FA Back 3.6

FA Back 3.6 provides you with tools to drill down into your underlying positions in Analytics+, easier way to access a linked portfolio directly from the Overview, and improvements in navigating between selected contacts and portfolios on the Overview.

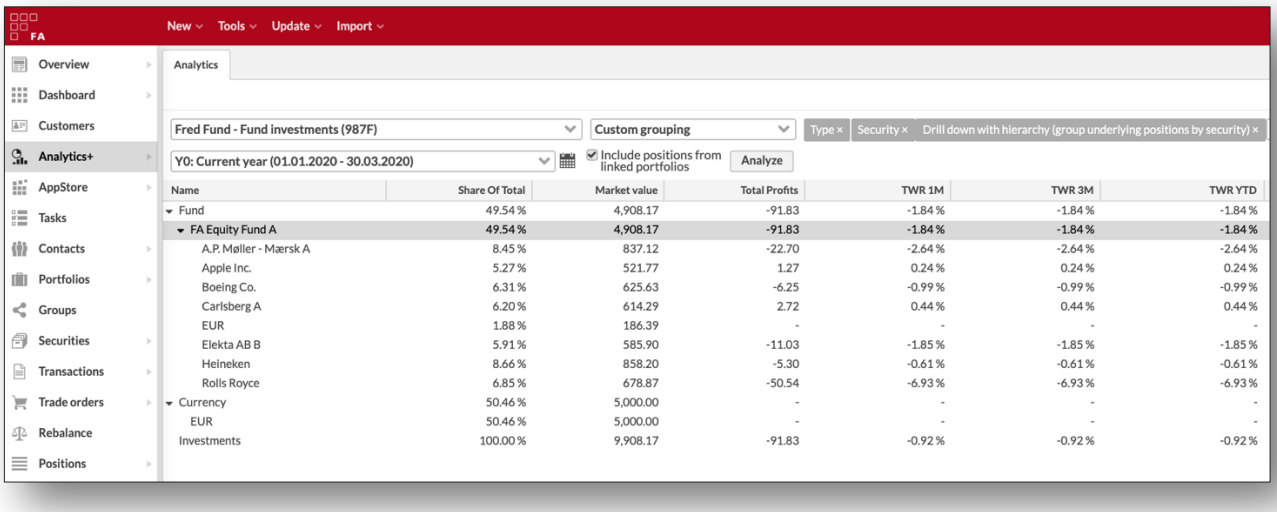
Drill down into underlying positions in Analytics+

Version 3.6 provides you with tools to drill down or look through into the contents of a position's linked portfolio, allowing you to see the underlying positions you own through your investment. For example, you can drill down to see the contents of your fund when you maintain the fund portfolio in FA, or to see your underlying investments in a shared ownership structure.

Include underlying positions in your analysis. *Include positions from linked portfolios* check fetches positions from linked portfolios and replaces your investment with the underlying positions in your analysis. As a result, instead of a fund position, your analysis shows the positions from your fund.

Visualize the drill down hierarchy. Custom groupings *Drill down hierarchy* allow you to visualize the hierarchy of your investments. When underlying positions are included, these groupings show the drill down in a tree structure. As a result, contents of a fund are shown in a tree below a fund position.

Drill down assumes you maintain the underlying positions in a portfolio in FA. Values for the positions fetched through drill down are calculated based on the market value of your investment, the market value of the linked portfolio, and the underlying position's share in the linked portfolio. Drill down works also with fund-of-fund structures, allowing you to drill down up to 10 levels.

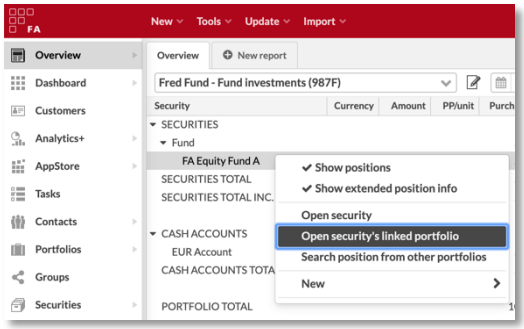


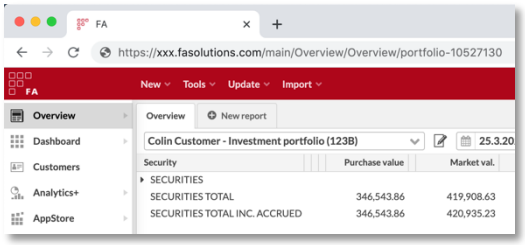
Easier ways to access portfolios on the Overview

Version 3.6 provides you with improvements on how to access your portfolios on the Overview in certain situations. These improvements allow you to navigate through your portfolios more efficiently, reducing the number of times you need to re-select a portfolio on the Overview.

Access position's linked portfolio from the Overview.

You can now right-click a position on the Overview to *Open security's linked portfolio*. This allows you to easily access for example a fund portfolio through a fund position. The selection is available if your position's security has a linked portfolio, and you are allowed to access it in terms of limited visibility. If you want to easily see which positions have a linked portfolio, select *Security linked portfolio* as a column on the Overview!





Navigate back and forth between selected contacts and portfolios on the Overview.

You can now use your browser's back and forward buttons to browse between the selections you have made on the Overview during your session. Every time you select something, your browser's URL reflects your selection – as a result, the back button takes you back to your previous selection.

Obfuscating certain client data in the database through simple substitution cipher

Version 3.6 provides you with an option to obfuscate certain sensitive client information before storing it into the database. The purpose of this feature is to ensure that information that could identify individual clients from the data can only be accessed by authenticated and authorized users of the application – that is, neither administrators of the application's technical environment nor anyone getting an access of a database backup would be able to access the sensitive information.

Sensitive client data is obfuscated using a simple substitution cipher. This approach was selected to maintain the usability of the system: users can still search and filter all data, even when it is obfuscated in the database. Obfuscation is only applied to fields that might contain sensitive client information, including contact's name, external ID and address, portfolio's email, profile data, and user information, such as first name, last name and email address. In addition, obfuscation is limited to upper- and lower-case Latin characters, numbers, and most common Scandinavian characters – for example Cyrillic and Arabic characters are not obfuscated but stored in the database as they are.

Obfuscation is enabled on the application level and requires certain preparations before it can be taken into use – if you are interested in this feature, contact FA for more details.

Other improvements on information security

Version 3.6 also introduces other smaller improvements on information security.

Auditing changes to permissions. System audit now tracks changes users make to Permissions in the Preferences view. Every time a user makes a change in permissions, the system audit contains a message "*User [username] changed permissions: {[permission change]}*".

Auditing changes to API tokens. System audit now also tracks changes users make to API tokens in the Administration view. Every time a user makes a change in an API token, the system audit contains a message "*User [username] created / deleted API token [token name]*".

Delete data not available in production. *Delete data* within the Administration view is no longer available in production environments – these features are useful in data migration phase during deployment, but are disabled in production environments to ensure data is not accidentally deleted.