

# Installing AxtrexNG 27 Remote Client

Technical Support Engineering  
Rosslare Security NA

For more information please see

[www.axtraxng.com](http://www.axtraxng.com)

Begin the installation by extracting the installation package .ZIP file to a directory and browse to that directory or by browsing to the CDROM, SW, AXTRAXNG directory.

Right click on the *AxtraxNGSetup.....EXE* file and select “Run As Administrator”.

Follow the instructions on the subsequent screens to complete the installation.

# AxTraxNG Setup



Extracting axtrax32GR.ico  
Extracting AUTORUN.INF  
Extracting CRRedist2008\_x86.msi  
Extracting hdd32.exe  
Extracting SQLEXPRESS\_x86\_ENU.exe  
Extracting setup.exe  
Extracting dotNetFx40\_Full\_x86\_x64.exe  
Extracting dotnetfx35.exe

- Navigate to the directory where the file was extracted.
- Right Click the AxtraxNGSetup...EXE and select "Run as Administrator".

Destination folder

C:\Users\bames\AppData\Local\Temp\RarSFX0

Browse...

Installation progress



Install

Cancel

Right click on the *AxtraxNGSetup.....EXE* file and select “**Run As Administrator**”.

On the following screen select the option to be installed.

AxtraxNG Client is the user interface where all configuration information and changes are made. User updates, event logs and reports are all accessed through AxtraxNG Client.

Guard Screen is provides a dedicated screen for security or receptionist use displaying the user information each time a badge is read. It may be installed alone or in conjunction with AxtraxNG Client.

Once you select START the installation will begin, follow through selecting the default as shown in the following slides, do not change any file locations or other data, click NEXT, INSTALL or FINISH on each screen to advance the installer.

- Check the box "I Agree".
- Select Client and/or Guard Screen.
- Click Start.

### AxTraxNG Installation v

#### AxTraxNG Server and Client Requirements:

Operating System	Windows 7 (32/64 bits) SP1
Processor	Minimum: Intel Dual core 2.4 GHz or Equivalent Recommended: Intel core i5 or i7 CPU
Memory	Minimum: 2 GB Recommended: 8 GB
Network	LAN card required for TCP/IP networking
Hard Disk Space	5 GB minimum

#### SQL- Server Express Requirements:

Processor	Pentium 4 or better
Memory	2 GB
Hard Disk Space	4 GB

Software of any kind provided with or as part of the product is provided explicitly "as is", within an explicit denial of all warranties, expressed or implied (including, without limitation, warranties of merchantability, non-infringement, or fitness for a particular purpose), but nevertheless, Rosslare guarantees that the software to be free from defects for a period of ninety (90) days after delivery. If any defect appears within the warranty period, you can contact Rosslare to receive replacement software free of charge at the discretion of Rosslare. Rosslare does not warrant and has no responsibility for the accuracy or completeness of any information, text, graphics, links, or other items contained within the software.

I agree

Select your installation configuration and press Start button

Server with Watchdog

Vitrax version 2.4.0.11545

Client

Vitrax LPR version 1.7.1 Beta (build 1000)

Watchdog

Start

Close

- Crystal Reports, Dahua Merge and Stroke Scribe packages will install just as they did on the Server machine.

## AxTraxNG Installation

### AxTraxNG Server and Client Requirements:

Operating System	Windows 7 (32/64 bits) SP1
Processor	Minimum: Intel Dual core 2.4 GHz or Equivalent Recommended: Intel core i5 or i7 CPU
Memory	Minimum: 2 GB Recommended: 8 GB
Network	LAN card required for TCP
Hard Disk Space	5 GB minimum

### SQL- Server Express Requirements:

Processor	Pentium 4 or better
Memory	2 GB
Hard Disk Space	4 GB

Software of any kind provided with or as part of the product is provided explicitly "as is", within an explicit denial of all warranties, expressed or implied (including, without limitation, warranties of merchantability, non-infringement, or fitness for a particular purpose), but nevertheless, Rosslare guarantees that the software to be free from defects for a period of ninety (90) days after delivery. If any defect appears within the warranty period, you can contact Rosslare to receive replacement software. Rosslare does not warrant and has no liability for any information, text, graphics, links, or other items

### Crystal Reports Basic Runtime for Visual Studio 2008



Please wait while Windows configures Crystal Reports Basic Runtime for Visual Studio 2008

Time remaining: 3 seconds



Cancel

### Start button

- Vitrax version 2.4.0.11545
- Vitrax LPR version 1.7.1 Beta (build 1000)

Please wait, Crystal Report Redistributable installing....



