FAQ • 04/2016

Firewall Settings for SIMATIC B.Data

SIMATIC B.Data V6.0 SP1

https://support.industry.siemens.com/cs/ww/en/view/109483556

This entry originates from Siemens Industry Online Support. The conditions of use specified there apply (www.siemens.com/nutzungsbedingungen).

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions only form one element of such a concept.

Customers are responsible to prevent unauthorized access to their plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Contents

1 Introduction

If single components of B.Data are installed on different computers, they are connected with each other via the network. During operation the data flow between the components is via this connection. If the network connection between single components is blocked by a firewall, problems might arise with the data transmission.

This FAQ response shows how to configure the firewall to ensure perfect communication between the components of B.Data and applies for operating systems Windows 7 / 8.1 and Windows Server 2008 / 2012.

The B.Data Acquisition Component as well as the B.Data Client and B.Data Web Server communicate with the application server. The application server itself communicates with the B.Data Database. Therefore, only the application server has access to the database. Furthermore, the so-called "Portal" is on the application server. The Portal is a Windows service that handles the communication between the application server and the other B.Data components. Communication between the Portal and a component is via a TCP Port, which is 4444 by default. If the port is blocked by the firewall, then there is no data flow to the application server.

The acquisition component also has a portal (distributed portal) through which there is a "portal-to-portal" connection between the application server and the acquisition component.

There are three network categories in Windows:

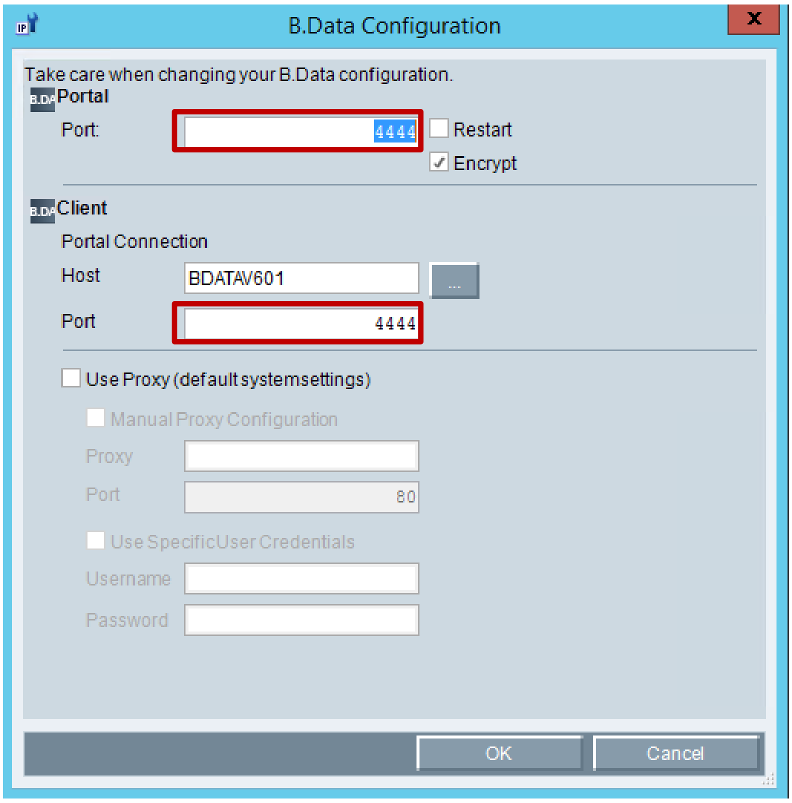
- Private (home network and work network)
- Public network
- Domain

A public network should be used for the connection between the acquisition computer and the application server when the data flow from the acquisition computer to the application server is via the internet. If the acquisition computer and the application server are in a local network, then a private network is sufficient. The connection between the acquisition component and the measuring devices in the field is usually a private network.

2 Changing the Default Port

You can change the port the first time B.Data is started or afterwards in the configuration settings of B.Data. You should note however that you can only change the port for the application server and the local B.Data client. The application server needs a local client so that the dialog can be opened. Note that this client counts for the license.

Figure 2-1 Port settings for the client and the application server



Take care when changing your B.Data configuration.

Portal

Port: 4444 □ Restart ☑ Encrypt

Client

Portal Connection

Host BDATAV601

Port 4444

□ Use Proxy (default systemsettings)

□ Manual Proxy Configuration

Proxy

Port 80

□ Use SpecificUser Credentials

Username

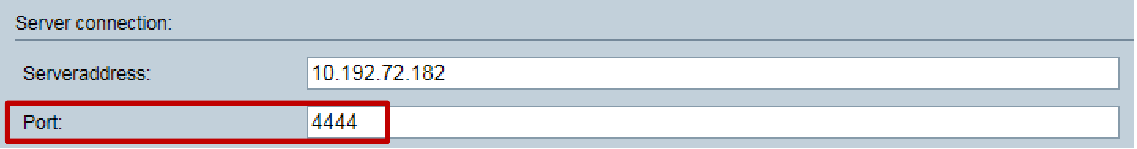
Password

If you use a remote client, you have to open the same dialog as shown in Figure 2-1 again on the remote client and change the port of the remote client there.

