



A SUBSIDIARY OF ALBERTA INNOVATES

200 Karl Clark Road | Edmonton | AB | T6N 1H2

ESPBend Installation Guide

**Copyright © 2026
C-FER Technologies**

**January 2026
ESPBEND-PRC-0001-Rev0**

TABLE OF CONTENTS

1. SYSTEM REQUIREMENTS.....	1
2. QUICK START GUIDE	2
2.1 End User Installation and Licence Activation	2
2.2 Licence Protection	2
3. INSTALLING PROGRAM	3
3.1 Program Files	3
3.2 Installing on Individual Computer	3
4. ACTIVATING LOCAL SOFTLOCK.....	8
5. ACTIVATING NETWORK SOFTLOCK	10
5.1 Server Requirements	10
5.2 Installing Network Key Server Manager	10
5.3 Network Key Server Manager Firewall Exceptions	12
5.3.1 Create Program Inbound Rule	12
5.3.2 Create Program Outbound Rule	18
5.3.3 Create Port Inbound Rule	24
5.3.4 Create Port Outbound Rule	30
5.4 Activating End User Licence	36
6. ACTIVATING C-FER SOFTLOCK	39
7. USER SUPPORT	41

1. SYSTEM REQUIREMENTS

To successfully run **ESPBend**, your system must have the following features or higher:

- Operating System: Windows 10/11 or Windows Server 2016/2019/2022
- Processor: Dual-core Processor
- RAM: 4 GB
- Storage: 60 GB (additional space must be available after installation for saving your working files)
- Display: Monitor supported by Microsoft Windows at a resolution of at least 1024x768
- Internet Access: (required) for software installation and operation

2. QUICK START GUIDE

2.1 End User Installation and Licence Activation

The following steps provide a brief overview of the installation process; please see the relevant section of this guide for more detailed instructions:

1. Run the file installer.
2. Review the Software Licence Agreement, and if you agree to the terms and conditions, select the confirmation checkbox.
3. Confirm the installation location.
4. Launch the program.
5. Activate your licence based on the licence type:

Local Softlock: Go to **Key Management > Registration**. Enter the Activation Code provided by C-FER. Select **Activate**.

Network Softlock: Go to **Key Management > Network**. Enter the Network Server address provided by your company IT service. Select **Connect**.

C-FER Softlock: Go to **Key Management > Network**. Enter the Network Server address provided by C-FER. Select **Connect**.

2.2 Licence Protection

ESPBend licences are copy-protected through the use of software-based ("Softlock") protection systems. All installations of **ESPBend** require a functioning internet connection to validate the user-key against C-FER's licencing server when the software is launched, and periodically during the program's execution. This measure prevents unlicensed use of **ESPBend**.

3. INSTALLING PROGRAM

3.1 Program Files

ESPBend is located in the **C:\Program Files (x86)\C-FER Technologies\ESPBend** folder. Installing newer versions **ESPBend** will remove any links to older versions that exist in the Windows Start menu. Any desktop shortcuts need to be updated to link to the new **ESPBend** software location in the program files directory.

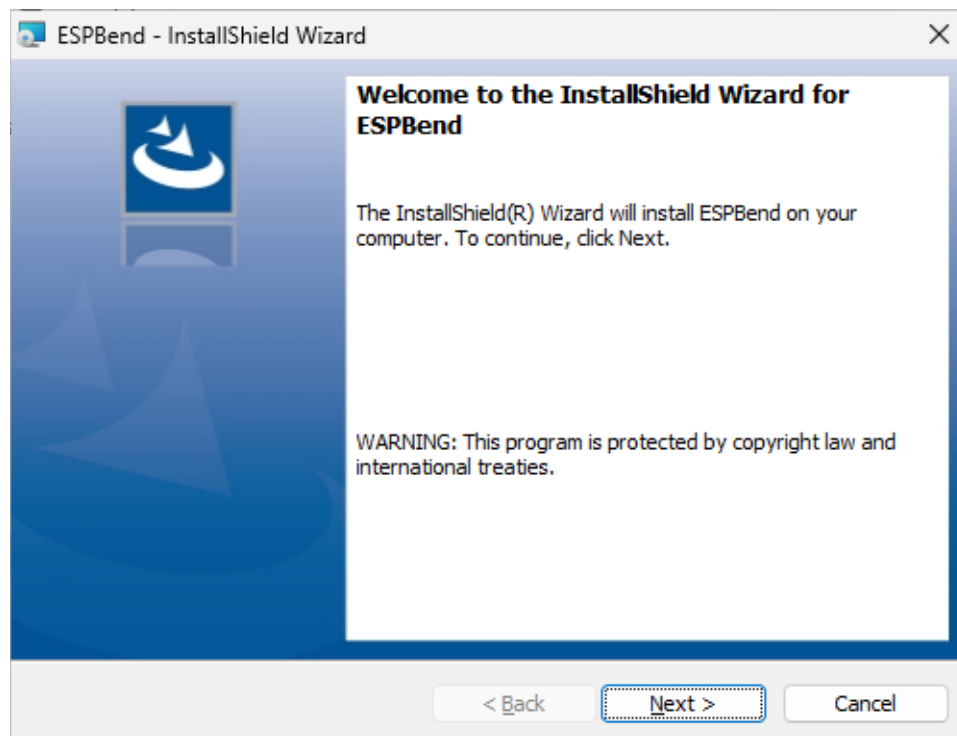
The latest version of **ESPBend** may be downloaded from <https://www.cfertech.com/espbend/user-area/>.

3.2 Installing on Individual Computer

To install **ESPBend** on your computer:

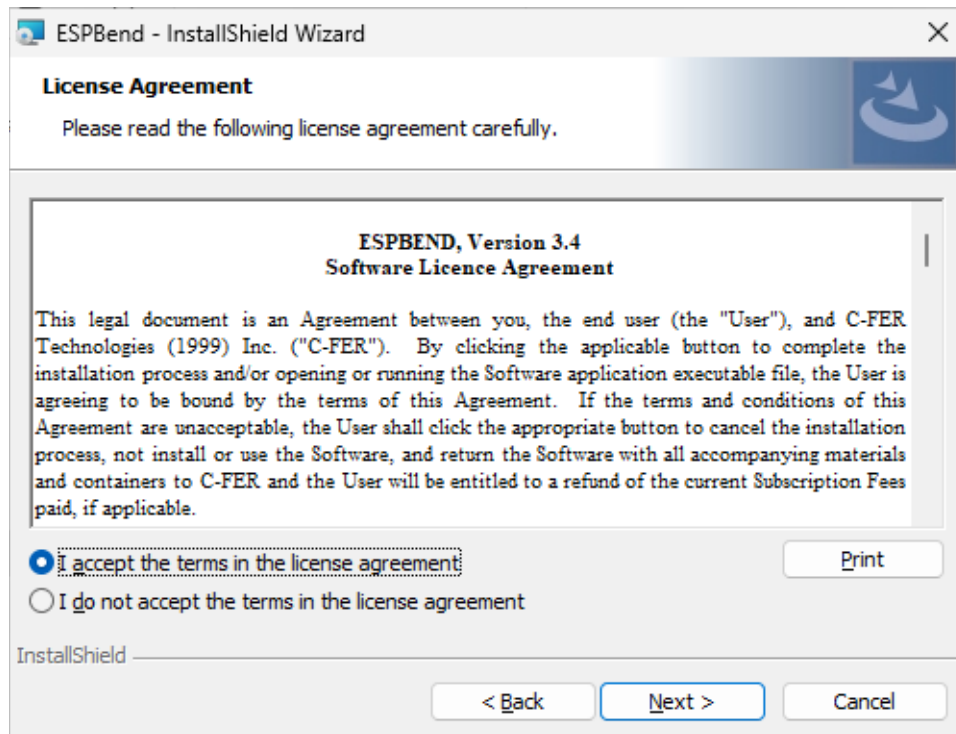
1. Log in with administrator privileges.
2. Close other major applications that are running on Microsoft Windows.
3. Double-click the program icon to start the installation process.
4. Select **Next**.

Installing Program



5. Review the **ESPBend** Licence Agreement:

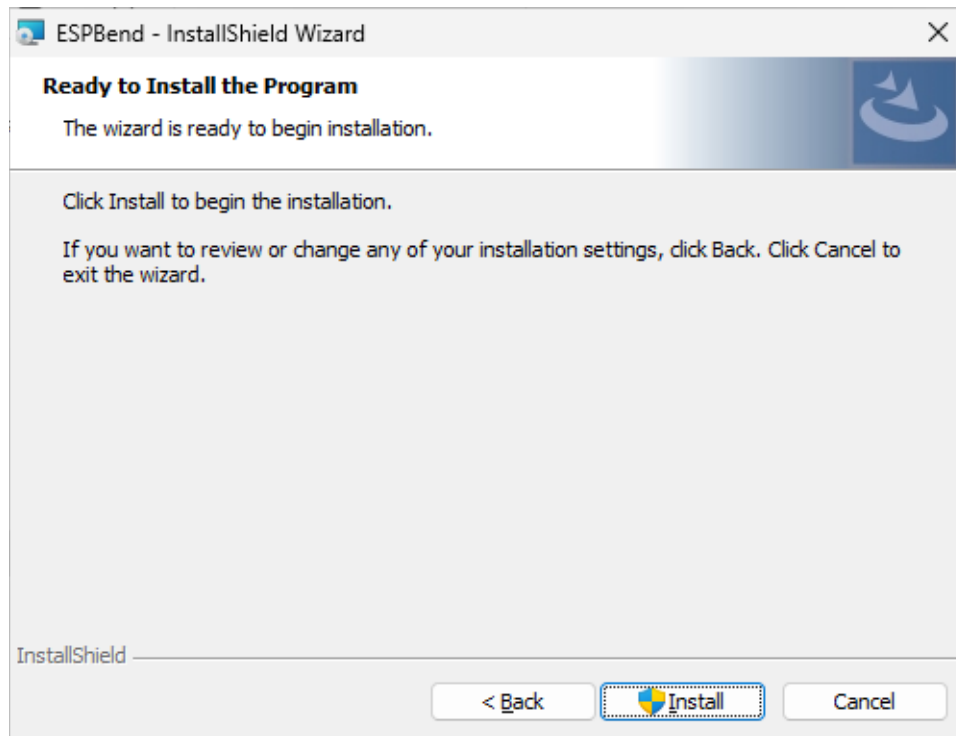
Installing Program



Select **I accept the terms...** and then **Next** if you agree to the terms and conditions.