Start

Close



## Welcome to the InstallShield Wizard for AxTraxNG Client

The InstallShield(R) Wizard will install AxTraxNG Client on your computer. To continue, click Next.

- This is the AxtraxNG Client.
- Click NEXT to install, cancel to skip.

Program is protected by copyright law and international treaties.

< Back

Next >

Cancel



## Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.



Install AxTraxNG Client to:

C:\Program Files (x86)\Rosslare\AxTraxNG Client\

Change...

- Do Not change the location.
- Click NEXT to install.

InstallShield

< Back

Next >

Cancel





## InstallShield Wizard Completed

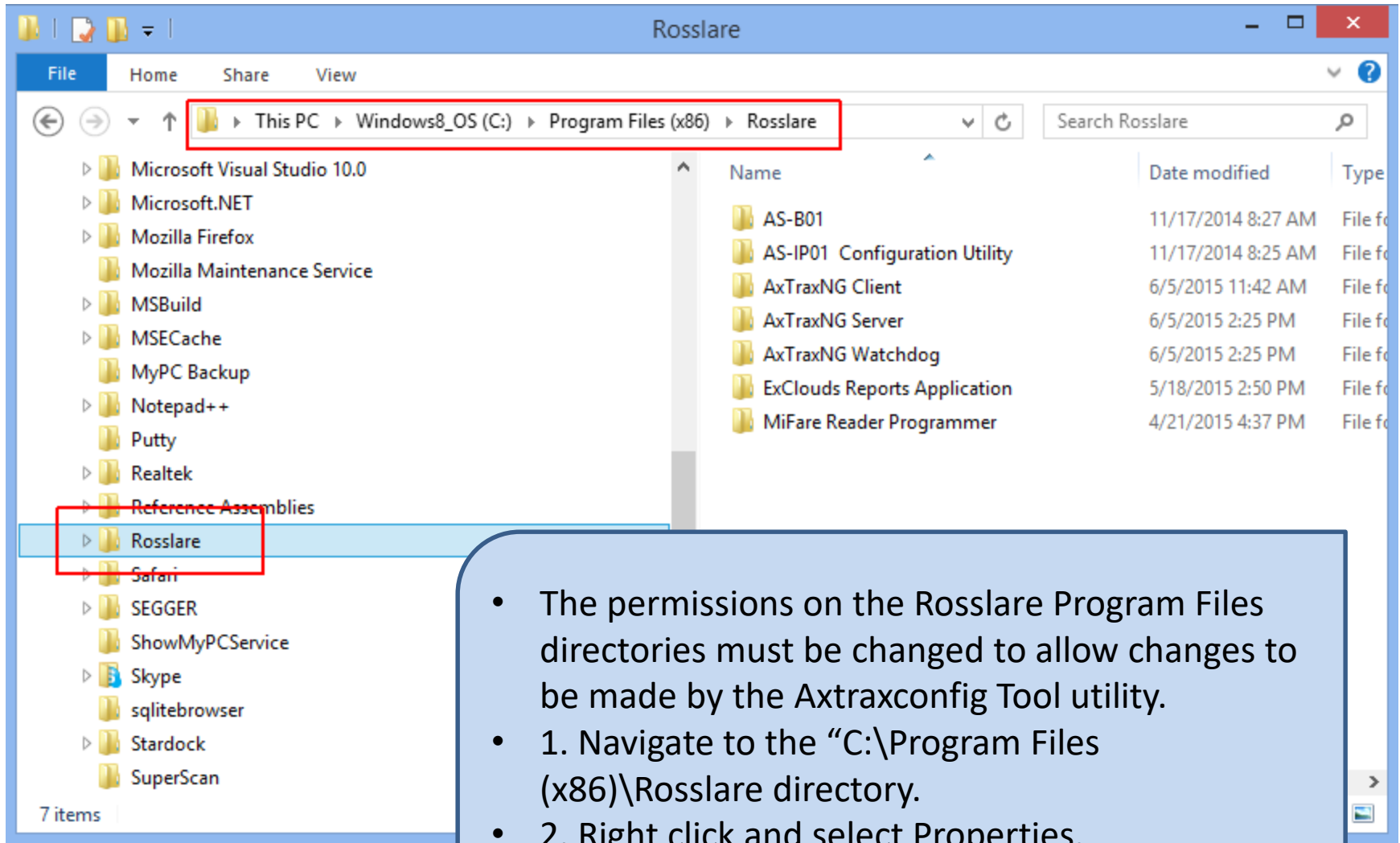
The InstallShield Wizard has successfully installed AxTraxNG Client. Click Finish to exit the wizard.