You can set the port for the acquisition component when logging on the acquisition component on the application server (pairing). The logon is done via the web browser of the acquisition component.

http://localhost/BDataAcquisition/Login.aspx

Figure 2-2 Port logon of the acquisition component on the application server



Server connection:

Serveraddress: 10.192.72.182

Port: 4444

If you want to change the port in the acquisition component after logon on the application server, you must first change the port of the application server and then the port of the acquisition component. This does not change the acquisition component ID, which ensures that there is no data loss (SINK files are not deleted).

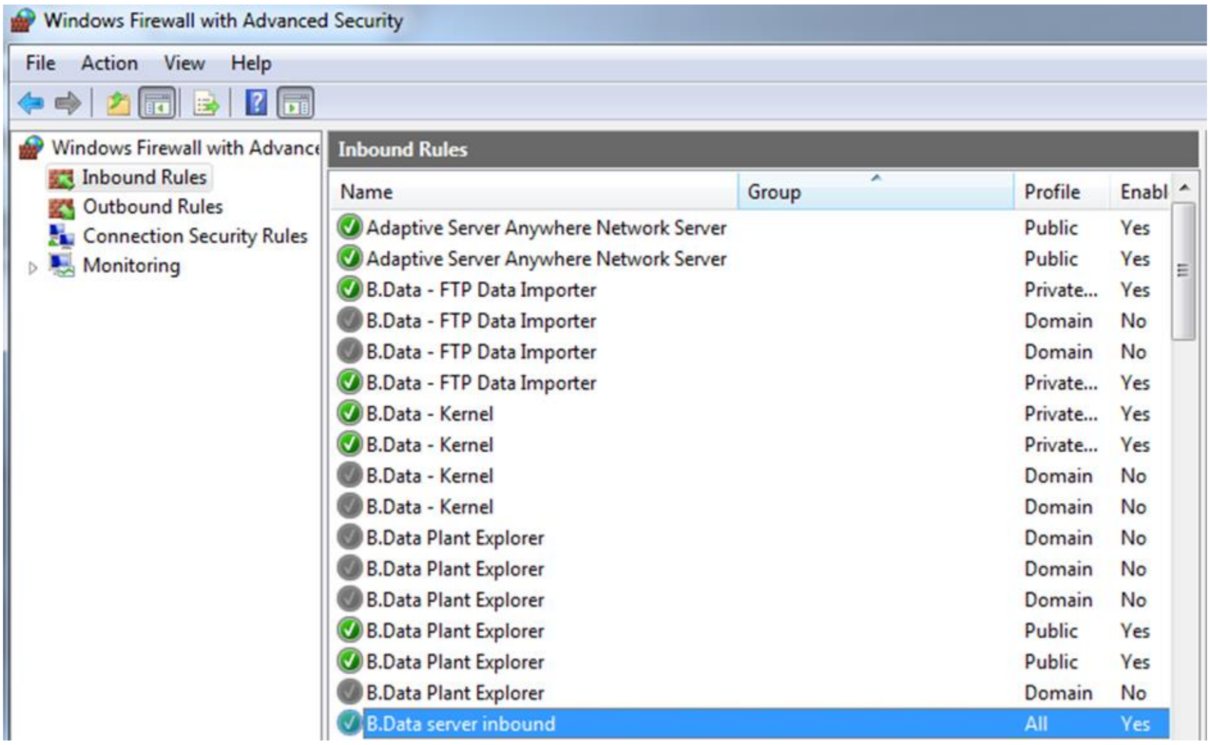
It is important here that the new port also has to be enabled in the firewall settings before you start B.Data, otherwise you would lock yourself out.

3 Firewall Settings on the Application Server

3.1 Make Inbound Rule

First you must make an inbound rule to open the port (also 4444) in the inbound direction on the application server. The same procedure applies here as described in Point 1, but for an inbound rule.

Figure 3-1 Inbound rule for port 4444


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabl
Adaptive Server Anywhere Network Server		Public	Yes
Adaptive Server Anywhere Network Server		Public	Yes
B.Data - FTP Data Importer		Private...	Yes
B.Data - FTP Data Importer		Domain	No
B.Data - FTP Data Importer		Domain	No
B.Data - FTP Data Importer		Private...	Yes
B.Data - Kernel		Private...	Yes
B.Data - Kernel		Private...	Yes
B.Data - Kernel		Domain	No
B.Data - Kernel		Domain	No
B.Data Plant Explorer		Domain	No
B.Data Plant Explorer		Domain	No
B.Data Plant Explorer		Domain	No
B.Data Plant Explorer		Public	Yes
B.Data Plant Explorer		Public	Yes
B.Data Plant Explorer		Domain	No
B.Data server inbound		All	Yes

This ensures that the acquisition component can send measured values to the application server via the portal. Furthermore, this enables a B.Data client to access the application server also from another PC.