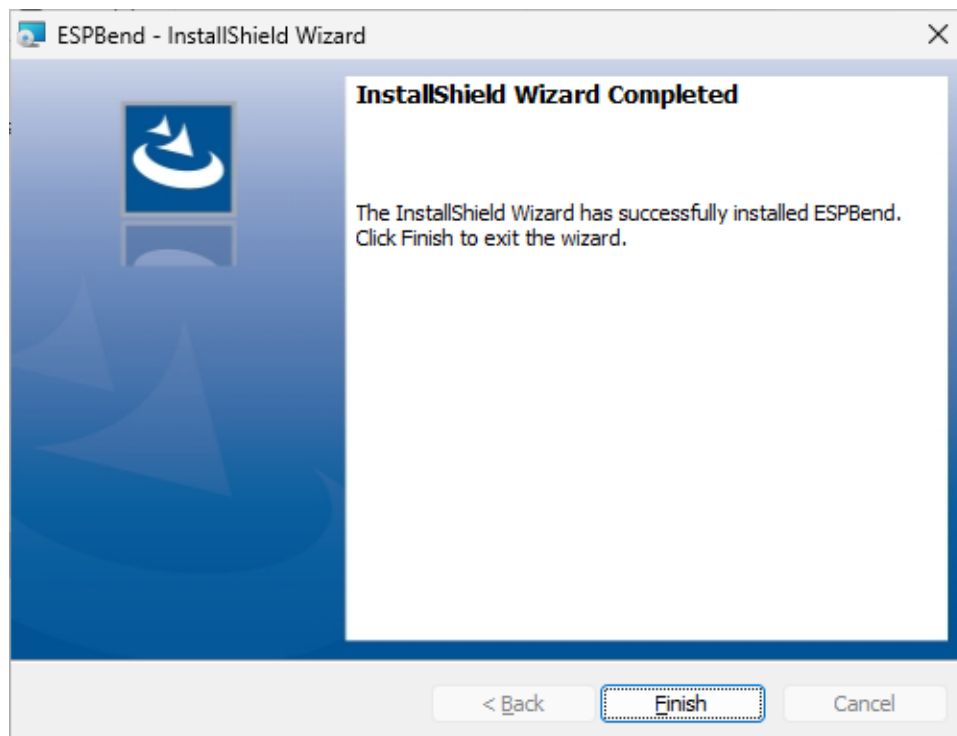
6. Select **Install** to begin installing the program:

Installing Program



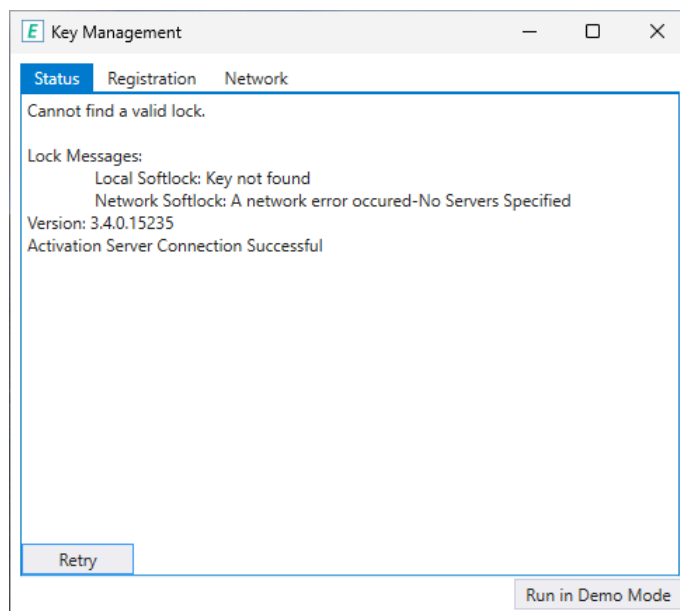
7. When the ESPBend installation is complete, select **Finish** to exit the installation program.

Installing Program

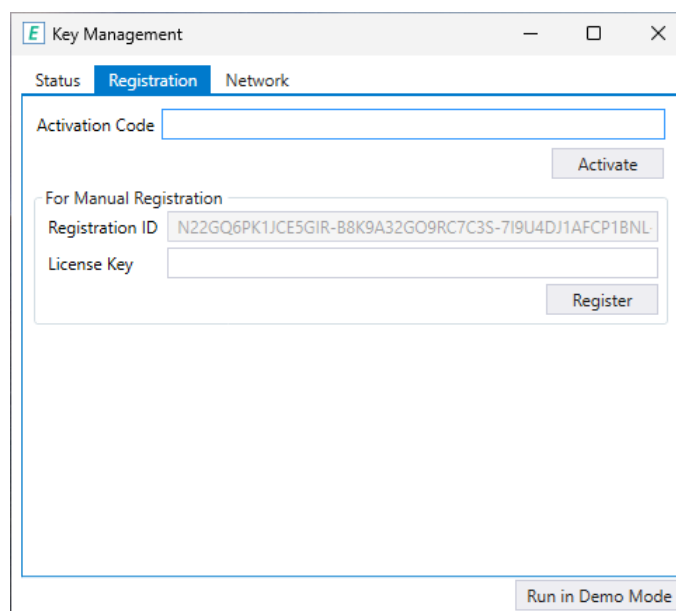


4. ACTIVATING LOCAL SOFTLOCK

1. Install **ESPbend** per the instructions provided in Section 3.2.
2. Launch **ESPbend**. The **Key Management** window will appear and indicate that the Softlock key was not found.



3. Go to the **Registration** tab.



Activating Local Softlock

4. In the **Activation Code** field, enter the activation code provided by C-FER and select **Activate** to register the Softlock key.
5. Go to the **Status** tab.
6. Select **Refresh**. The licence information for the Softlock key will be displayed.

5. ACTIVATING NETWORK SOFTLOCK

5.1 Server Requirements

To successfully run the **Network Key Server Manager**, your server must have the following features or higher:

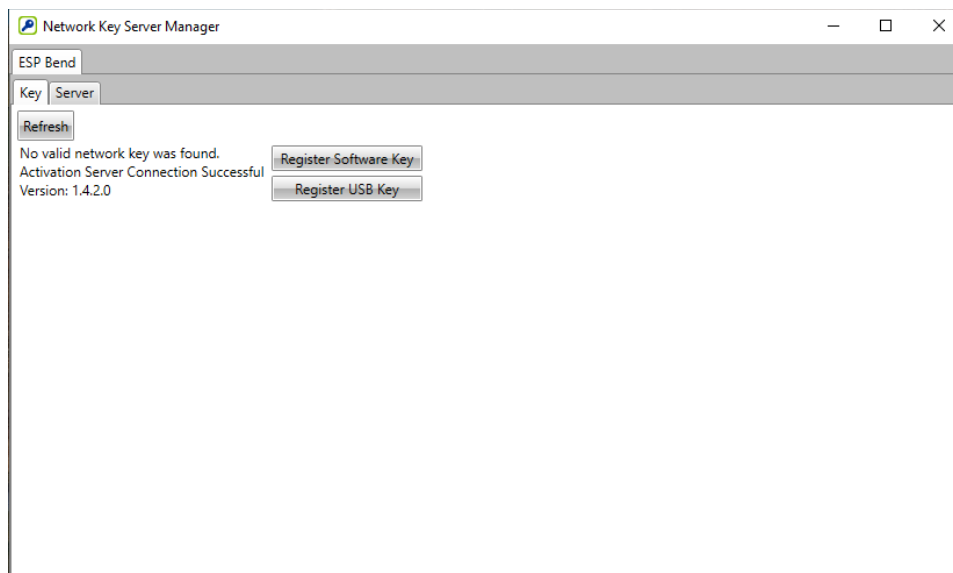
- Operating System: Windows 10/11 or Windows Server 2016/2019/2022
- Processor: Dual-core processor
- RAM: 2 GB
- Storage: 60 GB

5.2 Installing Network Key Server Manager

To use a Network Softlock, your IT team will need to install the **Network Key Server Manager** program on the **licence server**. This can be downloaded from <https://download.cfertech.com/shared/NetworkKeyServerManager.exe>. The **Network Key Server Manager** can be installed on either a physical or virtual server.

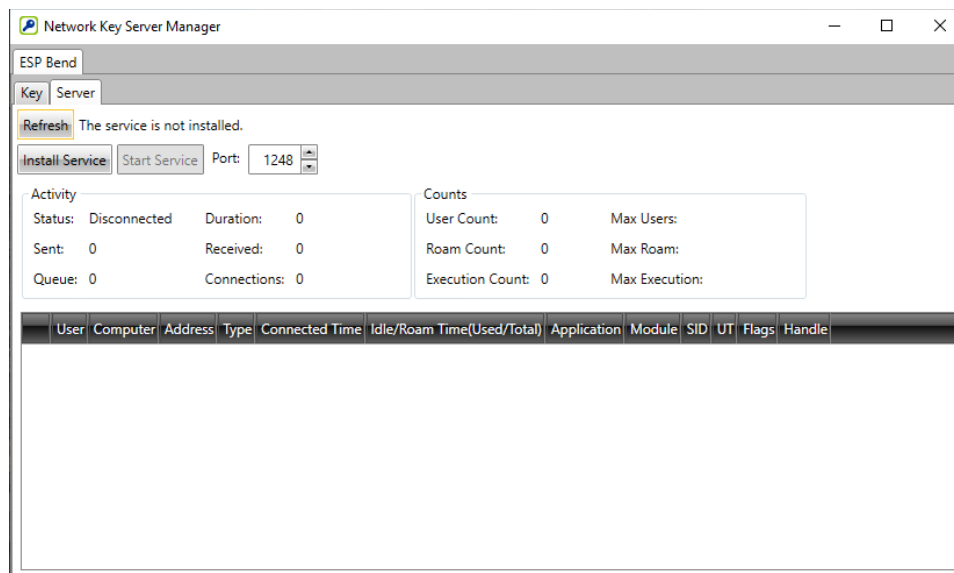
1. Install the **Network Key Server Manager** locally to the licence server.
2. Launch the **Network Key Server Manager** from the Windows Start menu and select **ESPBend**.
3. Go to the **Key** tab to verify the status of the Softlock key. If the key is correctly running, its activation status will be displayed. Otherwise, the Softlock key will need to be activated.