- Click Finish to continue.

< Back

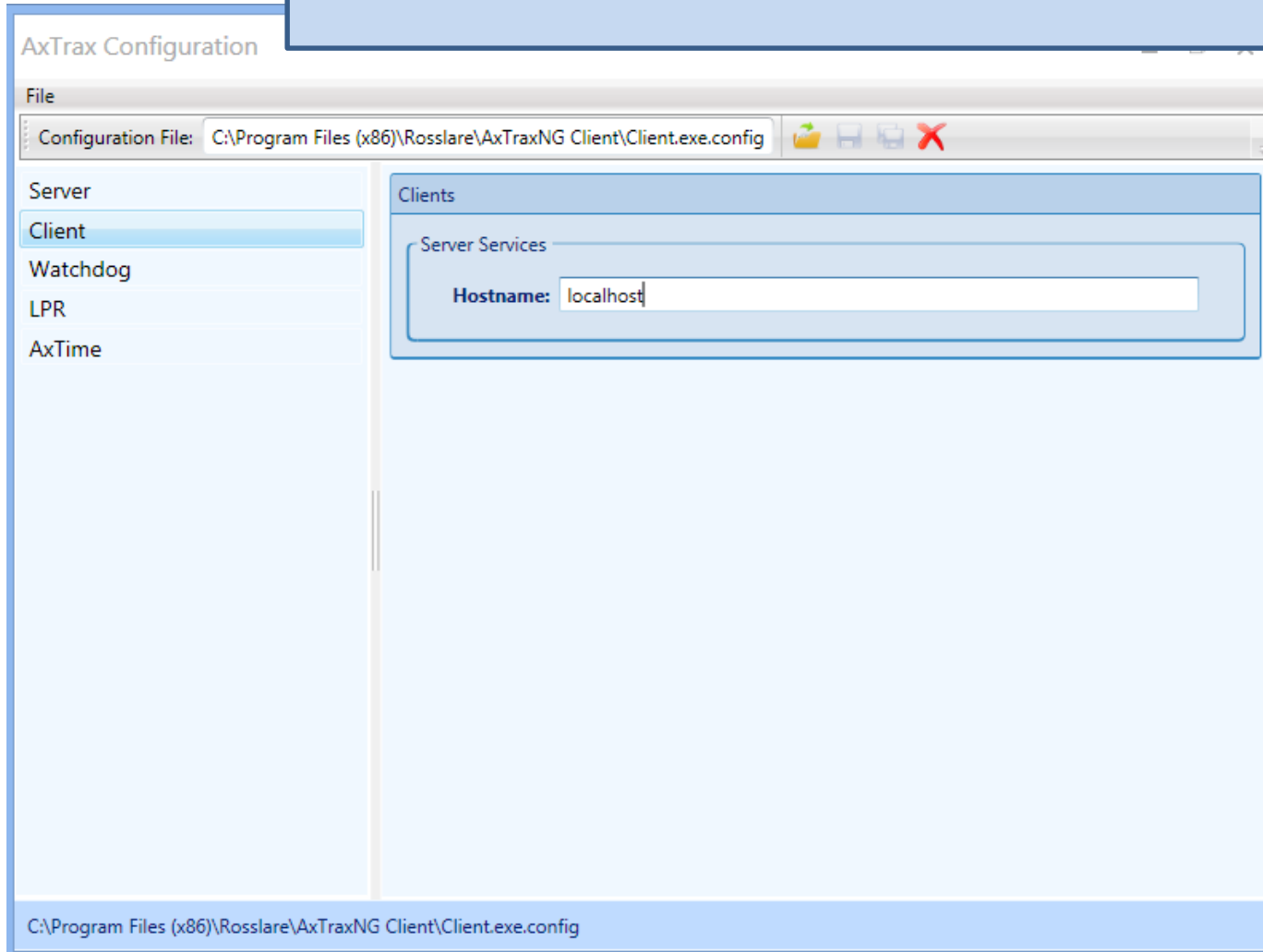
Finish

Cancel



- The permissions on the Rosslare Program Files directories must be changed to allow changes to be made by the Axtraxconfig Tool utility.
- 1. Navigate to the "C:\Program Files (x86)\Rosslare" directory.
- 2. Right click and select Properties.