3.2 Make Outbound Rule

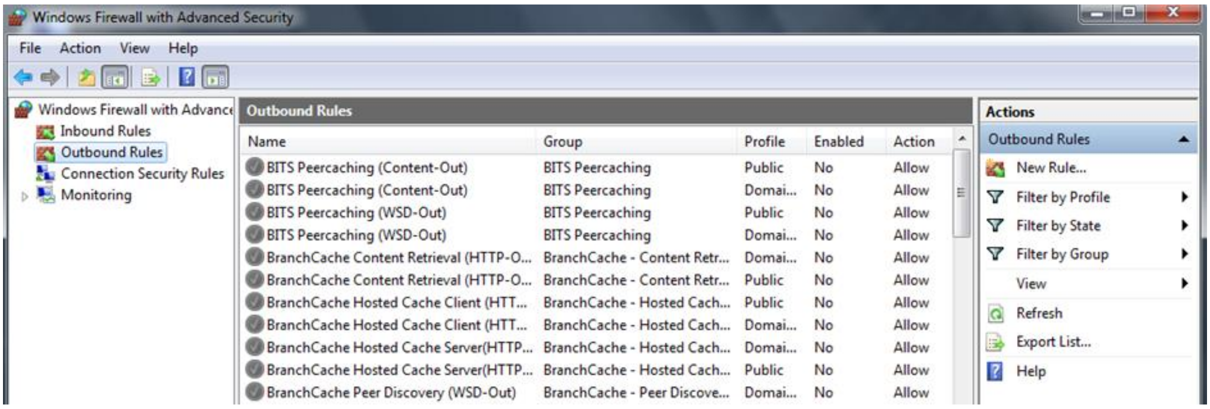
You must also make an outbound rule to open the port in the outbound direction on the application server. You need this rule to enable a B.Data client to search for the application server in the network. If this rule is missing, the application server can be accessed (inbound rule on the application server, Point 3.1), but no search can be made for it.

4 Firewall Settings on the Acquisition Computer

4.1 Make Outbound Rule

First you must make an outbound rule to open port 4444 in the direction of the application server. For this you have to define an outbound IP4 rule. You do this by clicking "New Rule...".

Figure 4-1 Outbound rule for port 4444

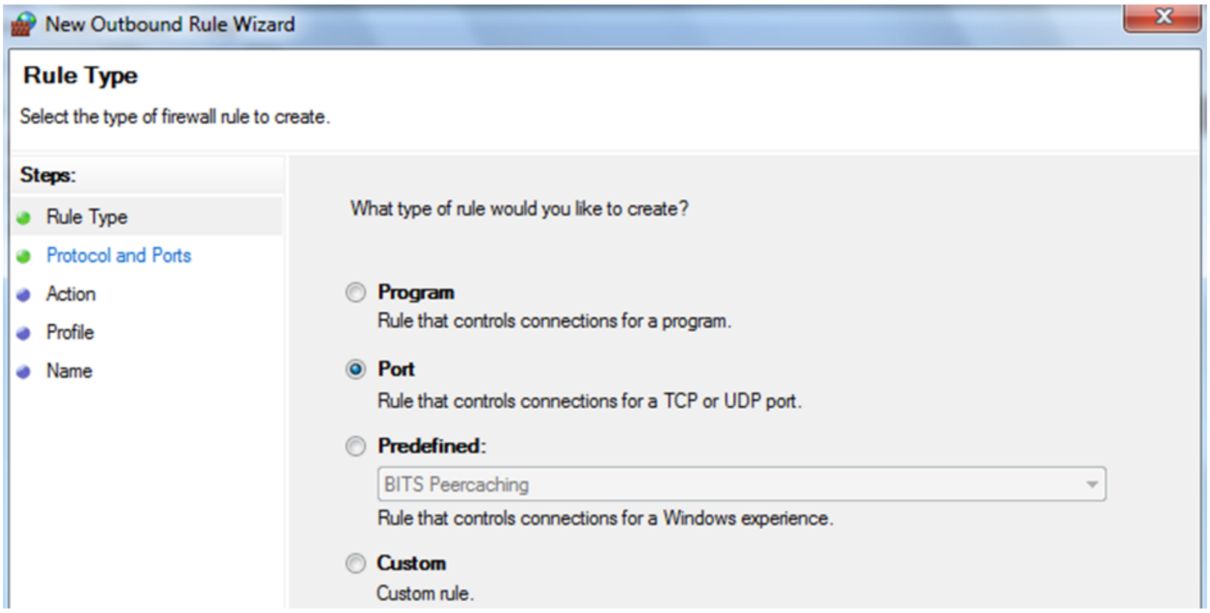


Outbound Rules

Name	Group	Profile	Enabled	Action
BITS Peercaching (Content-Out)	BITS Peercaching	Public	No	Allow
BITS Peercaching (Content-Out)	BITS Peercaching	Domai...	No	Allow
BITS Peercaching (WSD-Out)	BITS Peercaching	Public	No	Allow
BITS Peercaching (WSD-Out)	BITS Peercaching	Domai...	No	Allow
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	Domai...	No	Allow
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	Public	No	Allow
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	Public	No	Allow
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	Domai...	No	Allow
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	Domai...	No	Allow
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	Public	No	Allow
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	Domai...	No	Allow

Then you have to select the port.