Activating Network Softlock



4. To activate the Softlock key:
 - a) Select Register Software Key to open the Software Key Registration dialog box.
 - b) Enter the alpha-numeric key provided by C-FER into the Activation Code field.
 - c) Select Activate. If the Softlock key activation is successful, the dialog box will close, and the key status will automatically update.
5. Go to the **Server** tab.
6. Select **Install Service** to install the Softlock Windows service on the licence server.
7. Select **Start Service** to start the Softlock Windows service.

Activating Network Softlock



5.3 Network Key Server Manager Firewall Exceptions

If you are experiencing issues activating or connecting to your Network Softlock licence, exceptions may need to be added to the network or server firewall, depending on its configuration relative to the licence server. The following instructions are for creating Firewall exceptions in Windows Defender and should only be used if Windows Defender is the firewall system that is active on the licence server; these instructions may be adapted for your company-specific firewall product.

To launch Windows Defender:

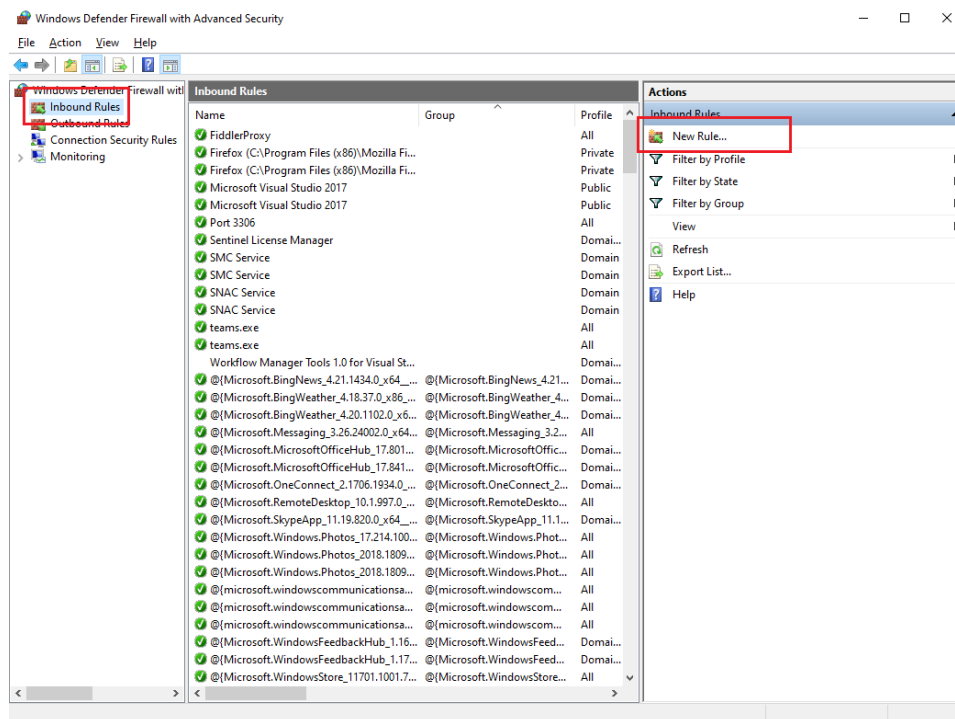
1. Go to **Start > Control Panel > Administrative Tools**.
2. Select **Windows Defender Firewall with Advanced Security**.

5.3.1 Create Program Inbound Rule

To create a program inbound rule:

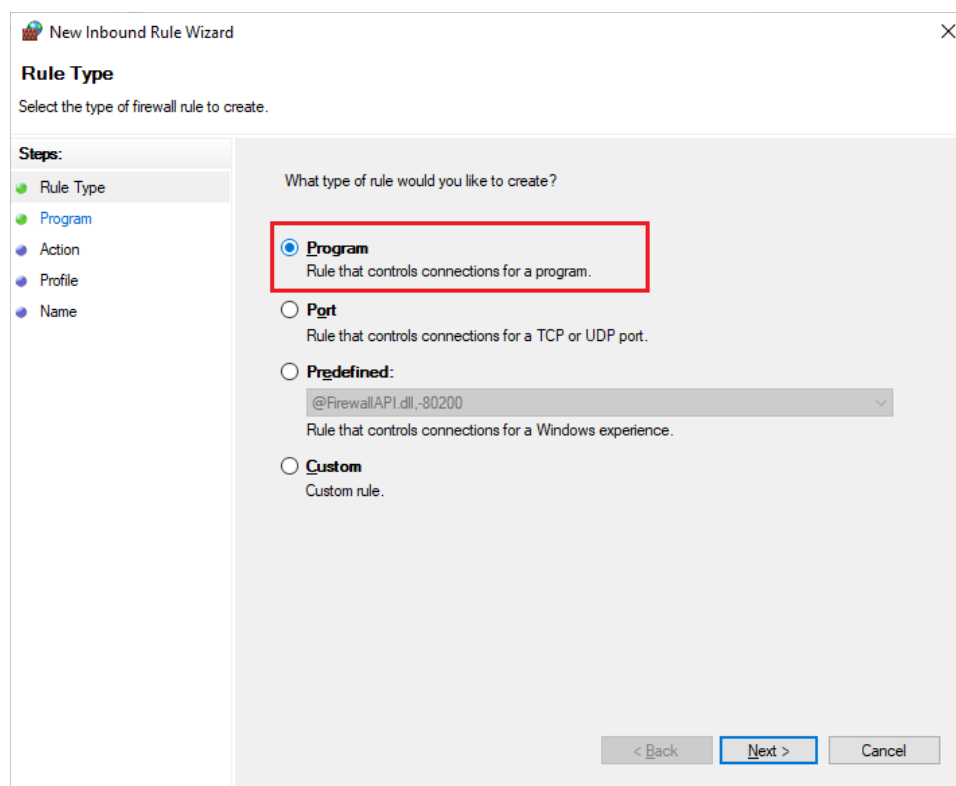
1. Select **Inbound Rules** and then **New Rule**.

Activating Network Softlock



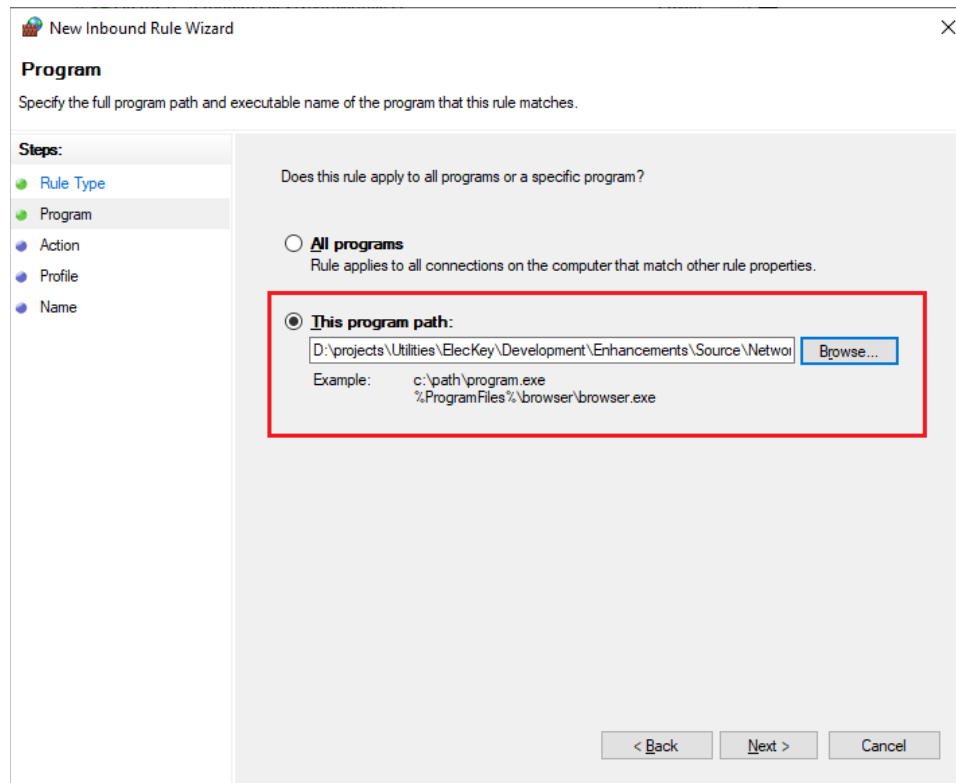
2. Select **Program** and then **Next**.

