# **SIEMENS**

Application description • 6/2016

# Windows firewall settings for X-Tools Server Pro

CMS X-Tools / V 04.03 / CPU 416-3 PN/DP

# Warranty and liability

#### Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice. If there are any deviations between the recommendations provided in these application examples and other Siemens publications – e.g. Catalogs – the

contents of the other documents have priority.

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

Security information Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit <u>http://www.siemens.com/industrialsecurity</u>.

To stay informed about product updates as they occur, sign up for a productspecific newsletter. For more information, visit <u>http://support.industry.siemens.com</u>.

## **Table of contents**

| Warr | anty and                               | liability  | 2                |
|------|--|--|------------------|
| 1    | Preface                                |  | 4                |
|      | 1.1<br>1.2<br>1.3<br>1.4<br>1.5<br>1.6 | Overview<br>Basic knowledge required<br>Required software<br>Required hardware<br>Scope of delivery<br>Further information | 4<br>4<br>5<br>5 |
| 2    | Allow X                                | -Tools Server Pro through the Windows firewall   | 7                |
| 3    | Advanc<br>Server I                     | ed firewall settings: how to create manual rules for X-Tools<br>Pro  | 11               |
|      | 3.1<br>3.2<br>3.3                      | Create inbound rules<br>Create outbound rules<br>Rules advanced settings   | 13<br>17<br>17   |
| 4    | Contact                                | information  | 20               |
| 5    | History                                |  | 20               |

## 1 Preface

### 1.1 Overview

The ION SIMATIC S7 PN is a software component used to acquire data from a SIMATIC controller with an integrated PROFINET module. The data acquired can then be analyzed and stored in X-Tools.

With the default settings of the Windows firewall, it is often impossible to set up this connection and exchange data with the device.

In this document, we will explain how to set up the Windows firewall and create the relevant rules to authorize the connection and data traffic between X-Tools and SW ION.



Figure 1-1: CMS X-Tools - architecture

## 1.2 Basic knowledge required

In order to understand this application description, a general knowledge of automation technology and software packages CMS X-Tools is required. In addition, you must be familiar with network technology (UDP/IP) and with using computers with Windows.

## 1.3 Required software

This document is valid for the following software:

- CMS X-Tools Professional V 04.03
- Microsoft Windows 7

Using different software versions can lead to variations in the steps described below.

**NOTE** To change the security settings of Windows and the firewall settings in particular, administrator rights are required. Some settings can only be managed by your system administrator.

### 1.4 Required hardware

PC with Microsoft Windows 7.
 For more details about the compatible hardware configurations for CMS X-Tools, check out the following document: CMS X-Tools (All Editions) User Manual – 01 – Introduction.EN.pdf/Page 25.

**NOTE** Although X-Tools is compatible with older configurations, in this tutorial we will only tackle the Windows 7 settings. These explanations are not relevant for Windows XP, because this OS leads to variations in the steps described below.

The X-Tools client and server can also be installed on different systems.

### 1.5 Scope of delivery

No files are delivered with this document.

### **1.6** Further information

This document will not provide a detailed description of all features. More information can be found in:

• CMS X-Tools – User Manual 01 - 07

# 2 Allow X-Tools through the Windows firewall at the first startup of X-Tools

When you start the X-Tools software for the first time, if the Windows firewall is enabled, this window could display:

| 💮 Windows Secu                  | rity Alert                         | ×   |
|---------------------------------|------------------------------------|---|
| Window                          | s Firewall has                     | 5 blocked some features of this program   |
| Windows Firewall h<br>networks. | as blocked som                     | e features of X-Tools Server Pro on all public and private                                    |
|                                 | Name:                              | X-Tools Server Pro  |
|                                 | Publisher:                         | Siemens AG  |
|                                 | Pat <u>h</u> :                     | C:\program files\siemens\cms x-tools pro v 04.03\server<br>\system\bin\x-tools server pro.exe |
| Allow X-Tools Serve             | er Pro to commu                    | unicate on these networks:  |
| Private netv                    | vorks, such as r                   | my home or work network   |
| Public netwo<br>because the     | orks, such as th<br>se networks of | ose in airports and coffee shops (not recommended<br>ften have little or no security)         |
| What are the risks              | of allowing a pr                   | ogram through a firewall?   |
|                                 |                                    | <u>Allow access</u> Cancel  |

Allow access for the desired network profiles. There are specific settings for each network profile (domain, private, public).

