

APLUS NETWORK KEYLOCK

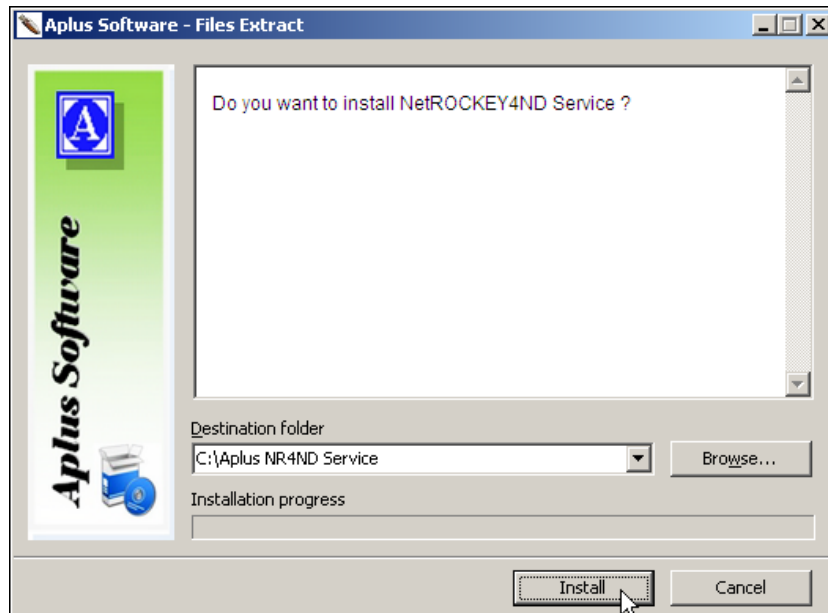
INSTALLATION GUIDE

(For Window 7 and above)

Aplus NetROCKEY4ND Installation



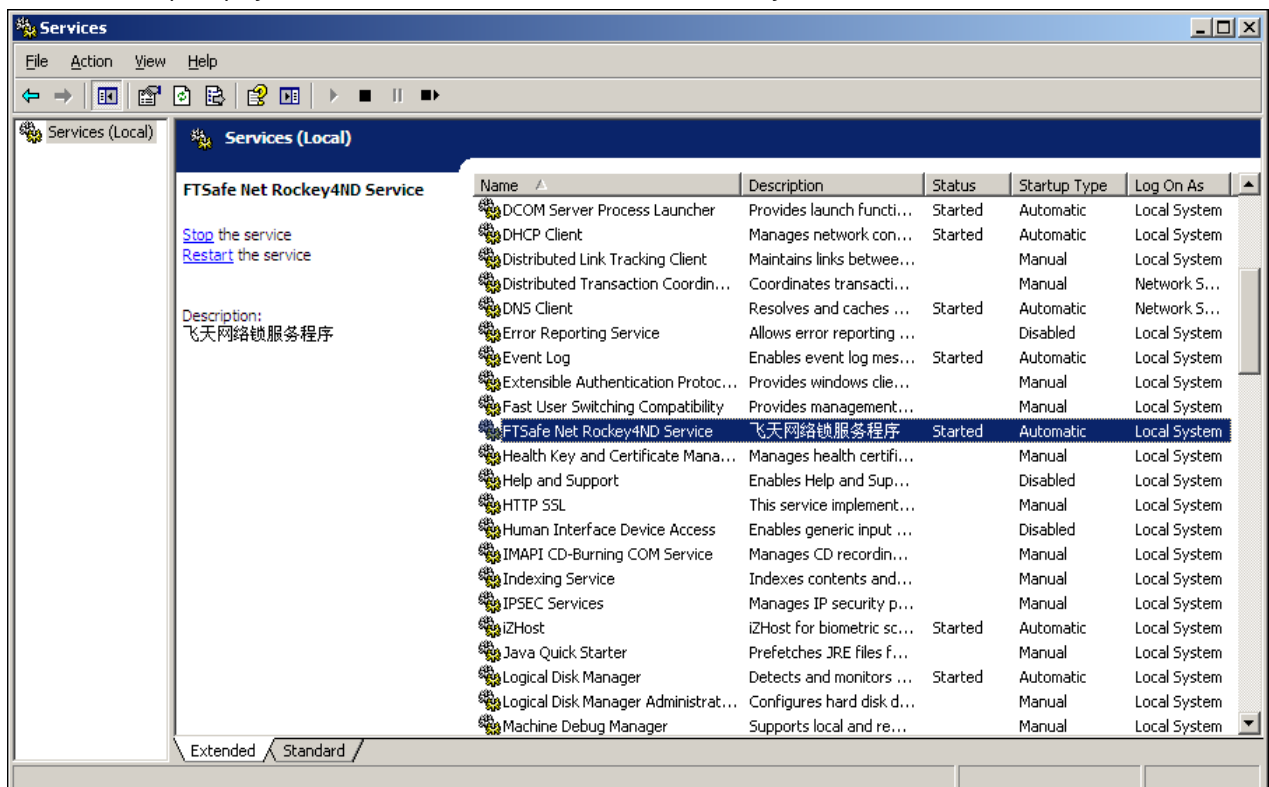
1. **Connect** NetRockey4ND keylock into computer USB port.
2. Please **wait** for Windows detect and complete installing driver automatic itself.
3. Run NetRockey4ND Service setup. Click **Install** button to start install.
4. Installation **completed**.