Activating Network Softlock



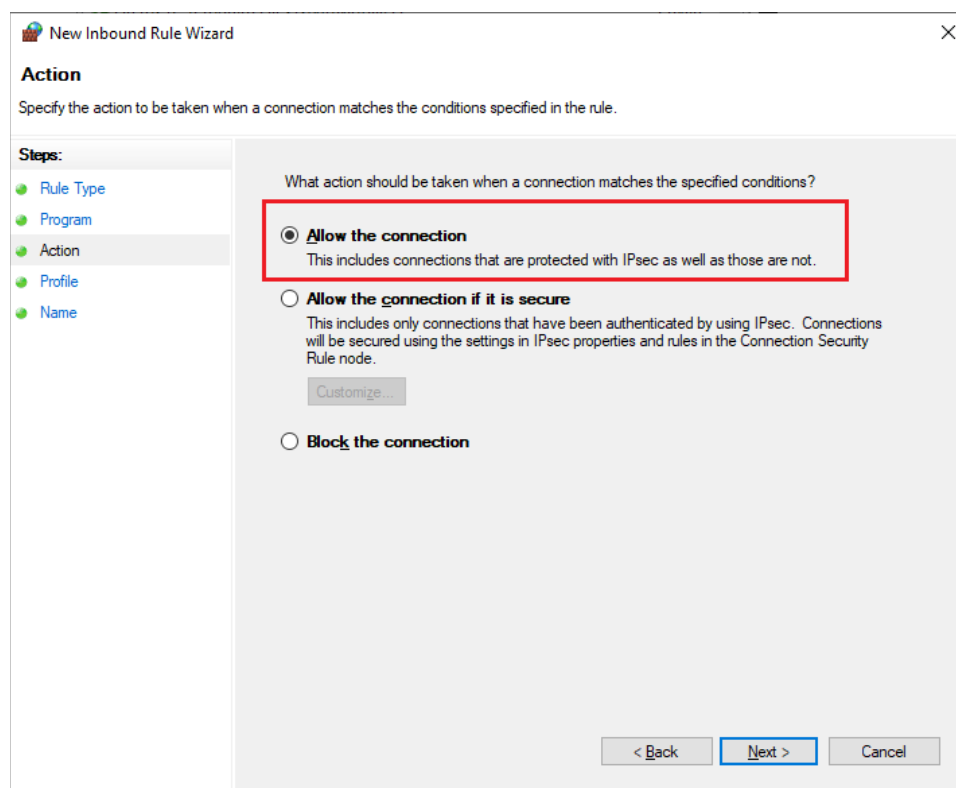
3. Select **This program path** and then **Browse**.

Activating Network Softlock



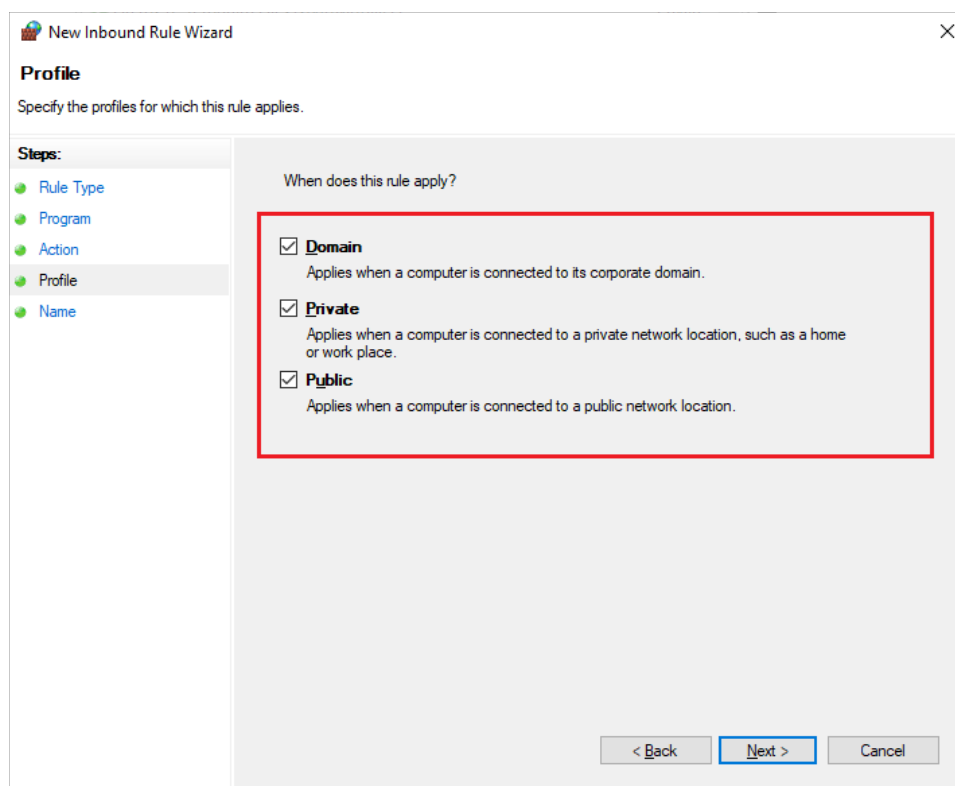
4. Select **C:\Program Files (x86)\C-FER Technologies\NetworkKeyServerManager\NetworkKeyServerManager.exe** and then **Next**.
5. Select **Allow the connection** and then **Next**.

Activating Network Softlock



6. Select all three items and then **Next**. Note that some of these options could be removed, depending on the network configuration.

Activating Network Softlock



7. Enter a rule name in the **Name** field and select **Finish**.

Activating Network Softlock

New Inbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

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

Name:
Network Key Server Manager - inbound

Description (optional):

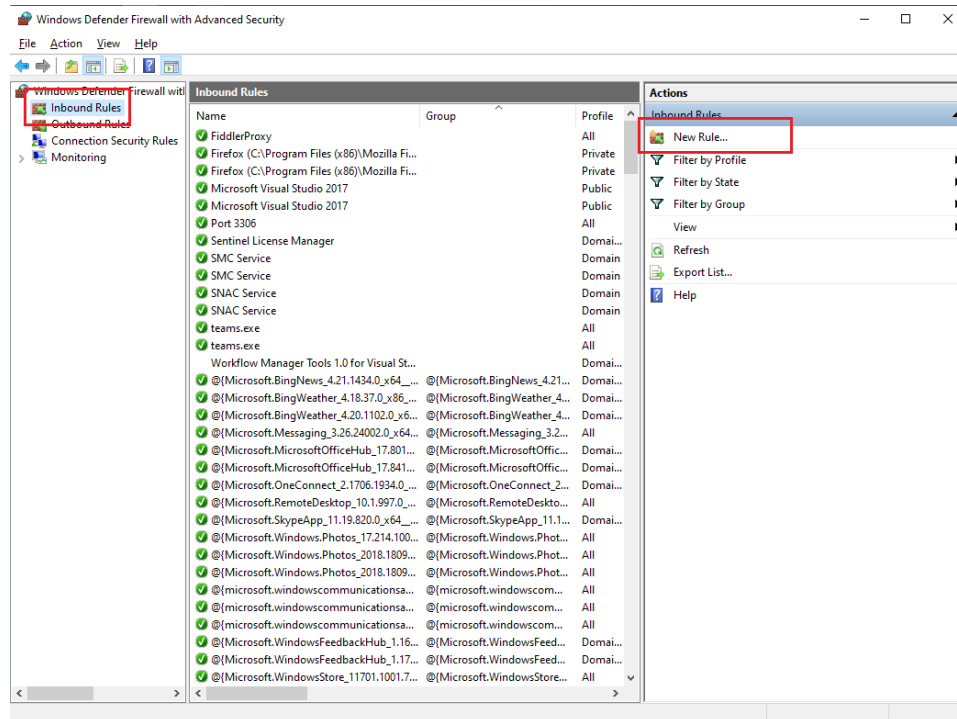
< Back Finish Cancel

5.3.2 Create Program Outbound Rule

To create a program outbound rule:

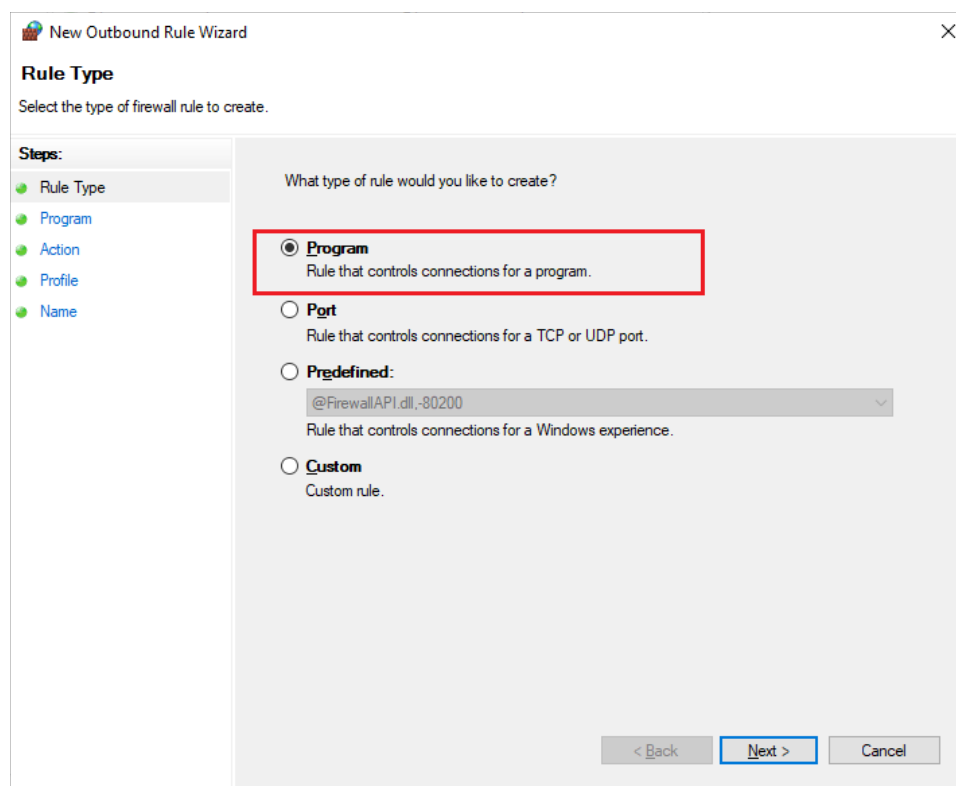
1. Select **Outbound Rules** and then **New Rule**.