You must have administration rights; if you don't, please contact your network administrator.

**NOTE:** Only inbound Rules will be created by Windows. You will have to manually create outbound Rules for the X-Tools server later.

3

## Add X-Tools Server Pro to the list of programs authorized by the Windows firewall

Most of the time, connection failures between the X-Tools Server and SW ION are caused by the Windows firewall. The default settings do not allow every application to exchange data on the network, and the specific rules for X-Tools may have not been created at the first start.

Illustration of the problem in the X-Tools Device Management System interface:



... but the Device Profile startup fails (blue status  $\rightarrow$  no data in the MDS explorer) This is usually a Windows firewall issue. In this situation, you must manually configure the Windows firewall to allow the X-Tools server to communicate with a network through the firewall.

Go to the Windows Control Panel and open the System and Security settings.



Select Allow a program through Windows Firewall.



Click on *Change Settings* (administrator rights required) and add *X-Tools Server Pro* to the allowed programs and features) for the relevant network categories (domain, private, public).

| Programs: |                              |                     |              |
|-----------|------------------------------|---------------------|--------------|
| 🖉 Settin  | g                            |                     |              |
| UaExp     | pert                         |                     |              |
| Unins     | tall                         |                     |              |
| Winda     | ows DVD Maker                |                     |              |
| Winda     | ows Fax and Scan             |                     |              |
| 😨 Winde   | ows Media Center             |                     |              |
| 🗳 Windo   | ows Remote Assistance        |                     |              |
| XPS V     | iewer                        |                     | ſ            |
| X-Too     | ls Client Pro                |                     | 6            |
| X-Too     | ls Server Pro                |                     |              |
| X-Too     | ls Tray Pro                  |                     |              |
| ath:      | C:\Program Files\Sien        | nens\CMS X-Tools Pr | o V ( Browse |
|           | and the second second second | rogram2             |              |

Click on Change Settings and check the desired profile options.

| add, change, or remove allowed programs      |              |                       |             |                 |      |
|--|--------------|-----------------------|-------------|-----------------|------|
| add, change, of remove allowed programs      | and ports, c | lick Change settings. | _           | <u> </u>        |      |
| at are the risks of allowing a program to co | mmunicate    | ?                     |             | 牙 Change settir | ngs  |
|  |              |                       | 202         |                 |      |
| For your security, some settings are mana    | aged by you  | r system administrato | or.         |                 |      |
| Manual management of factors                 |              |                       |             |                 |      |
| anowed programs and reacures.                |              |                       | 1.5.5.7.64- | (s. 1993)       | 1251 |
| Name   | Domain       | Home/Work (Pri        | Public      | Group Policy    | 1    |
| Windows Firewall Remote Management           |              |                       |             | No              |      |
| Windows Management Instrumentatio            |              |                       |             | No              |      |
| □ Windows Media Player                       |              |                       |             | No              |      |
| Windows Media Player Multicast Strea         |              |                       |             | Yes             |      |
| Windows Media Player Multicast Strea         |              |                       |             | Yes             |      |
| Windows Media Player Network Sharin          |              |                       |             | No              |      |
| Windows Media Player Network Sharin          |              |                       |             | No              |      |
| Windows Peer to Peer Collaboration Fo        |              |                       |             | No              |      |
| □ Windows Remote Management                  |              |                       |             | No              |      |
| Wireless Portable Devices                    |              |                       |             | No              |      |
|  |              |                       |             |                 |      |

**NOTE:** You may be unable to add X-Tools Server Pro to the list of authorized programs.



If an error appears, go on to the next step and the advanced Firewall Settings. We will now describe how to manually add new rules in the Windows firewall for the X-Tools Server.

# 4

## Advanced firewall settings: how to manually create rules for X-Tools Server Pro

The two previous steps may not succeed. What's more, these steps will add only inbound rules. To exchange data on the network, specific outbound rules for X-Tools Server need to be created as well, and you must add these rules manually.

- ✓ If you managed to create inbound rules in one of the previous steps, go on to step 3.2 to create outbound rules
- ✓ If you did not, begin working here:

Go on to the Windows Control Panel.

Open System and Security, and Windows Firewall.





Open the Advanced Firewall Settings.