- Before the Client is run for the first time you must configure the client software. From the windows desktop, go to Start, Programs, Rosslare and start the AxtraxConfigTool utility.



AxTrax Configuration

File

Configuration File: C:\Program Files (x86)\Rosslare\AxTraxNG Client\Client.exe.config

Server

Client

Watchdog

LPR

AxTime

Clients

Server Services

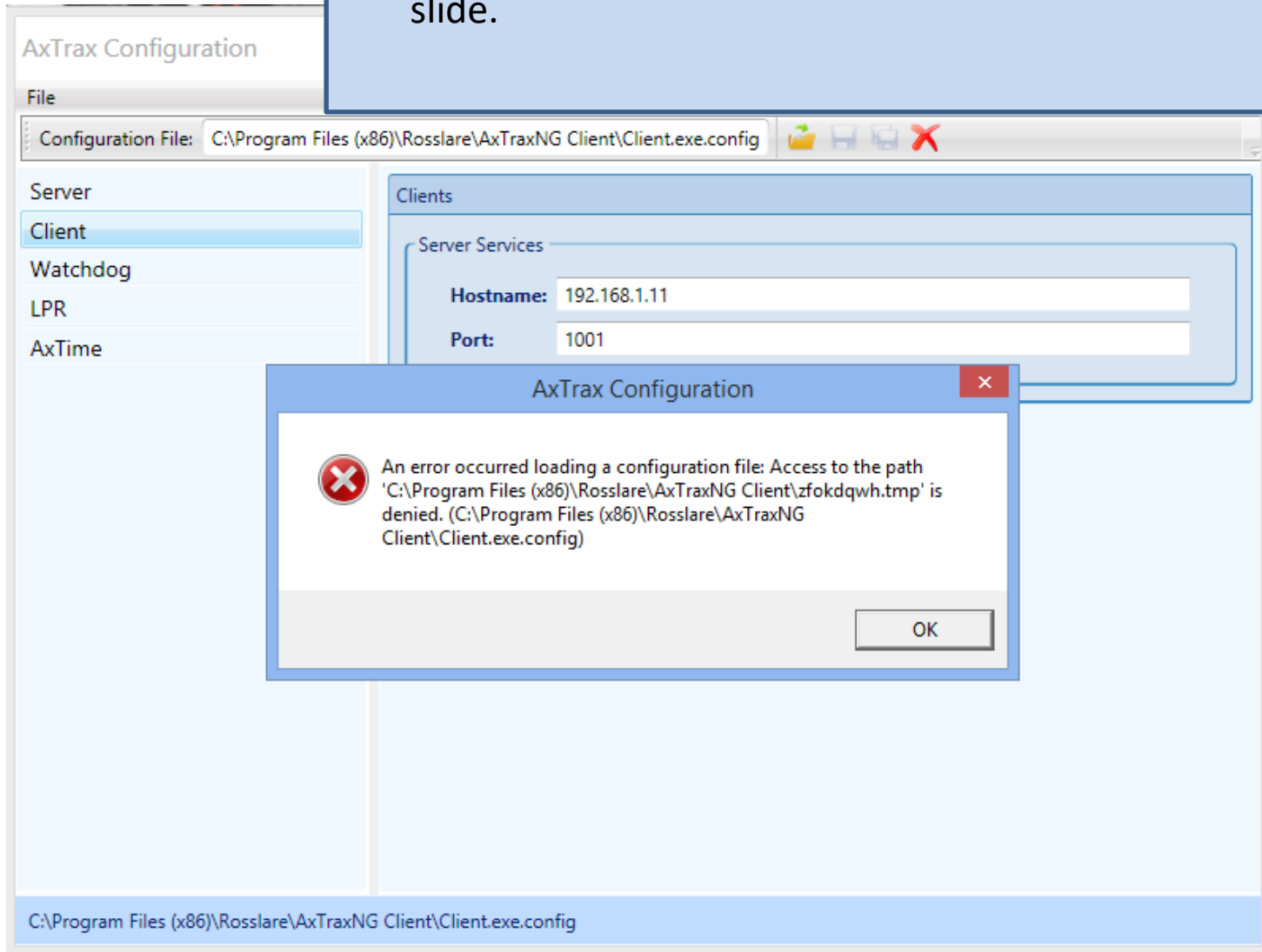
Hostname: 192.168.1.11

Port: 1001

- Enter the IP address of the AxtraxNG server machine. You must also specify the port to use, 1001 is the default.
- If this is being done to a remote server machine (not on the same LAN);
  - then enter the public IP address of the server site
  - insure that port 1001 is forwarded to the server machine at the remote site.
- To save you changes you must click the save icon circled in red.

C:\Program Files (x86)\Rosslare\AxTraxNG Client\Client.exe.config

- If you encounter the following error you must run the configuration tool as administrator as described in the next slide.



- Open the Windows file manager and navigate to the following directory; C:\Program Files (x86)\Rosslare\AxTraxNG Configuration Tool.
- Right click on AxtraxConfigTool.exe and select run as administrator.
- Set the IP address and port as shown in the previous slides and select save.

# Firewall Configuration Windows 7,8 and 10

Configuring the Windows Firewall for  
Remote Client Connection

- The following steps must be performed on the AxtraxNG Server machine, not the remote client machine.
- Open Control Panel
- Select Windows Defender Firewall



Windows Defender Firewall

Control Panel > All Control Panel Items > Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off





Restore defaults

**Advanced settings**


Troubleshoot my network

### Help protect your PC with Windows Defender Firewall

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

 Private networks	Not connected 
 Guest or public networks	Connected 

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	 ROSSLAREUS
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Select Advanced Settings

## Select Inbound Rules

The screenshot displays the Windows Defender Firewall with Advanced Security console. The title bar reads "Windows Defender Firewall with Advanced Security on Local Computer". The left-hand navigation pane shows a tree view with "Inbound Rules" highlighted and enclosed in a red rectangular box. Other items in the tree include "Outbound Rules", "Connection Security Rules", and "Monitoring". The main content area shows an "Overview" section with three profiles: "Domain Profile", "Private Profile", and "Public Profile is Active". Each profile lists the status of the firewall and connection rules. A right-hand "Actions" pane is visible, containing options such as "Import Policy...", "Export Policy...", "Restore Default Policy", "Diagnose / Repair", "View", "Refresh", "Properties", and "Help".

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows.

Overview

**Domain Profile**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

**Private Profile**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

**Public Profile is Active**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

[Windows Defender Firewall Properties](#)

**Actions**

- Import Policy...
- Export Policy...
- Restore Default Policy
- Diagnose / Repair
- View
- Refresh
- Properties
- Help