Figure 4-2 Rule type: Port



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

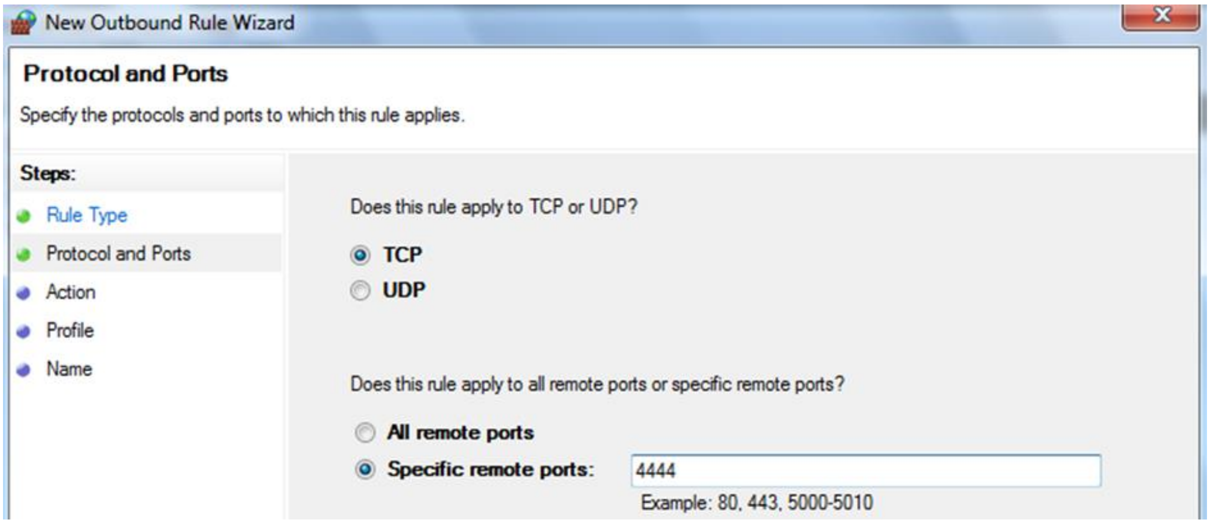
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BITS Peercaching
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

You must also specify the relevant port. In addition you have to select the TCP protocol.

Figure 4-3 Definition of the port



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP
○ UDP

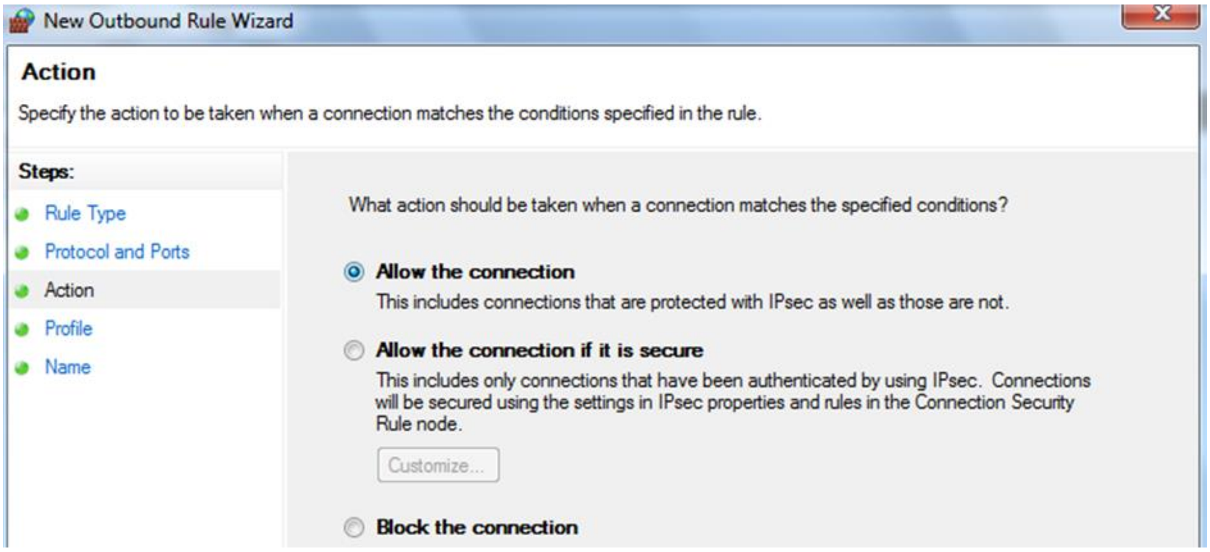
Does this rule apply to all remote ports or specific remote ports?