The following window displays. We will now create specific *inbound* and *outbound rules* for the X-Tools server.

| ndows Firewall with Advanced   | Windows Firewall with Advanced Security on Local Computer   | Actions                                     |
|--|---|---|
| Inbound Rules<br>Outbound Rules<br>Connection Security Rules<br>Monitoring | Windows Firewall with Advanced Security provides network security for Windows computers.  | Windows Firewall with Advanced Sec          |
|  |   | Restore Default Policy<br>Diagnose / Repair |
|  | Domain Profile  | View  |
|  | <ul> <li>Windows Firewall is on.</li> <li>Inbound connections that do not match a rule are blocked.</li> </ul>  | Refresh     Properties                      |
|  | Outbound connections that do not match a rule are allowed.  | 😰 Help                                      |
|  | Private Profile Windows Firewall is on. Insound connections that do not match a rule are blocked. Insound connections that do not m |   |
|  | Couldant controllar is that do not match a rule are blocked.      Public Profile is Active     Windows Firewall is on.     Inbound connections that do not match a rule are blocked.  |   |
|  | Outbound connections that do not match a rule are allowed.     Windows Firewall Properties  |   |
|  | Getting Started         Authenticate communications between computers         Create connection security rules to specify how and when connections between computers are auth protected by using Internet Protocol security (IPsec).         Image: Connection Security Rules   |   |
|  | View and create firewall rules<br>Create firewall rules to allow or block connections to specified programs or ports. You can also allow  |   |

## 4.1 Create inbound rules

We will first create inbound rules:



Choose the Program rule type.

| Prew Inbound Rule Wiza                         | ard  |
|--|--|
| Rule Type<br>Select the type of firewall rule  | to create.   |
| Steps:<br>Program<br>Action<br>Profile<br>Name | What type of nule would you like to create? <b>Porgram</b> Rule that controls connections for a program. <b>O Pot</b> Rule that controls connections for a TCP or UDP pot. <b>Prodefined Prodefined RanchCache - Content Retrieval (Uses HTTP) Rule that controls connections for a Windows experience. O Lostom Leam more about rule types Leam more about rule types</b> |
|  |  |

Type the program path or choose the Browse option to explore the disk.



In the next step, choose Allow the connection or Allow the connection if it is secure, if required in this use case.

| Action  |   |
|---|---|
| Specify the action to be tak                                | en when a connection matches the conditions specified in the rule.  |
| Steps:<br>Rule Type<br>Program<br>Action<br>Profile<br>Name | <ul> <li>What action should be taken when a connection matches the specified conditions?</li> <li>Allow the connection</li> <li>This includes connections that are protected with IPsec as well as those are not.</li> <li>Allow the connection if it is secure</li> <li>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.</li> <li>Customize</li> </ul> |
|   | Block the connection Learn more about actions Back Next Cancel  |

| Prew Inbound Rule W                                 | zard   |
|---|--|
| Profile<br>Specify the profiles for which           | h this rule applies.   |
| Steps:<br>Rule Type<br>Program<br>Action<br>Profile | When does this rule apply?           Image: Domain Applies when a computer is connected to its corporate domain.   |
| Name  | <ul> <li>Private         Applies when a computer is connected to a private network location.</li> <li>Public         Applies when a computer is connected to a public network location.</li> </ul> |
|   | Learn more about profiles          < Back  |

Select the profiles to which the rule will apply.

#### Choose a name for the rule.

| Name                          |                         |
|-------------------------------|-------------------------|
| Specify the name and descript | of this rule.           |
| Steps:                        |                         |
| Rule Type                     |                         |
| Program                       |                         |
| Action                        |                         |
| Profile                       | Name:                   |
| Name                          | X-Tools Server Pro      |
|                               | Description (optional): |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               |                         |
|                               | < Back Finish Cancel    |

