ASPECT4 FOUNDATION Y22Q4

Continued focus on safety

There is a large and increasing focus around us on security and on closing potential security breaches as effectively as possible.

Fortunately, security has always been a top priority for ASPECT4, and the basic security setup has fortunately proven to be robust thanks to the basic authentication and authorisation model for ASPECT4 and solidly supported by IBM in server and OS architecture.

However, ASPECT4 typically forms part of much more complex IT landscapes, and integration between systems is now quite common and business-critical. Therefore, there is also a need to constantly re-evaluate safety aspects. A key aspect is the risk of intrusion. Release Y22Q3 contained a modernised model for the storage of so-called "secrets", which is used when systems identify themselves to each other.

EG

Let's go further

New stricter security model

The release also included a brand new model, based on the new concept for secrets, for meeting stricter security requirements from Microsoft in connection with mail receipt from Exchange Online.

This time, the time has come for increased security when logging in to ASPECT4. For ASPECT4 Client, login takes place technically in a closed environment, while login from ASPECT4 Client for Web and the mobile platform ASPECT4 CrossPad can take place via the Internet.

ASPECT4 Client for Web has a time supported two-factor login, and with Y22Q4, two-factor login can also be used when logging in from the mobile apps in ASPECT4 CrossPad. Two-factor login is known from many similar solutions and adds a significant layer of security on top of a traditional and simple login with a fixed password.

Whether two-factor login is to be used is configured in ASPECT4 backend and uses TOTP (time-based one-time passwords) as a supplement to the usual password. One-time passwords are generated through an Authenticator app that supports TOTP, and the one-time password of 6 digit pastes or entered into CrossPad when logging in.

Let's go further

Change password in CrossPad

At the same time, CrossPad has been expanded with access for the user to change and enter a new, permanent password. Naturally, the new password must comply with and be checked against the policies that the company has set up for IBM in passwords.

The new feature is convenient for users who only operate ASPECT4 from CrossPad apps, but are also an extremely important part of the increased focus on security. ASPECT4 users can now change their passwords on the move and away from the office immediately if they suspect a password leak.