Remark :

After installation completed, NetROCKEY4ND Service (FTSafe Net Rockey4ND Service) will auto run us services on your windows startup. (Start > Setting > Administrative Tools > Services)

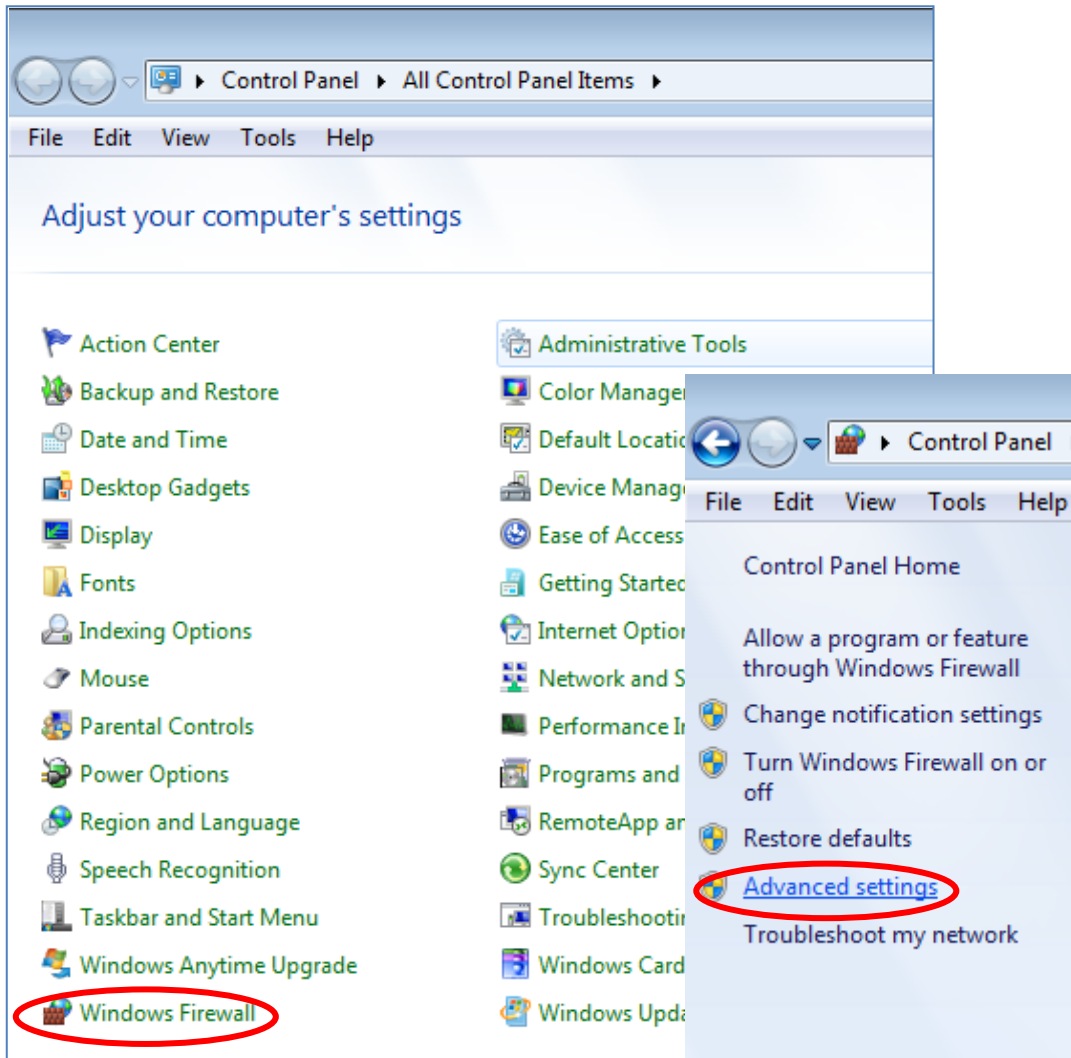
* You can Start/Stop/Display/Re-Install/Remove NetROCKEY4ND Service on your Start Menu.