| Windows Firewall with Advanced | Inbound Rules          |       |         |         |       |          |          |               |                   |            | Actions                               |
|--------------------------------|------------------------|-------|---------|---------|-------|----------|----------|---------------|-------------------|------------|---------------------------------------|
| Inbound Rules                  | Name                   | Group | Profile | Enabled | Acti  | Override | Program  | Local Address | Remote Address    | Protocol ^ | Inbound Rules 🔺                       |
| Connection Security Bules      | X-Tools Server Pro     |       | Domai   | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | ka New Rule                           |
| Monitoring                     | Albd_Server            |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | Filter by Profile                     |
|                                | 🕑 CleardIg             |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        |                                       |
|                                | 🕜 CleardIg             |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | Y Filter by State                     |
|                                | <b>O</b> Clearexplorer |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | Filter by Group                       |
|                                | Clearfindco            |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | View                                  |
|                                | 🕑 ClearIstype          |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | Default                               |
|                                | Cleartool              |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | Ga Kerresh                            |
|                                | Core Networking        |       | Domain  | No      | Allow | No       | Any      | Any           | Any               | ICMPv4     | Export List                           |
|                                | 🔇 Core Networking      |       | Domai   | Yes     | Allow | No       | Any      | Any           | Any               | ICMPv4     | 7 Help                                |
|                                | Ост                    |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        |                                       |
|                                | Inbound Ports for      |       | Domain  | Yes     | Allow | No       | Any      | Any           | 139.25.127.102, 1 | TCP        | X-Tools Server Pro                    |
|                                | Inbound Ports for      |       | Domain  | Yes     | Allow | No       | Any      | Any           | 139.25.127.102, 1 | UDP        | Disable Rule                          |
|                                | 🕑 Internet Explorer M  |       | Domain  | Yes     | Allow | No       | %progra  | Any           | Any               | UDP        | K Cut                                 |
|                                | 🕑 Internet Explorer M  |       | Domain  | Yes     | Allow | No       | %progra  | Any           | Any               | UDP        | B. Carri                              |
|                                | IPINS - home at Eagle  |       | Domain  | Yes     | Allow | No       | Any      | Any           | 139.25.231.128/27 | TCP        | ев сору                               |
|                                | 🕑 Java_1.8.0.65        |       | Domain  | Yes     | Allow | No       | C:\Progr | Any           | Any               | Any        | 🗙 Delete                              |
|                                | 🕑 Java_1.8.0.65_x86    |       | Domain  | Yes     | Allow | No       | C:\Progr | Any           | Any               | Any        | Properties                            |
|                                | Microsoft commun       |       | Domain  | Yes     | Allow | No       | %Progra  | Any           | Any               | Any        | 12 Help                               |
|                                | Microsoft Office Co    |       | Domain  | Yes     | Allow | No       | C:\Progr | Any           | Any               | UDP        | I I I I I I I I I I I I I I I I I I I |

Your rule now appears on the list. The green dot shows that the rule is enabled.

**NOTE:** You can check that X-Tools Server Pro has been added to the list of the programs authorized by the Windows firewall for the selected profiles:

| hat are the risks of allowing a program to cor | nmunicate  | 2                     |        | 🖁 Change settir |
|--|------------|-----------------------|--------|-----------------|
| For your security, some settings are mana      | ged by you | r system administrate | or.    |                 |
| Allowed programs and features:                 |            |                       |        |                 |
| Name   | Domain     | Home/Work (Pri        | Public | Group Policy    |
| Windows Firewall Remote Management             |            |                       |        | No              |
| Windows Management Instrumentatio              |            |                       |        | No              |
| Windows Media Player                           |            |                       |        | No              |
| Windows Media Player Multicast Strea           |            |                       |        | Yes             |
| Windows Media Player Multicast Strea           | ~          |                       |        | Yes             |
| Windows Media Player Network Sharin            |            |                       |        | No              |
| Windows Media Player Network Sharin            |            |                       |        | No              |
| Windows Peer to Peer Collaboration Fo          |            |                       |        | No              |
| Windows Remote Management                      |            |                       |        | No              |
| Wireless Portable Devices                      |            |                       |        | No              |
| ☑ X-Tools Server Pro                           |            |                       |        | No              |
|  | 3250       | 1 - 1770 P. 1         |        |                 |

### 4.2 Create outbound rules

| File Action View     | Help  |                        |
|----------------------|---|------------------------|
| Windows Firewall wit | h Advanced Outbou                                       | nd Rules               |
| Connection Se        | New Rule  | ta                     |
| Monitoring           | Filter by Profile<br>Filter by State<br>Filter by Group | , ta<br>ta<br>ta<br>ta |
|                      | View  | ↓ er                   |
|                      | Refresh<br>Export List                                  | ier<br>ier             |
|                      | Help  | ec                     |

The steps are the same. See the explanation for creating inbound rules.