Activating Network Softlock



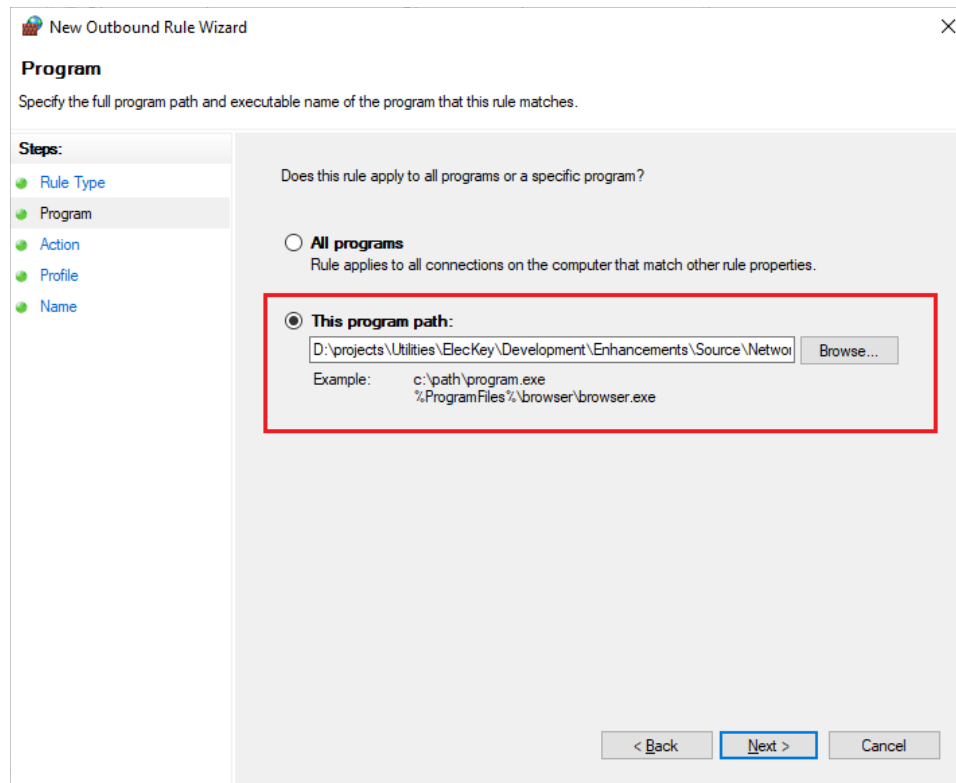
2. Select **Program** and then **Next**.

Activating Network Softlock



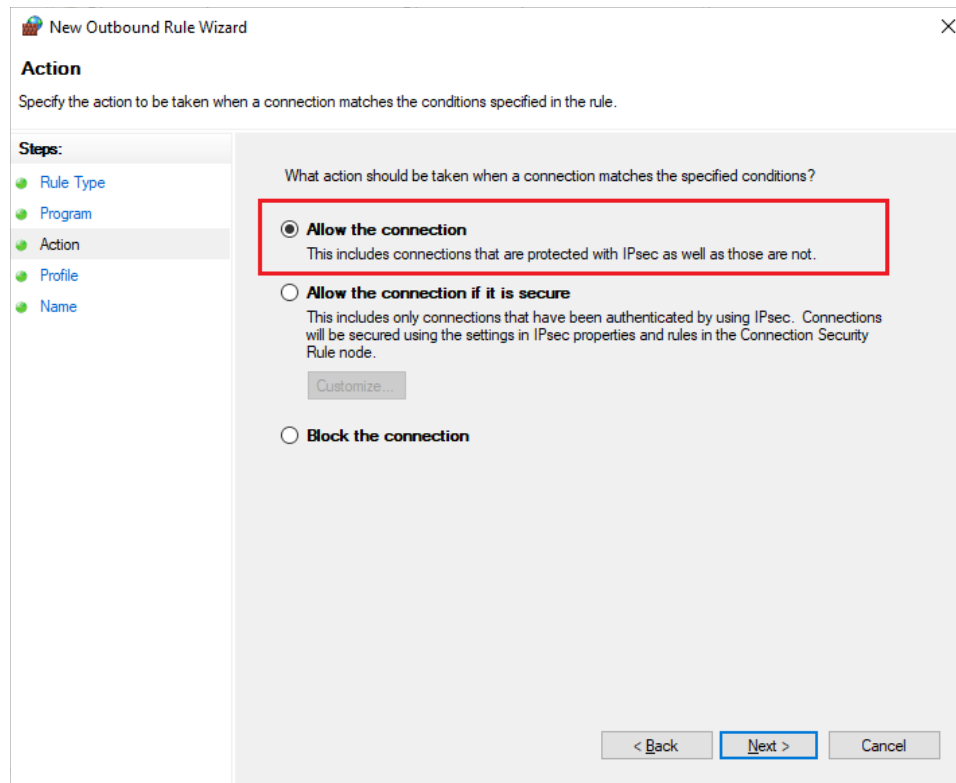
3. Select **This program path** and then **Browse**.

Activating Network Softlock



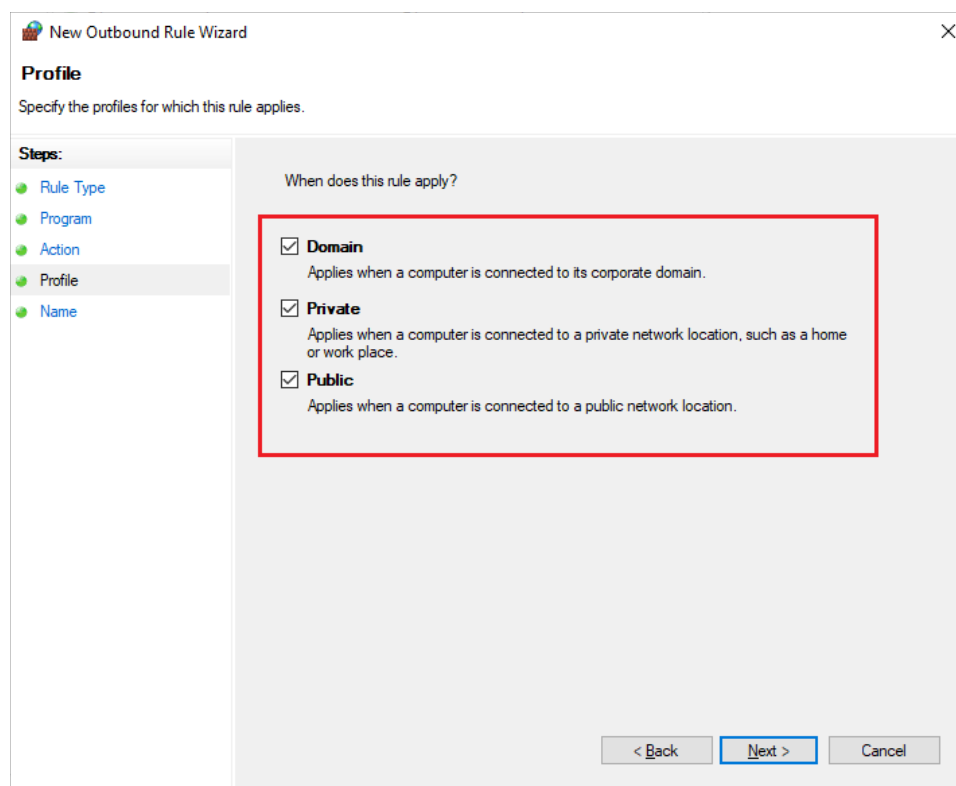
4. Select **C:\Program Files (x86)\C-FER Technologies\NetworkKeyServerManager\NetworkKeyServerManager.exe** and then **Next**.
5. Select **Allow the connection** and then **Next**.

Activating Network Softlock



6. Select all three items and then **Next**. Note that some of these options could be removed, depending on the network configuration.

Activating Network Softlock



7. Enter a rule name in the **Name** field and select **Finish**.

Activating Network Softlock

New Outbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

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

Name:
Network Key Server Manager - outbound

Description (optional):

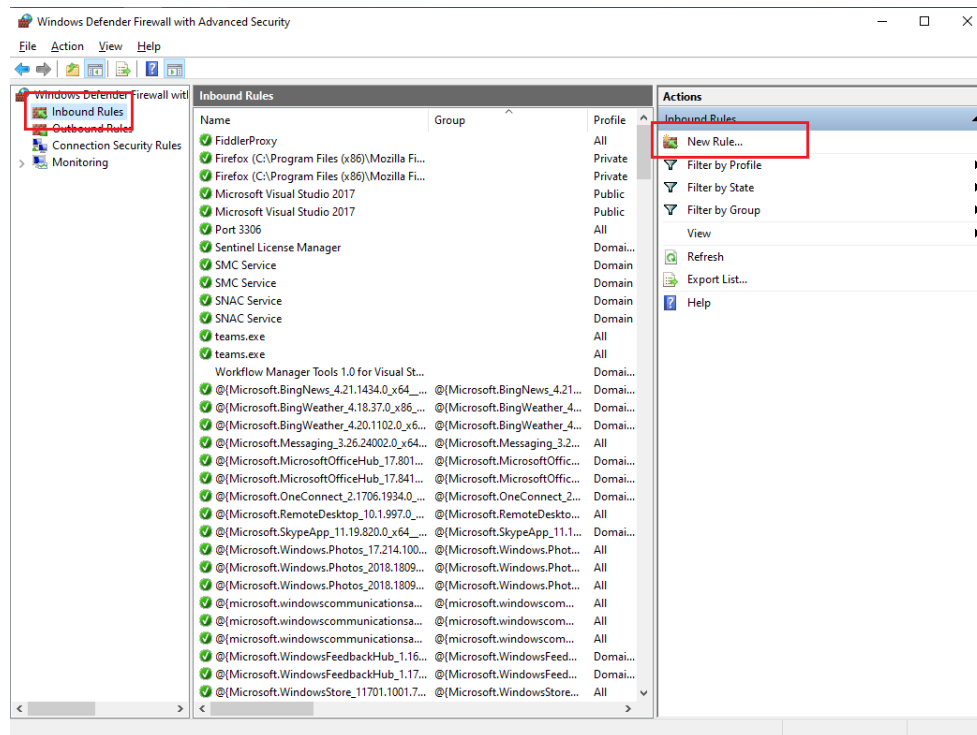
< Back Finish Cancel

5.3.3 Create Port Inbound Rule

To create a port inbound rule:

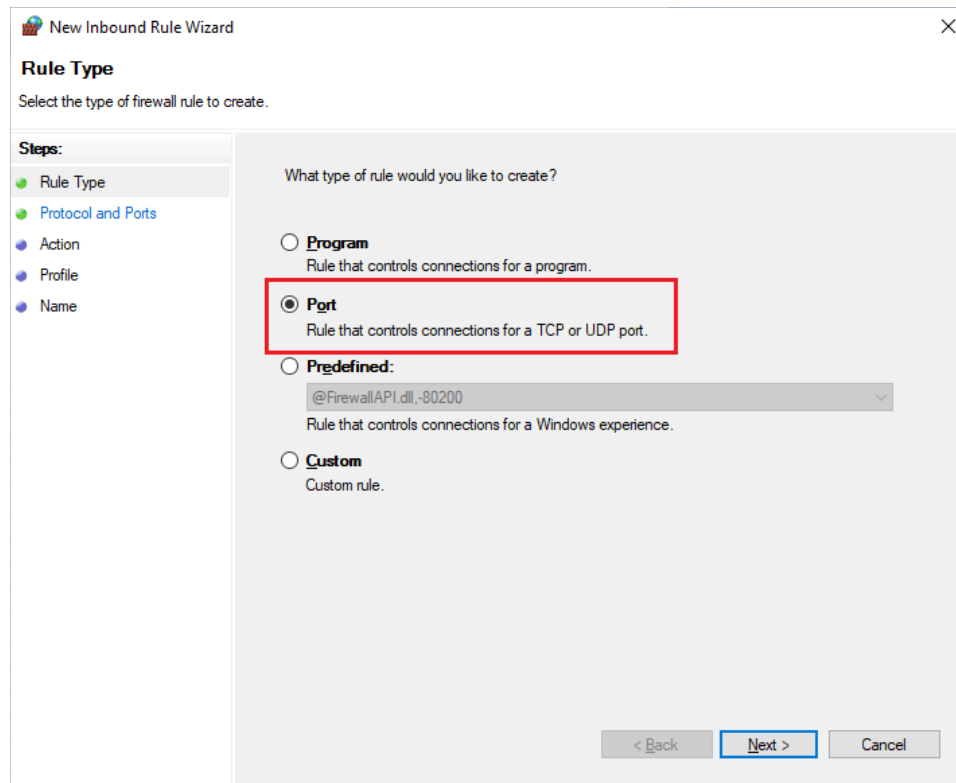
1. Select **Inbound Rules** and then **New Rule**.

Activating Network Softlock



2. Select **Port** and then **Next**.

Activating Network Softlock



3. Enter the port number from the **Network Key Server Manager's Server** tab (the default is 1248) in the **Specific local ports** field and select **Next**.

Activating Network Softlock

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The 'Steps' pane on the left lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions. The first, 'Does this rule apply to TCP or UDP?', has 'TCP' selected. The second, 'Does this rule apply to all local ports or specific local ports?', has 'Specific local ports:' selected. A red rectangle highlights the 'Specific local ports:' section, which includes a text box containing '1248' and an example 'Example: 80, 443, 5000-5010'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound 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 local ports or specific local ports?

☐ All local ports

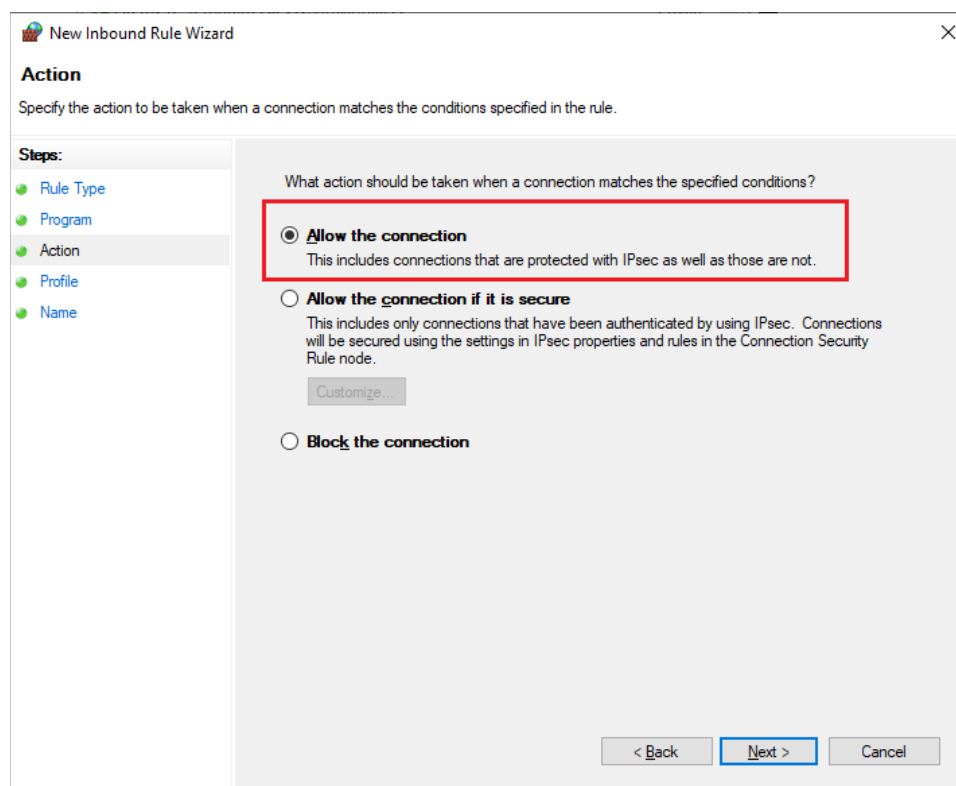
☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

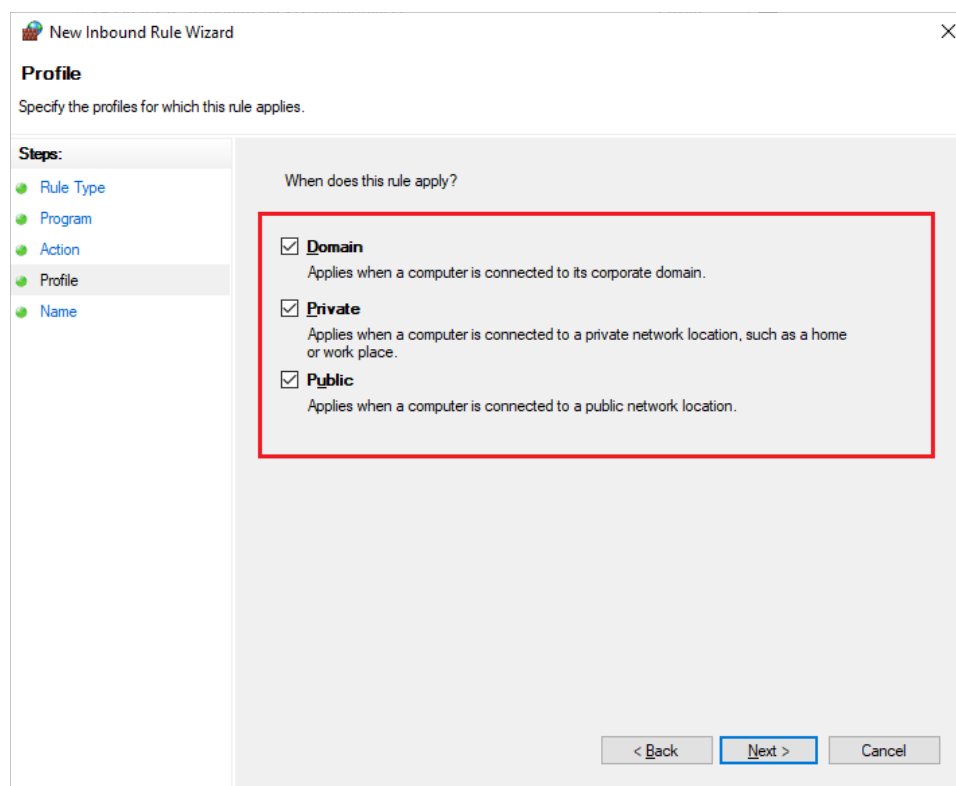
4. Select **Allow the connection** and then **Next**.

