

IP Access List

 Translate: EN


The "IP Access List" section is intended for setting the fetch protection system. For example, you found out that some negative actions were made from one or several subnetworks. In such cases, you can block the entire subnetwork(s). If the access permission is needed for a part of IP-addresses included into the list of blocked ones, the instruction permitting the access must be located lower than that of blocking. When a group of addresses is blocked, no user (client, manager, administrator) can connect the server from any address inside the blocked group.

Up to 511 rules of access right limitation from different addresses. By default, all addresses are considered as permitted.

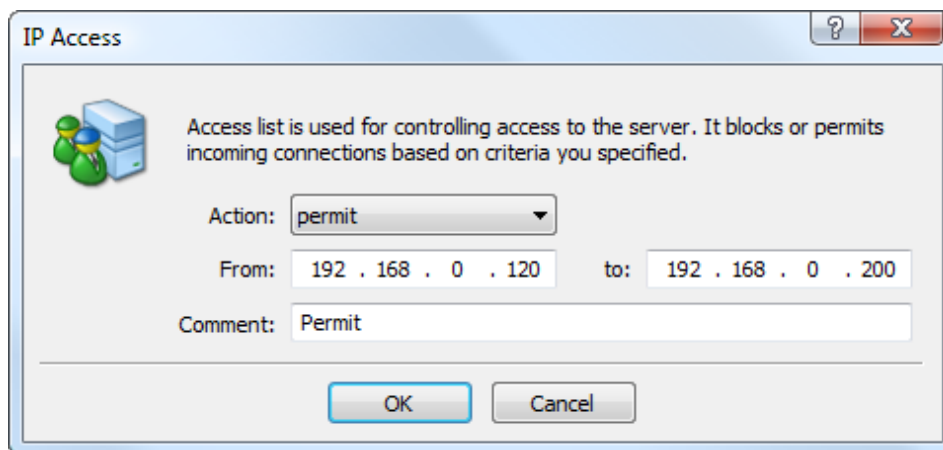
From	To	Comment
192.168.0.1	192.168.0.255	Block
192.168.0.120	192.168.0.200	Permit

Each address check is made top-to-bottom. The last rule concerning the address should be applied to it regardless of former instructions. Thus, the position of each instruction in the list is a very important condition for access right limitation for IP-addresses. In the example given above, the permitting instruction is located lower than that of blocking and this allows to create a pass within the range of the blocked addresses. But the interchanging the instructions disables this pass since the latest access rule prescribes blocking the whole list. In this case, the permitting instruction will be simply ignored.

The "permit always" rule is applied irrespective of its position in the list. If this rule is met for an IP address, all further instructions will be ignored. Addresses marked as "permit always" are not checked by the [Antiflood control](#) system.

To configure the instruction location in the list, the context menu commands as "Move Up" and "Move Down" should be used, as well as the same commands in the "Edit" menu, and the following buttons of the toolbar: and .

When adding or editing a rule (with the context menu "Add" and "Edit" commands, as well as the same commands of the "Edit" menu, and the following buttons of the toolbar: and) the setting window will open:




Action — action applying to the given list of IP-addresses (Block — block access; Permit — permit access);

From — IP-address to be the first to which the given access rule will be applied;

To — IP-address to be the last to which the given access rule will be applied;

Comment — the text of comment.

The context menu "Delete" command, as well as the "Edit" menu command and the button of  on the toolbar will delete the instruction selected.

Warnings:

Do not block the IP-addresses list including the IP-address used by the administrator when connecting to the server. After the access rules have come into effect, you will not be able to connect to the server.

You should think over in detail both the rules of access blocking and permission, and their location in the list. Keep in mind that only the latest rule concerning the given address can apply to this address. All preceding rules will be — ignored.

[Gateway](#)

[Data Centers](#)

© 2000-2022, [MetaQuotes Ltd.](#) Copying or republishing in whole or in part is prohibited