○ All remote ports
● Specific remote ports: 4444

Example: 80, 443, 5000-5010

Finally, the connection has to be allowed.

Figure 4-4 Enabling the connection



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

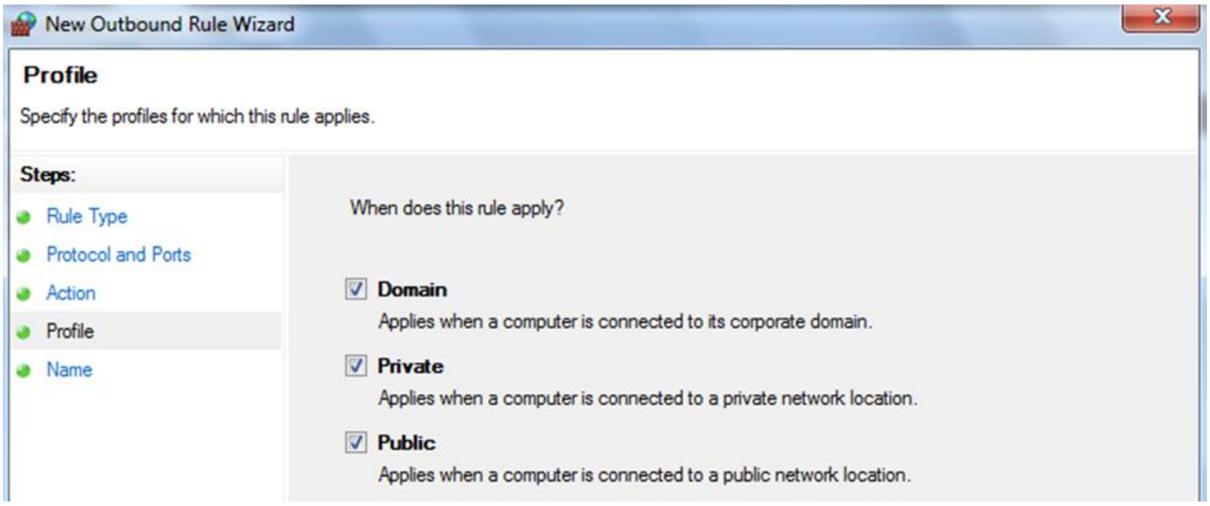
● Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

For each rule made you can select a network profile for which that rule is to be valid.

Figure 4-5 Network type of the rule



New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

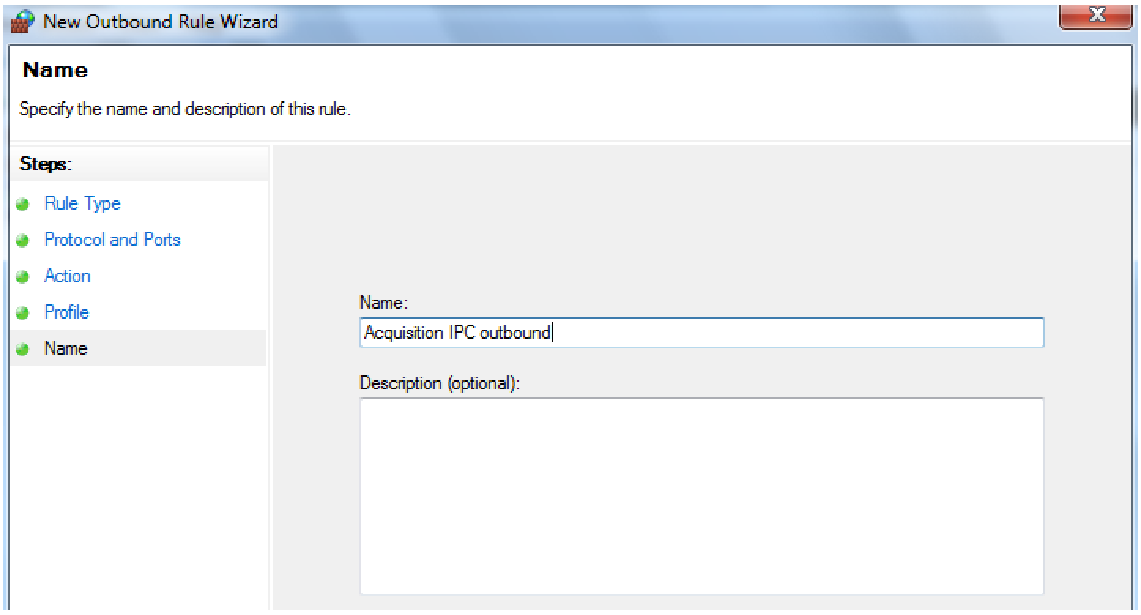
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Each rule needs a name so that the rule can be put subsequently in the list of the outbound rules.

