Configuring the Microsoft Windows Personal Firewall to Run Natural

Configuring the Microsoft Windows Personal Firewall to Run Natural

In Windows, the firewall is switched on by default. When you do not configure the firewall to allow Natural, it is not possible to start Natural.

Warning:
Software AG does not recommend to disable a firewall. Disabling a firewall is solely your responsibility as user.

For detailed information on configuring the Windows firewall, see the Microsoft documentation.

This chapter provides examples of how to run Natural in an environment protected by the Windows firewall. However, these examples only provide technical guidelines; Software AG cannot guarantee that the examples given will provide the security you require.

The examples are based on two methods: one to allow a specific executable to open ports, the other to allow a specific port to be used by a certain program on your PC. These methods use Natural as an example. For other Natural components, see *Overview of Executables and Port Numbers* for the relevant information.

If elevated rights are required on Vista (for example, to remove an allowed program or to close a port), run *cmd.exe* by executing the **Run as administrator** command which is available when you invoke the context menu for *cmd.exe*.

This chapter covers the following topics:

- Method 1 - Allow a Specific Executable to Open a Port
- Method 2 - Allow a Specific Port to be used on your PC
- Overview of Executables and Port Numbers

Method 1 - Allow a Specific Executable to Open a Port

This method involves adding the Natural executable as an "allowed program". This means it can open any port for both TCP and UDP communication.

The parameters may be customized during the installation process. If you did not install using the default settings, you will need to use your custom parameters.

The following examples apply to the Natural executable. To add other Natural or Entire Access components as allowed programs, see *Overview of Executables and Port Numbers* below.

Note:
The examples below use the default installation settings for Windows and Natural for Windows Version 6.3.

To add Natural as an allowed program

- Enter the following command:

```
netsh firewall add allowedprogram program="C:\Program Files\Software AG\Natural\6.3\Bin\natural.exe" name="Natural" profile=ALL
```

To remove Natural as an allowed program

- Enter the following command:

```
netsh firewall delete allowedprogram program="C:\Program Files\Software AG\Natural\6.3\Bin\natural.exe" profile=ALL
```

Method 2 - Allow a Specific Port to be used on your PC

This method involves opening a specific port.

The following examples apply to the Natural executable. To open a port for other Natural or Entire Access components, see *Overview of Executables and Port Numbers* below.

To open a specific port

- Enter the following command:

```
netsh firewall add portopening protocol=TCP port=nnnnn name="Natural" profile=ALL
```

  where *nnnnn* is the number of the port that is to be opened.

To close a specific port

- Enter the following command:

```
netsh firewall delete portopening protocol=TCP port=nnnnn profile=ALL
```

  where *nnnnn* is the number of the port that is to be closed.

Overview of Executables and Port Numbers

To run all of Natural and its subprograms, you will need to open a variety of communications ports, depending on the functionality you are using. Below is a list of programs that need to establish communications ports. You may choose which of the programs or ports you want to use on the PC.

See *Method 1 - Allow a Specific Executable to Open a Port* and *Method 2 - Allow a Specific Port to be used on your PC* for the required syntax.

Important:
The file locations and the port numbers listed below are the default settings. These parameters may be customized during the installation process. If you did not install using the default settings, you will need to use your custom parameters.

Component	**Method 1**		**Method 2**
	Executable	**File Location**	**Default Port number**
Natural	*natural.exe*	*C:\Program Files\Software AG\Natural\6.3\bin*	
Debugger	*natdbgsv.exe*	*C:\Program Files\Software AG\Natural\6.3\bin*	2600
Terminal Emulation	*natpccserver2.exe*	*C:\Program Files\Software AG\Natural\6.3\Terminal*	22334
Entire Access Server	*serversingle.exe*	*C:\Program Files\Software AG\Entire Access\6.1.1\bin*	
Entire Access Client	*vtx3.dll*	*C:\Program Files\Software AG\Entire Access\6.1.1\bin*	