Authentication Exemption

Exempt computers or computer groups from being required to authenticate, regardless of other connection security rules. This rule type is commonly used to grant access to infrastructure computers that this computer must communicate with before authentications can be performed. It is also used for other computers that cannot use the form of authentication you configure for this policy and profile.

Infrastructure computers, such as Active Directory domain controllers, certification authorities (CAs), or DHCP servers, might be allowed to communicate with this computer before authentication can be performed.

To create an authentication exemption rule, you only need to specify the computers or a group or range of IP addresses (computers) and give the rule a name and, optionally, a description.

To get to this wizard page

1. In the Windows Firewall with Advanced Security MMC snap-in, right-click **Connection Security Rules**, and then click **New Rule**.
2. On the **Rule Type** page, select **Authentication Exemption**.

Importing and exporting Firewall Policies

The process of creating and modifying rules in the Windows Firewall With Advanced Security console can be time-consuming, and repeating the process on multiple computers even more so. Therefore, the console makes it possible for you to save the rules and settings you have created by exporting them to a policy file.

A policy file is a file with a .wfw extension that contains all the property settings in a Windows Firewall installation and all its rules, including the preconfigured rules and those you have created or modified. To create a policy file, select Export Policy from the Action menu in the Windows Firewall With Advanced Security console, and then specify a name and location for the file.

You can then duplicate the rules and settings on another computer by copying the file and using the Import Policy function to read in the contents.