Figure 4-6 Name of the new rule



New Outbound Rule Wizard

Name

Specify the name and description of this rule.

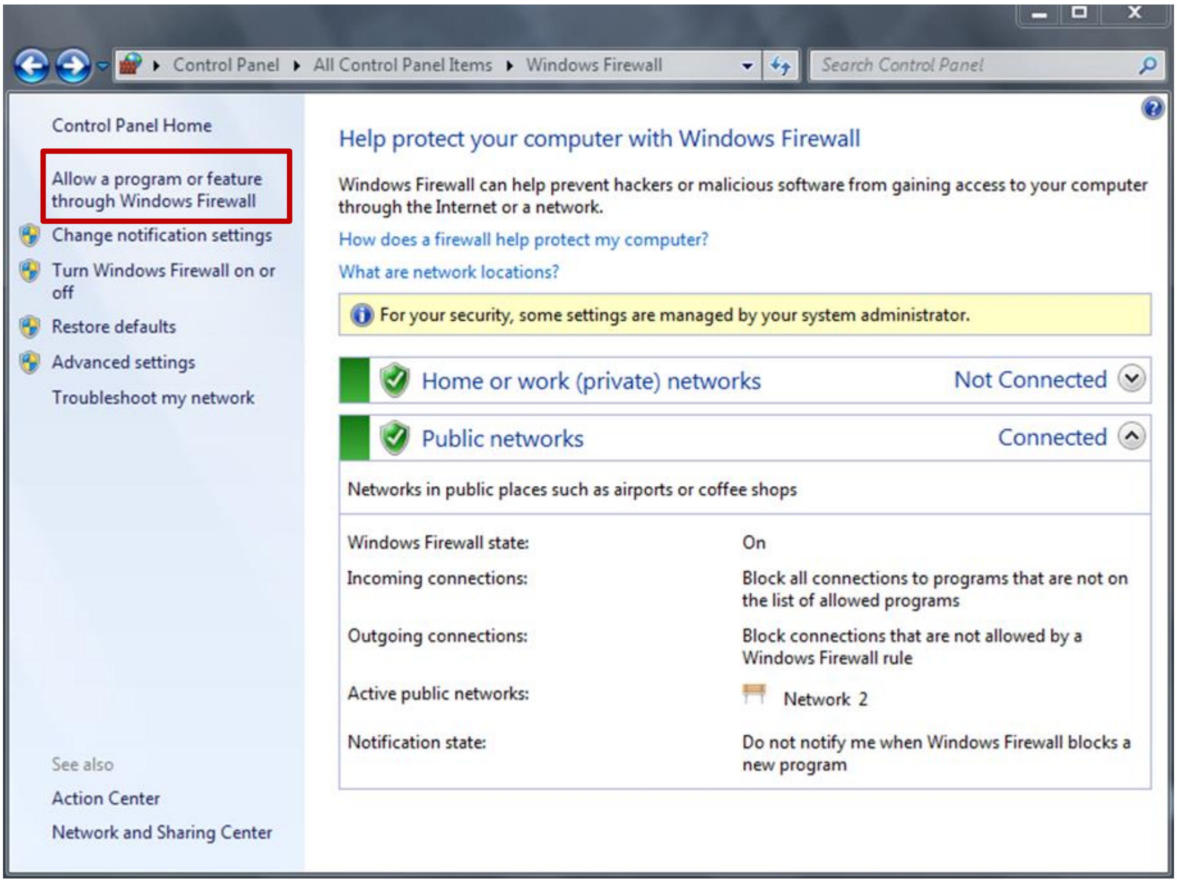
Name:
Acquisition IPC outbound

Description (optional):

4.2 Adding the Applications "B.Data Kernel" and "B.Data Portal" as Exceptions

You then have to make the applications "B.Data Kernel" and "B.Data Portal" (remote portal) exceptions for the firewall. You get to the settings of a firewall directly via the Control Panel by clicking "Windows Firewall". In the Settings dialog of the firewall you then have to click the link "Allow a program or feature through the Windows Firewall".

Figure 4-7 Windows Firewall


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

For your security, some settings are managed by your system administrator.

Home or work (private) networks — Not Connected

Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs

Outgoing connections: Block connections that are not allowed by a Windows Firewall rule