Activating Network Softlock



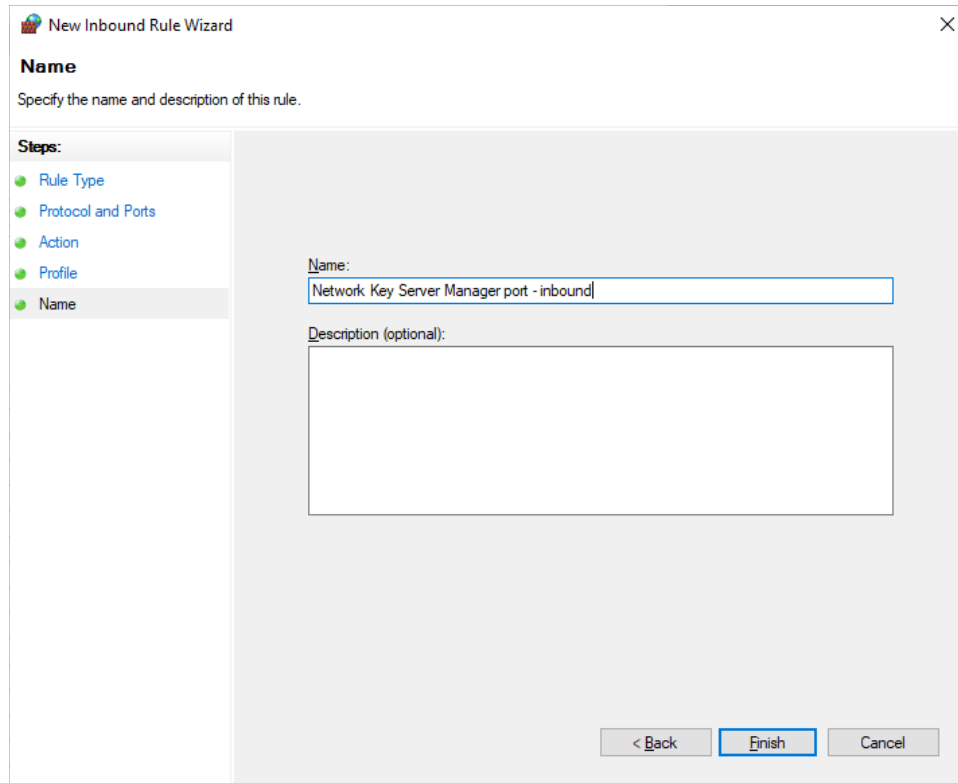
5. Select all three items and then **Next**. Note that some of these options could be removed, depending on the network configuration.

Activating Network Softlock



6. Enter a rule name into the **Name** field and select **Finish**.

Activating Network Softlock



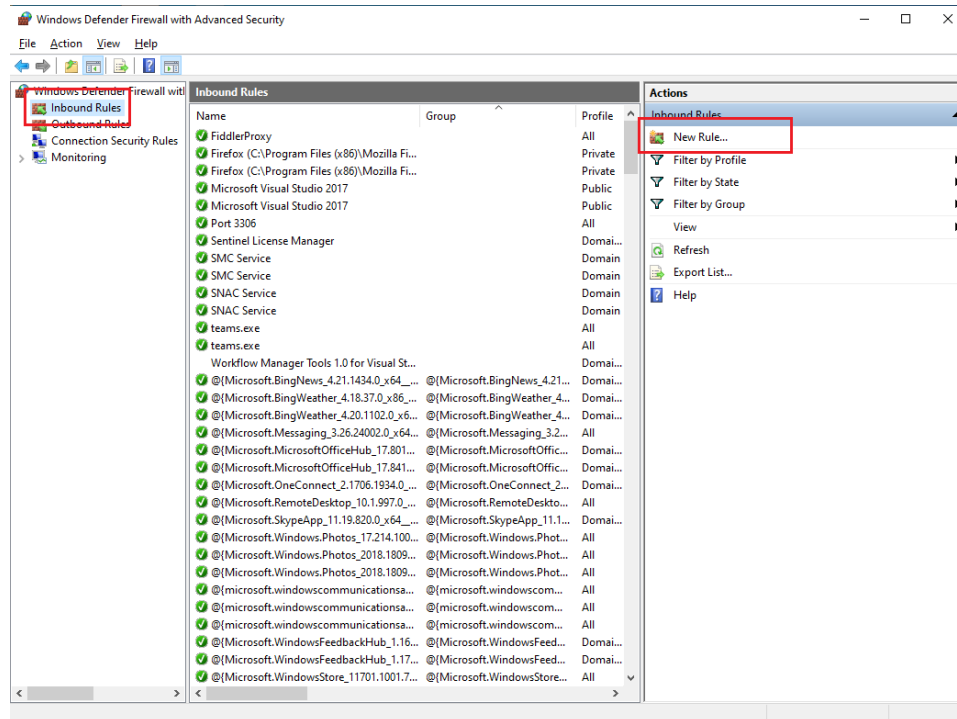
The image shows a 'New Inbound Rule Wizard' dialog box. It has a title bar with a close button (X). Below the title bar, the word 'Name' is followed by the instruction 'Specify the name and description of this rule.' On the left side, there is a 'Steps:' section with a list of steps: 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Name' step is currently selected and highlighted. The main area of the dialog contains a 'Name:' label followed by a text input field containing the text 'Network Key Server Manager port - inbound'. Below this is a 'Description (optional):' label followed by a larger, empty text area. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a blue border.

5.3.4 Create Port Outbound Rule

To create a port outbound rule:

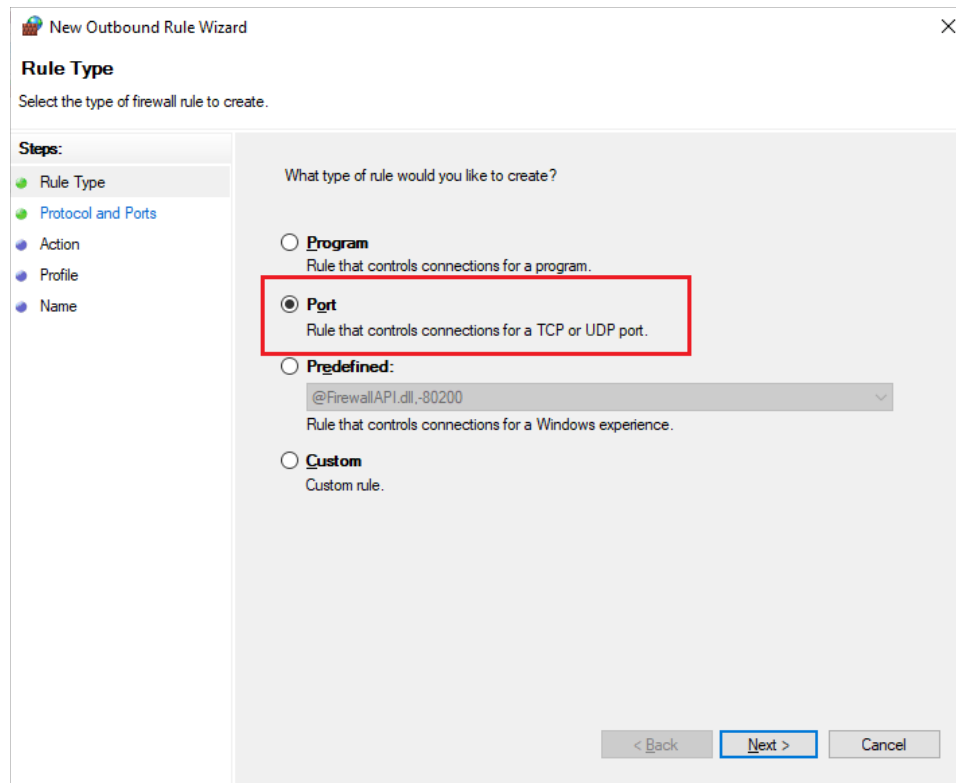
1. Select **Outbound Rules** and then **New Rule**.

Activating Network Softlock



2. Select **Port** and then **Next**.

Activating Network Softlock



3. Enter the port number from the **Network Key Server Manager's Server** tab (the default is 1248) into the **Specific local ports** field and select **Next**.

Activating Network Softlock

The screenshot shows the 'New Outbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The 'Steps' pane on the left lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions. The first question, 'Does this rule apply to TCP or UDP?', has 'TCP' selected with a radio button. The second question, 'Does this rule apply to all remote ports or specific remote ports?', has 'Specific remote ports:' selected with a radio button. A red rectangle highlights the 'Specific remote ports:' section, which includes a text input field containing '1248' and an example text 'Example: 80, 443, 5000-5010'. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

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

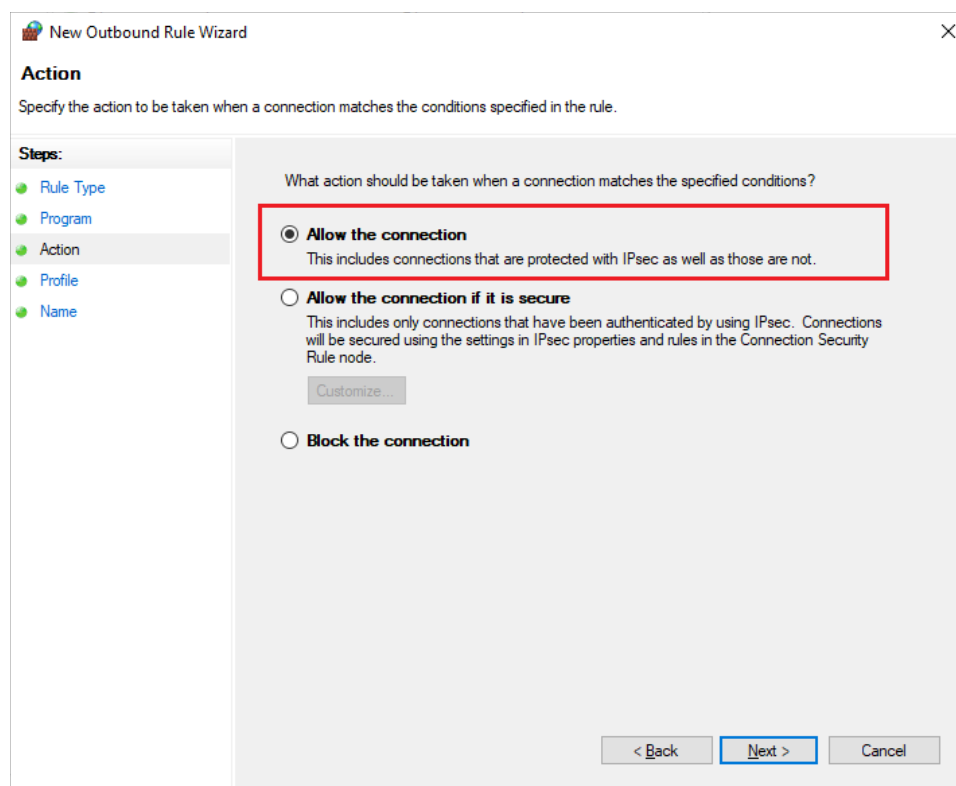
Does this rule apply to all remote ports or specific remote ports?