### 4.3 Rules advanced settings

The previous wizard helps you create new rules with basic settings.

The *Properties* menu opens an overview of all the advanced settings, to create safe and custom rules for your particular use case.

| File Action View Help                            |  |                                       |  |   |
|--|--|---------------------------------------|--|---|
| P Windows Firewall with Advance                  | Outbound Rules   |                                       |  |   |
| Inbound Rules                                    | Name   | Group                                 |  | Prof                                    |
| Lage Connection Security Rules<br>▷ 🛃 Monitoring | <ul> <li>X-Tools Server Pro</li> <li>Wireless Portable Devices (UPn</li> <li>Wireless Portable Devices (UPn</li> <li>Wireless Portable Devices (TCP</li> <li>Wireless Portable Devices (TCP</li> <li>Wireless Portable Devices (SSD</li> </ul> | Disable Rule<br>Cut<br>Copy<br>Delete | le Devices<br>le Devices<br>le Devices<br>le Devices<br>le Devices<br>le Devices | Don<br>All<br>All<br>Priv<br>Don<br>All |
|  | Windows Peer to Peer Collabo<br>Windows Peer to Peer Collabo<br>Windows Peer to Peer Collabo   | Properties<br>Help                    | o Peer Colla<br>o Peer Colla<br>o Peer Colla                                     | All<br>All<br>All                       |

You can change the profiles to which the rule applies (add or delete) in the Advanced tab.



You can filter the IP addresses allowed in the Scope tab.

| General                                     | Programs and Ser           | vices   | Computers  | Any  |
|---|----------------------------|---|--|--|
| Protocols and Ports                         | Scope                      | Advanced  | Users  | Local sub  |
| Local IP address<br>C Any IP ac<br>These IP | ldress<br>addresses:       | Add   |  | Local sul<br>Any<br>Local sul<br>Local sul<br>Any<br>Local sul |
| Remote IP address                           | IP Addres                  | s<br>the IP addresses to  | o match:   |  |
| Inese Ir                                    | 123                        | .456.5.8  | inst.  |  |
| Leam more about setting                     | the sec This<br>Fro<br>To: | mples: 192.168.0.<br>192.168.1.<br>2002:9d3b<br>2002:9d3b<br>2002:9d3b<br>IP address range:<br>n: | 12<br>0/24<br>:1a31:4:208:74ff fe35<br>:1a31:4:208:74ff fe35 | 9:6c43<br>9:0/112  |
|   | Leam m                     | ore about specifyir   | iq IP addresses<br>OK  | Cancel   |

You can also specify a protocol and a port: allow the connection for just one specific port, for example.

| General                    | Programs and Services  |  | ces      | Computers |     |
|----------------------------|------------------------|--|----------|-----------|-----|
| Protocols and Ports        | Sco                    | ope  | Advanced | Use       | ers |
| Protocols and ports        |                        |  |          |           |     |
| Protocol ty                | pe:                    | Any  |          | -         |     |
| Protocol nu                | umber:                 | Any<br>Custom<br>HOPOPT  |          |           |     |
| Local port:                |                        | ICMPv4<br>IGMP   |          |           |     |
| Remote po                  | rt:                    | UDP<br>IPv6<br>IPv6-Route<br>IPv6-Frag<br>GRE<br>ICMPv6<br>IPv6-NoNx | e<br>t   |           |     |
| Internet Co<br>(ICMP) sett | ntrol Message<br>ings: | VRRP<br>PGM<br>L2TP  |          |           |     |
| am more about prot         | ocol and ports         |  |          |           |     |

If necessary, create one specific rule for each protocol and security setting you are going to use.

## 5 Contact information

Should you have any questions concerning the software application, please refer to the Industry Sector Technical Support.

### Department

Siemens AG

Industry Sector

### Phone

+49 (0) 911 895 7222 (Monday to Friday, 9:00 a.m. to 5:00 p.m. CET/CEST)

### Fax

+49 (0) 911 895 7223

#### Internet

https://support.industry.siemens.com/cs/

Thank you for using one of the above-mentioned contacts to ensure that your inquiry is registered and can be processed.

# 6 History

| Version | Date    | Modifications |
|---------|---------|---------------|
| V1.0    | 07/2016 | First version |
|         |         |               |
|         |         |               |