Active public networks: Network 2

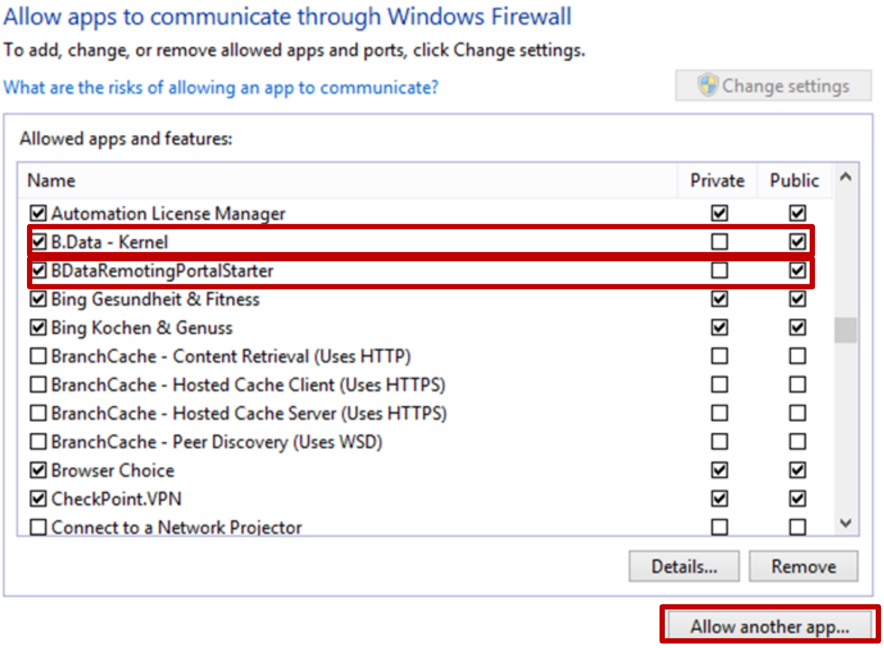
Notification state: Do not notify me when Windows Firewall blocks a new program

Using the "Allow another app..." button you can search for the "Kernel.exe" and "BDataPortal.exe" files and add the exceptions. These two applications are in the installation directory of B.Data.

- Kernel.exe: C:\BData\GUI
- BDataPortal.exe: C:\BData\GUI\BData2008 (depending on the installation directory)

The Kernel is also a Windows service and is the actual acquisition software of B.Data. The Kernel processes the data to data records. In addition, calculations can be made in the Kernel (calculation level 1) and data pre-compressed (for example, the sum or the counter difference).

Figure 4-8 Firewall exceptions on a PC with installed acquisition component



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

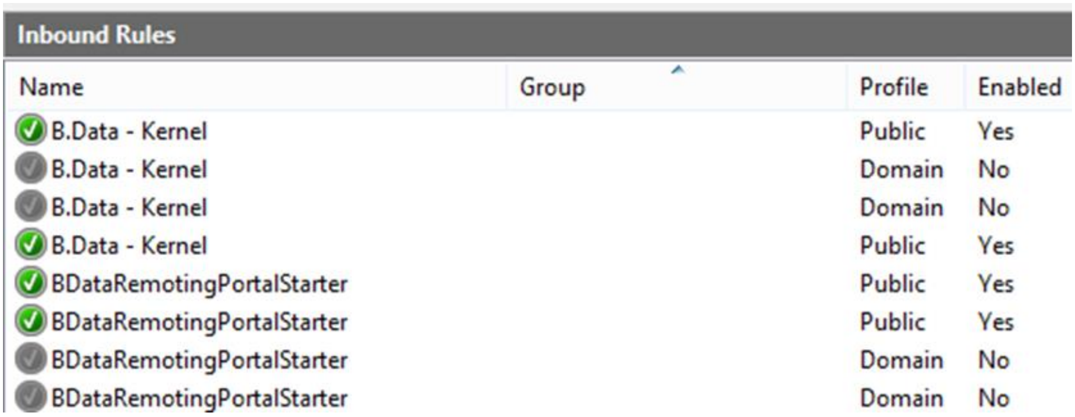
What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Automation License Manager	☑	☑
☑ B.Data - Kernel	□	☑
☑ BDataRemotingPortalStarter	□	☑
☑ Bing Gesundheit & Fitness	☑	☑
☑ Bing Kochen & Genuss	☑	☑
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
☑ Browser Choice	☑	☑
☑ CheckPoint.VPN	☑	☑
□ Connect to a Network Projector	□	□

By adding exceptions you make four inbound rules for each application, one for each protocol (TCP, UDP) as well as for the current network type (public or private) and for the domain network. However, the domain network is not enabled. If the UDP protocol is not permitted, you can disable or delete that rule.

Figure 4-9 Inbound rules of the exception



Inbound Rules

Name	Group	Profile	Enabled
B.Data - Kernel		Public	Yes
B.Data - Kernel		Domain	No
B.Data - Kernel		Domain	No
B.Data - Kernel		Public	Yes
BDataRemotingPortalStarter		Public	Yes
BDataRemotingPortalStarter		Public	Yes
BDataRemotingPortalStarter		Domain	No
BDataRemotingPortalStarter		Domain	No

These four inbound rules are enabled for each port. This ensures acquisition of the measured values from the field level.

It is important still to define in which network profile the applications are to be permitted.

5 Firewall Settings on the Client

If you are using another remote client, you have to adapt the firewall also for this component. The firewall settings for the client are the same as for the acquisition component, which means that an outbound rule is needed for the port (see section 3.1).