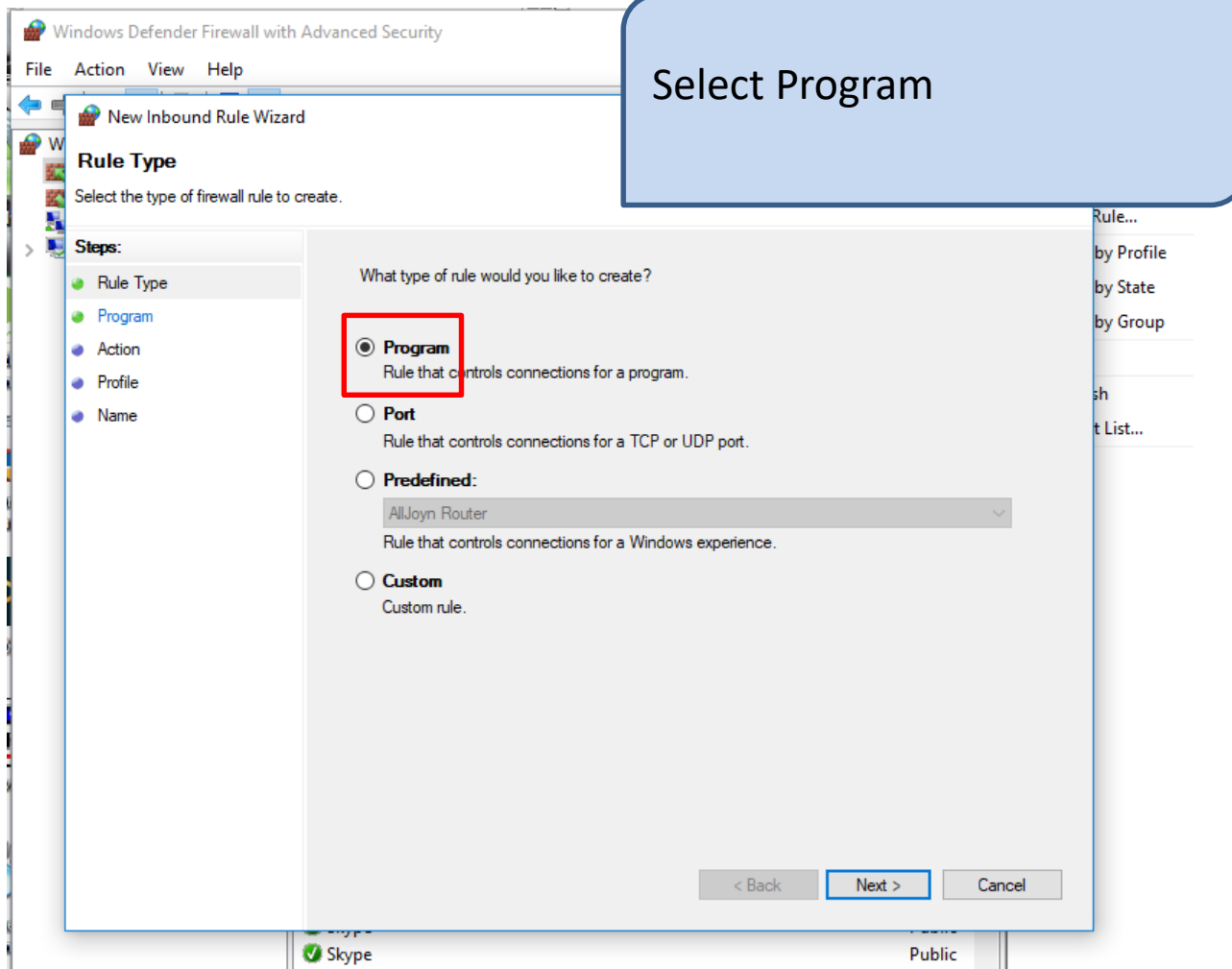
Select New Rule on the Right

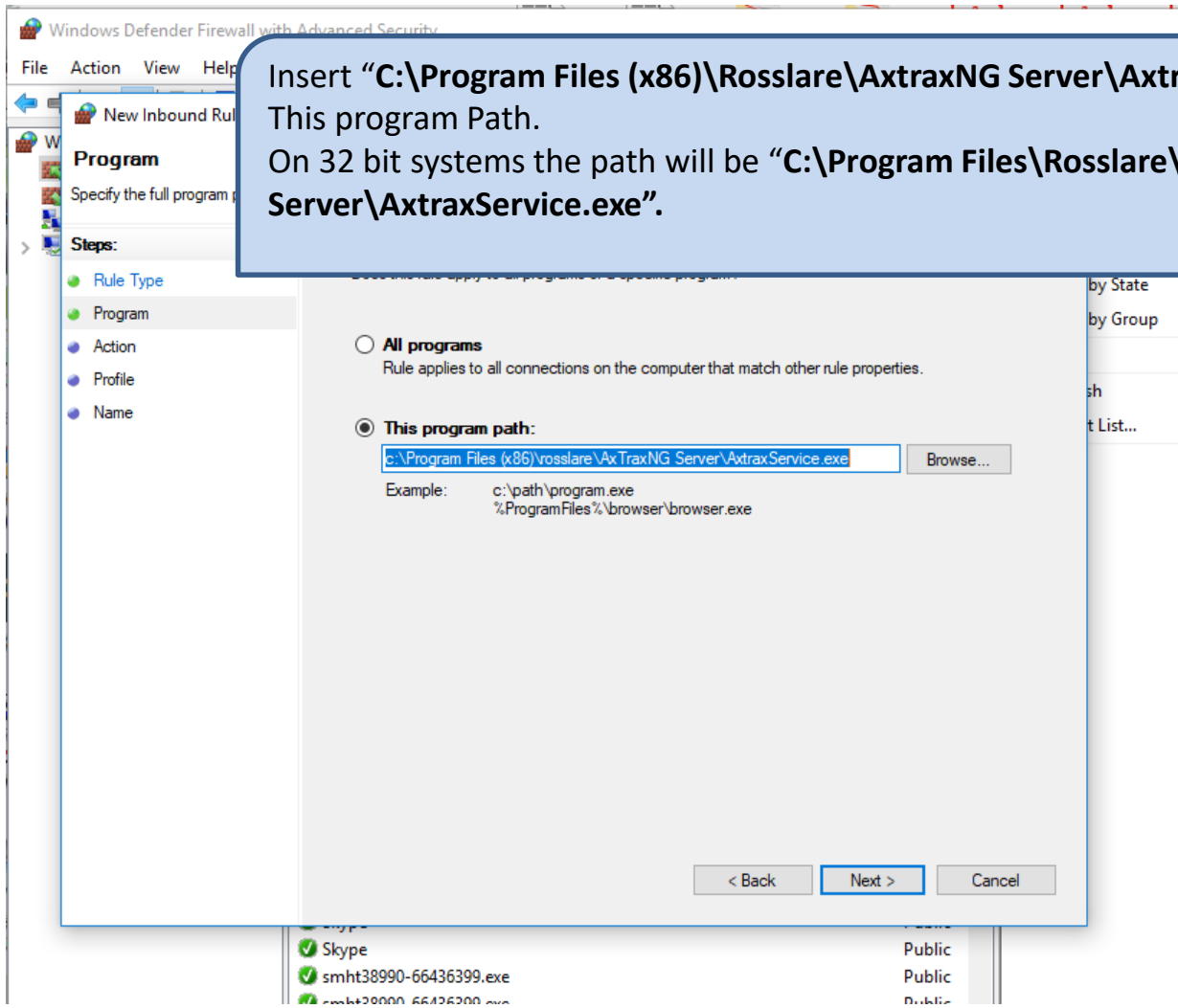
The screenshot shows the Windows Defender Firewall with Advanced Security console. The main pane displays a list of Inbound Rules. The 'Actions' pane on the right is open, and the 'New Rule...' option is highlighted with a red rectangle.

Name	Group	Profile
AS-IP01 Configuration Utility		Public
AS-IP01 Configuration Utility		Public
AxtraxNG Server		All
ivms-4200		Public
ivms-4200		Public
Imi_rescue.exe		Public
Imi_rescue.exe		Public
McAfee Management Service Host (x64)		All
McAfee Management Service Host (x86)		All
Microsoft Office Outlook		Public
nginx		Public
nginx		Public
SADPTool 应用程序		Public
SADPTool 应用程序		Public
ShowMyPCAuto		All
ShowMyPCAuto		All
ShowMyPCAuto		All
ShowMyPCAuto		All

**Actions**

- Inbound Rules**
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help





Insert "C:\Program Files (x86)\Rosslare\AxtraxNG Server\AxtraxService.exe" for This program Path.  
On 32 bit systems the path will be "C:\Program Files\Rosslare\AxtraxNG Server\AxtraxService.exe".

Windows Defender Firewall with Advanced Security

File Action View Help

New Inbound Rule Wizard

**Action**  
Specify the action to be taken when a connection matches the conditions specified

**Steps:**

- Rule Type
- Program
- 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**

< Back   Next >   Cancel

by Profile  
by State  
by Group  
sh  
t List...

Skype	Public
smht38990-66436399.exe	Public
smht38990-66436399.exe	Public
smht47184_41423100.exe	Public

## Select Allow the Connection

### New Inbound Rule Wizard

#### Profile

Specify the profiles for which this rule applies.

##### Steps:

- Rule Type
- Program
- Action
- Profile
- Name

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, such as a home or work place.
- Public**  
Applies when a computer is connected to a public network location.

< Back   Next >   Cancel

Leave all profiles selected

by Profile  
by State  
by Group  
sh  
t List...

Skype  
cmht38990-66436399.exe

Public  
Public

Windows Defender Firewall with Advanced Security

File Action View Help

### New Inbound Rule Wizard

**Name**  
Specify the name and description of this rule.

**Steps:**

- Rule Type
- Program
- Action
- Profile
- Name**

Name:

Description (optional):

< Back Finish Cancel

by Profil  
by State  
by Group  
sh  
t List...

Skype  
smht38990-66436399.exe  
Public  
Public

Enter "axtraxng" for the name then click Finish