updated.

Note: If the triggered action is “Block and Pull”, then Optiq will trigger the purge of the order book and send the relevant notifications to the Risk Managers and the risk-monitored entity. When orders are killed, then the current exposure is recalculated and is checked against the configured thresholds, which may or may not lead to the triggering of a new Breach Action.

6.5.2 Functional events that can impact the Current Exposure

Please see below some functional kinematics which can impact the Current Exposure Position according to the golden rules defined immediately above.

1. New Order submission can lead to:

- The booking of the submitted order
- Triggering of the Self Trade Prevention (STP) that may cause order cancellation(s)
- Triggering of a Market Maker Protection (MMP) that may cause order cancellation(s)
- A "normal" trade;
  - partial *(only the partial quantity is considered for the traded quantity of the CEP)* or full match *(the full quantity is then considered for the traded quantity of the CEP)*;
- Aggressive match with an existing Implied;
- Generation of a new Implied which is then aggressive against another order
  - Or the generated Implied *(the one mentioned in the previous bullet point)* matches against another existing Implied

2. Order modification can lead to:

- "Standard" impact, meaning, order or quote quantity increased / decreased
- Plus all cases listed under "New Order Submission" in the situation where the replacement leads to a trade

3. Cancellations *(please note that in those cases only the Leaves Qty is considered)* can lead to:

- Single order cancellations triggered by the risk-monitored entity or Market Surveillance
- Mass cancellation request triggered by the risk-monitored entity
- Trade cancellation (incl. strategy trades) triggered by Market Surveillance (incl. TRF temporary trades)
- Order cancelled due to Trade Price Validation (TPV) – applicable only for options
- Triggering of an MMP breach causing cancellation of existing booked orders

4. Other cases

- Central Order Book Uncrossing and RFC Uncrossing that lead to trade execution
- Triggering of a MMP breach causing cancellation of resting orders

Please note that the different events listed above may impact just the short, just the long, or both.

6.5.3 Reload of Orders (GTC/GTD)

At Start of Day, while loading active GTC (Good Till Cancel) and GTD (Good Till Date) orders, Optiq calculates the Start of Day Exposure, i.e. the Current Exposure Position along with potential action(s) that should be triggered (if any).

- If the CEP reaches the following threshold "**0** - **Alert only**", when the Risk Manager connects:

- A ERGMEPBreachAlert (U76) message is sent to indicate the action in place
- A UserNotification 39 / FIX (CB) is sent to indicate the MEP Threshold currently activated (i.e. Alert Only)

- If the CEP reaches the threshold where the action triggered is "**1 – Accept Positions that decrease the position only**", there is no impact for the GTC/GTD orders in the book, the action will only apply to incoming requests once the market opens. When the Risk Manager connects:
  - A ERGMEPBreachAlert (U76) message is sent to indicate the action in place
  - A UserNotification 39 / FIX (CB) is sent to indicate the MEP Threshold currently activated (i.e. Accept Positions that decrease the position only)

- If the CEP reaches the threshold where the action triggered is "**2 - Block Only**", there is no impact for the GTC/GTD orders in the book, the action will only apply to incoming requests once the market opens. When the Risk Manager orders:
  - A ERGMEPBreachAlert (U76) message is sent to indicate the action in place
  - A UserNotification 39 / FIX (CB) is sent to indicate the MEP Threshold currently activated (i.e. Block Only)

- If the CE reaches the threshold where the action triggered is "**3 - Block and pull all orders**", Optiq will pull all active orders in the book and the CEP is updated to reflect the positions as well as the potential Breach Actions in place. When the Risk Manager connects:
  - A ERGMEPBreachAlert (U76) message is sent to indicate the action in place
  - A UserNotification 39 / FIX (CB) is sent to indicate the MEP Threshold currently activated (i.e. Block and pull all orders)

When the risk-monitored entity connects, Kill (O5) or FIX ExecutionReport (08) messages are broadcasted for each of the killed orders.

6.5.4 Handling order movement between Logical Accesses

When orders are moved between Logical Accesses (LAs) due to modifications or through the Ownership Requests feature in Optiq, the following rules apply to ensure accurate exposure management under the Maximum Exposure Position (MEP) settings:

1. **Scenarios covered:**

- **Scenario 1**: An order submitted through one LA (e.g., LA A) is modified through another LA (e.g., LA B), causing the order to "move" from LA A to LA B.

- **Scenario 2**: An order is transferred from one LA to another via an Ownership Request message.

2. **Actions to be taken:**

- If the **destination LA** has **MEP (Maximum Exposure Position)** activated:

  - The Current Exposure of both the original LA and the destination LA will be updated by the remaining order quantity, i.e. the remaining order quantity will shift from the original LA exposure to the destination LA exposure.
  - The breach action (if any) applied to the original LA **will not propagate** to the destination LA.

- The system will validate whether the modification or Ownership Request complies with the MEP rules set for the destination LA before accepting the action.

- If the **destination LA** has **no MEP activated**:

  - The exposure of the original LA must be adjusted to exclude the order's impacts. Only the Current Exposure of the original LA will be updated by the remaining order quantity.
  - No exposure adjustments nor order quantity checks are performed for the destination LA.

This ensures consistent exposure management while respecting the MEP configuration of each Logical Access.