6 More Outbound and Inbound Rules in the Firewall Settings for the Interfaces

More rules have to be defined depending on the data source from which the data is taken. The following additional rules are to be defined for the separate interfaces:

Table 6-1 Additional ports required for the separate interfaces

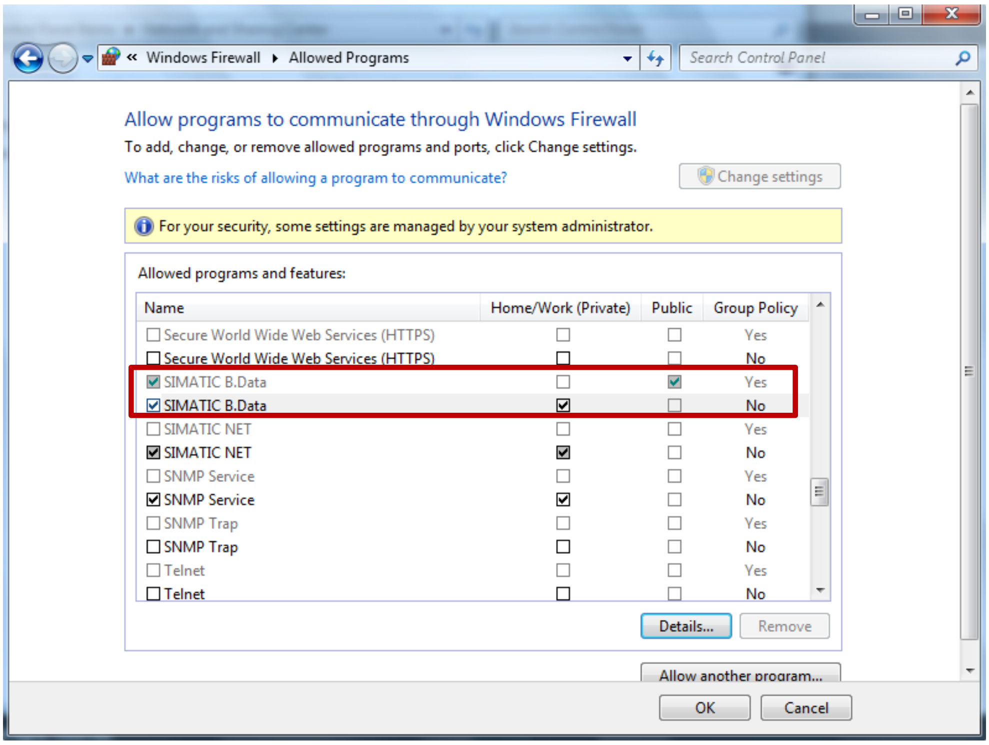
Interface	Port	Program
S7 Connection	Inbound, 102 TCP	
Modbus TCP	Outbound, 502 UDP and TCP	
Modbus RTU device	Outbound, 17002 UDP and TCP	
OPC UA Discovery	Inbound, 4840 TCP	
OPC UA Server	Inbound, 4852 (SIMATIC NET) TCP	
FTP Transfer B.Data	Outbound, 20,21,22 TCP Inbound, 20,21,22 TCP	FTPTransfer.exe
FTP Server	Outbound, 21 TCP Inbound, 21 TCP	svchost.exe
FTP Server passive	Inbound, all TCP	svchost.exe
sFTP Server	Outbound, 989 TCP Inbound, 990 TCP	svchost.exe

Once a rule has been made it can be further processed and added to a program, for example. So you do not have to make a rule for each program and each port. You only have to make a separate rule for each protocol (TCP, UDP).

7 Acquisition IPC

When using an Acquisition IPC you should note that the firewall is already preconfigured so that you do not have to change the firewall at all.

Figure 7-1 Predefine firewall setting of the Acquisition IPC



« Windows Firewall ▸ Allowed Programs

Search Control Panel

Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Change settings

For your security, some settings are managed by your system administrator.

Allowed programs and features:

Name	Home/Work (Private)	Public	Group Policy
☐ Secure World Wide Web Services (HTTPS)	☐	☐	Yes
☐ Secure World Wide Web Services (HTTPS)	☐	☐	No
☑ SIMATIC B.Data	☐	☑	Yes
☑ SIMATIC B.Data	☑	☐	No
☐ SIMATIC NET	☐	☐	Yes
☑ SIMATIC NET	☑	☐	No
☐ SNMP Service	☐	☐	Yes
☑ SNMP Service	☑	☐	No
☐ SNMP Trap	☐	☐	Yes
☐ SNMP Trap	☐	☐	No
☐ Telnet	☐	☐	Yes
☐ Telnet	☐	☐	No

Remark

The Acquisition IPC has two network adapters The adapter with the ID X1P1 is to be used for the internet/intranet (public network) and the adapter X2P1 is reserved for the process network (private network) in which the field level measuring devices are incorporated. The Windows firewall on the Acquisition IPC is pre-configured accordingly (see Figure 7-1).