☐ All remote ports
☒ Specific remote ports: 1248
Example: 80, 443, 5000-5010

< Back Next > Cancel

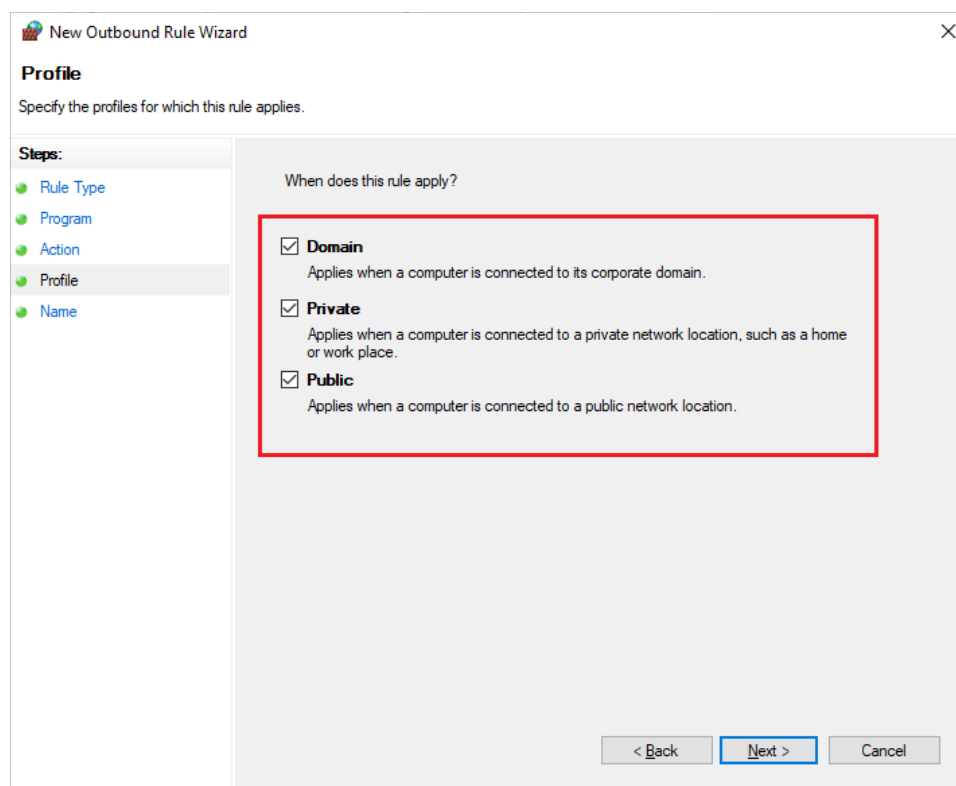
4. Select **Allow the connection** and then **Next**.

Activating Network Softlock



5. Select all three items and then **Next**. Note that some of these options could be removed, depending on the network configuration.

Activating Network Softlock



6. Enter a rule name in the **Name** field and select **Finish**.

Activating Network Softlock

New Outbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:
Network Key Server Manager port - outbound

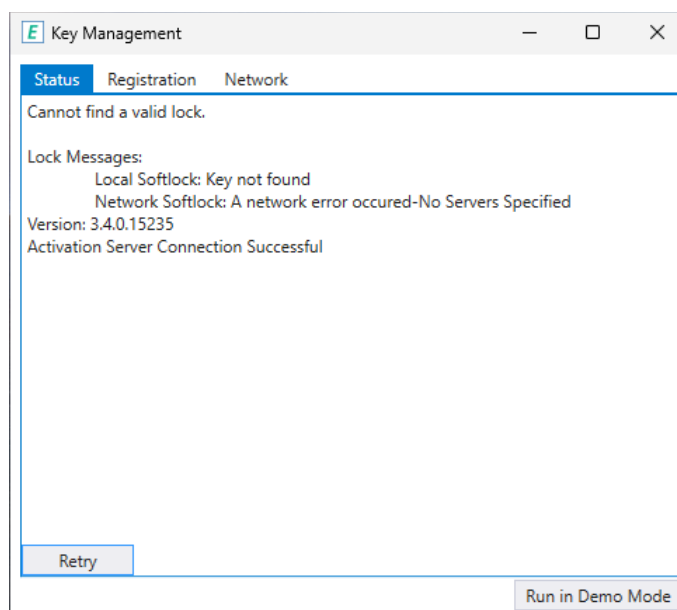
Description (optional):

< Back Finish Cancel

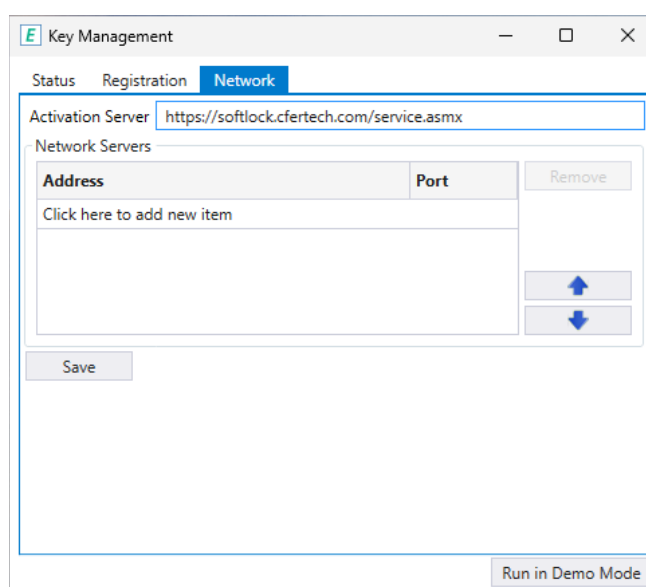
5.4 Activating End User Licence

1. Install **ESPBend** per the instructions in Section 3.2.
2. Launch **ESPBend**. The **Key Management** window will appear and indicate that the Network Softlock was not found.

Activating Network Softlock



3. Go to the **Network** tab.



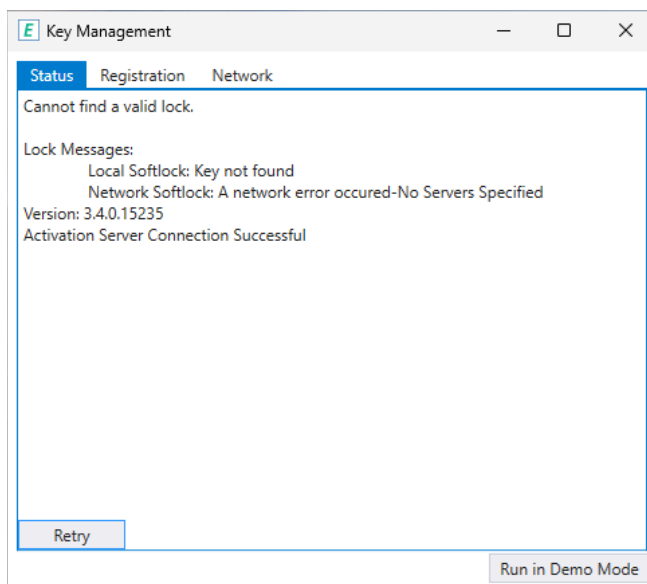
4. In the **Network Servers** area, enter the IP address or server name of the licence server provided by your IT team, and the Port where the Softlock key has been activated (Port 1248 is the default) – This Port must be open. The Network Server Address is the location where the Network Key Server Manager has been installed. Select **Save**.
5. Go to the **Status** tab.

Activating Network Softlock

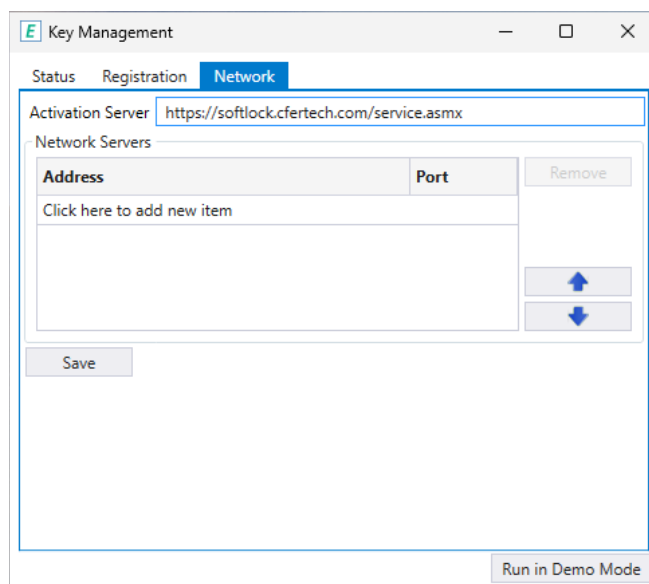
6. Select **Retry**. The licence information for the Softlock key will be displayed.

6. ACTIVATING C-FER SOFTLOCK

1. Install **ESPbend** per the instructions in Section 3.2.
2. Launch **ESPbend**. The **Key Management** window will appear and indicate that the Network Softlock was not located.



3. Go to the **Network** tab.



Activating C-FER Softlock

4. In the **Network Servers** area, enter the IP address or server name of the licence server provided by your IT team, and the Port where the Softlock key has been activated (Port 1248 is the default) – This Port must be open. The Network Server Address is the location where the Network Key Server Manager has been installed. Select **Save**.
5. Go to the **Status** tab.
6. Select **Retry**. The licence information for the Softlock key will be displayed.

7. USER SUPPORT

If you have any questions about **ESPBend**, upgrading, or installing, please contact C-FER by phone at (780) 450-3300 or by email at espblend@cfertech.com.