6.6 Formula used to calculate the Exposure

6.6.1 Overview

The Current Exposure is computed for each pair of Risk Manager + Targeted Firm + Contract as following:

- **For Future contracts:**

$$CEP\ long = WOB + WSBL + (TB\text{-}TS)$$

$$CEP\ Short = WOS + WSSL + (TS\text{-}TB)$$

Where:

- *WOB* - Working Outright Buy orders: Quantity of buy order * trading unit
- *WSBL* - Working Strategy Buy legs: Sum of ratio for buy legs * quantity order * trading unit
- *WOS* - Working Outright Sell orders: quantity of sell order * trading unit
- *WSSL* - Working Strategy Sell legs (Sum of ratio for sell legs * quantity order * trading unit)
- *TB*: Traded Buy quantity * trading unit
- *TS*: Traded Sell quantity * trading unit

- **For options,** Optiq considers the instrument type i.e. Call or Put. Therefore:

  - *WOB*: Long Call orders or Short Put orders quantity * trading unit
  - *WOS*: Short Call orders or Long Put orders quantity * trading unit
  - *WSBL*: (Sum of ratio of Long Call legs + Sum of ratio of Short Put legs) * (quantity of strategy order * trading unit)
  - *WSSL*: (Sum of ratio of Short Call legs + Sum of ratio of Long Put legs) * (quantity of strategy order * trading unit)

The calculation of the Current Exposure is always:

- rounded down for positive values;
- rounded up for negative values.

Please note that while for all other contracts the Current Exposure (CE) is computed **in number of underlying shares**, when it comes to Index Derivatives contracts the CE **is computed in notional amount**.

The following chapters provide more details about the calculation of the sub-components of the formula.

6.6.2 Working Outright Buy Orders & Working Outright Sell Orders

WOB is the aggregation of the number of working buy orders across all expiries while WOS is the aggregation of the number of working sell orders across all expiries.

Example: *Assuming Trading Unit = 100*

Expiry	MAR	JUN	SEP	DEC	Overall without Trading Unit
Working Buy Orders (Lots)	60	40	15	20	**135**
Working Sell Orders (Lots)	30	25	35	80	**170**

WOB = (60 + 40 + 15 + 20) * 100 = 13,500

WOS = (30 + 25 + 35 + 80) * 100 = 17,000

6.6.3 Example of a current exposure for a contract on outright orders

Consider the following situation for a given contract where the Trading unit is different per expiry:

Expiry	MAR		JUN		SEP		DEC		Overall
	Lots	Trading Unit	Lots	Trading Unit	Lots	Trading Unit	Lots	Trading Unit	
Working Buy Orders	10	10	50	20	15	20	40	50	**3,400**
Working Sell Orders	-	-	-	-	-	-	5	50	**250**

Expiry	Mar		Jun		Sep		Dec		Overall
	Lots	Trading Unit	Lots	Trading Unit	Lots	Trading Unit	Lots	Trading Unit	
Traded Outright Buy (Lots)	45	10	-	-	-	-	-	-	**450**
Traded Outright Sell (Lots)	-	-	-	-	-	-	25	50	**1,250**

CE Long = *WOB + TB – TS = 3,400* + 450 – 1 250 = 2,600

CE Short = *WOS + TS – TB* = 250 + 1,250 – 450 = 1,050

Please note that the sub-components of the formulas have been computed within the column "Overall" of the tables above based on the formulas previously introduced.

The following events then occur on the book:

- Submission of one new Sell order on the September expiry of 15 lots.
- Matching of the December Sell order completely to generate a trade of 5 lots.

The new situation is:

Expiry	MAR		JUN		SEP		DEC		Overall
	lots	trading unit	lots	trading unit	lots	trading unit	lots	trading unit	
Working Buy Orders	10	10	50	20	15	20	40	50	**3,400**
Working Sell Orders	-	-	-	-	15	20	5	50	**550**

Expiry	MAR		JUN		SEP		DEC		Overall
	Lots	Trading Unit	Lots	Trading Unit	Lots	Trading Unit	Lots	Trading Unit	
Traded Outright Buy (Lots)	45	10	-	-	-	-	-	-	**450**
Traded Outright Sell (Lots)	-	-	-	-	-	-	30[1]	50	**1,500**

CE Long = *WOB + TB – TS = 3,400* + 450 – 1,500 = 2,350

CE Short = *WOS + TS –TB = 550* + 1,500 – 450 = 1,600

Please note that the sub-components of the formulas have been computed within the column "Overall" of the tables above, based on the formulas previously introduced.

Notes:

- In cases where the CE Short is equal to zero (0), it does not mean that there is no activity; it simply means that the Traded Long is equal to the Traded Short + Working Outright Short
- When an order is matched, its value is transferred from Working Outright to Traded. It does not increase the CE on its side. However, it decreases the position on the opposite side.

6.7 Messages not in scope of the MEP

Please note that even if the MEP is activated at the System level **and** the MEP is activated by the Risk Manager on a given Firm and there is an active threshold breach action (different than "No Action, Alert Only) then the following messages are still accepted:

- RFC and Wholesale orders;
- Mass cancellations are accepted regardless of the action;
- Any request such as Open Order Request (15), Ownership Request (18) are accepted regardless of the action as they do not impact the positions in any way.

7. Additional features

7.1 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:

3. Firm ID *(*through *TargetFirmID (tag: 21098)* field)
4. Logical Access (through *TargetLogicalAccessID (tag: 21099)* field)
5. ExecutionWithinFirmShortCode (through *TargetPartyID (tag: 21095)* field)
6. 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 are updated in real time.

7.2 Email alerts

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

Risk Managers can define a list of email recipients to which automatic emails will be sent in the case that some RiskGuard controls are triggered, e.g. Suspend, Unsuspend, Block, Unblock.

RiskGuard Clearers can also set email recipients for their NCMs.

For more details, please refer to the User Guide.

7.3 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. It is the responsibility of the Risk Manager to make sure that the short codes declared in the User Interface are the same as those declared in the SLC Manager and used at the order entry level. There is no consistency check with the SLC Manager.

For more details, please refer to the User Guide.

euronext.com