How does the block-list (Protector!) work?

One of the most popular and widely appreciated features of Syncplify Server! has always been its **powerful and automatic block-list** (formerly known as blacklist). Starting from v4 (and subsequent versions) Syncplify Server! brought that concept to an even higher level with its **Syncplify Protector!™** technology.

Protector! is a leap forward. It's still **fully automatic**, but its controls are **an order of magnitude more accurate** and integrated much deeper in the protocols handler themselves. If used to its full potential, Protector! can be very harsh, therefore we felt the need to let our users configure its "sensitivity". It is possible to set Protector! to either one of the following 4 "aggressiveness thresholds":

Indulgent: when set to "indulgent", Protector! will only detect authentication/authorization level violations, but will not consider a connect-disconnect sequence as a violation (thus it's compatible with external "heartbeat" network and host monitors) – regardless, we still recommend the use of our safe-list for this purpose, and to set Protector! to indulgent only when Syncplify Server! is run in totally isolated networks not connected to the Internet.

Normal: this setting will tell Protector! to behave similarly to the previous block-list (as seen in the old v1-v3), only with a much higher degree of accuracy. This is the default setting.

Strict: this is a harsher setting, ideal when a server is open to external users that don't belong to your organization, and whose client software you have no control on. The "strict" setting, in fact, will treat all protocol level errors as violations, and trigger the *strike-count* for the block-list. Requesting the download of a non-existent file, or the list of a directory without permissions, all these occurrences (and the like) will increase the *strike-count*, and eventually kick the connection and block-list the remote IP.

Paranoid: similar to "strict" but… more. When Protector! is configured in "paranoid" mode, even just disconnecting without sending the "BYE" command will be considered a violation, and trigger the *strike-count* increase. So, we recommend to use this mode only when you have full control over the client's behavior and you know for sure that the client is going to honor the protocol 100%, because in "paranoid" mode anything less than absolute perfection is a violation, and will eventually get you block-listed.

Revision #1
Created 19 July 2023 11:12:53 by DevTeam
Updated 22 July 2023 00:51:45 by DevTeam