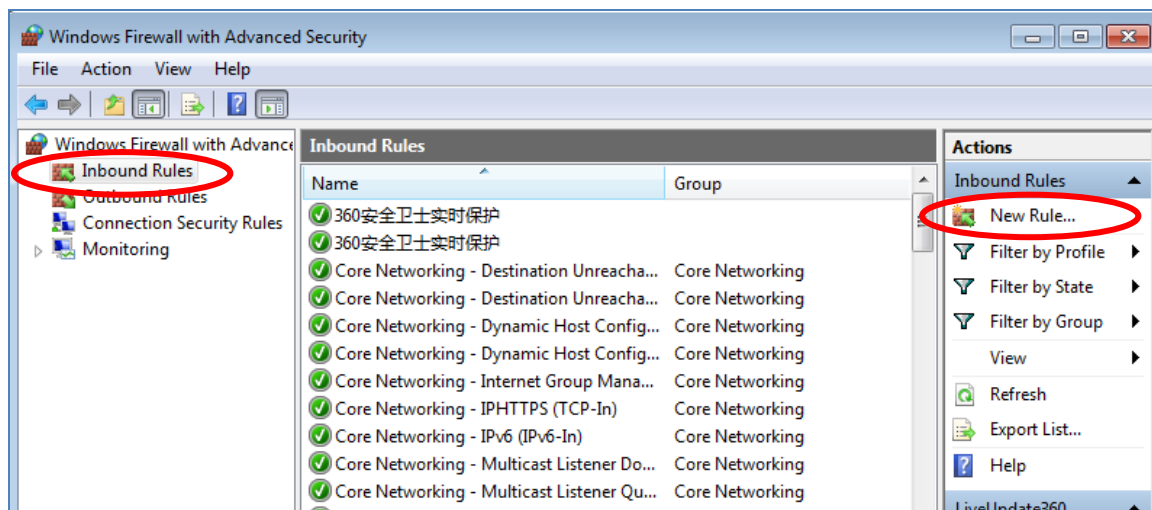
NetROCKEY4ND Firewall Setting for Windows 7

For Main/ Server Computer only

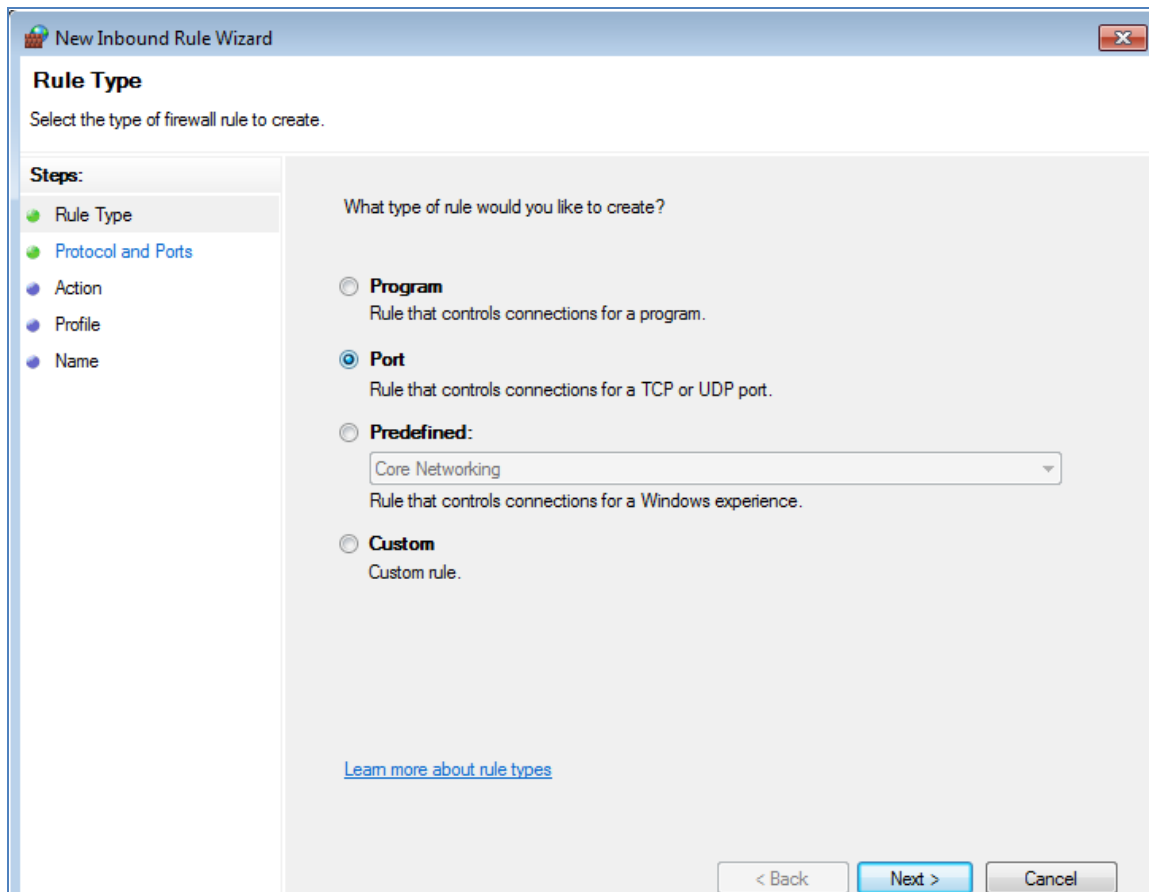
1. Go to Control Panel on the Main Computer (Computer are connected with NetRockey4ND Keylock)
2. Double click on Window Firewall, click on the Advance Setting



3. Click Inbound Rules and click New Rules



4. Select Port and click Next

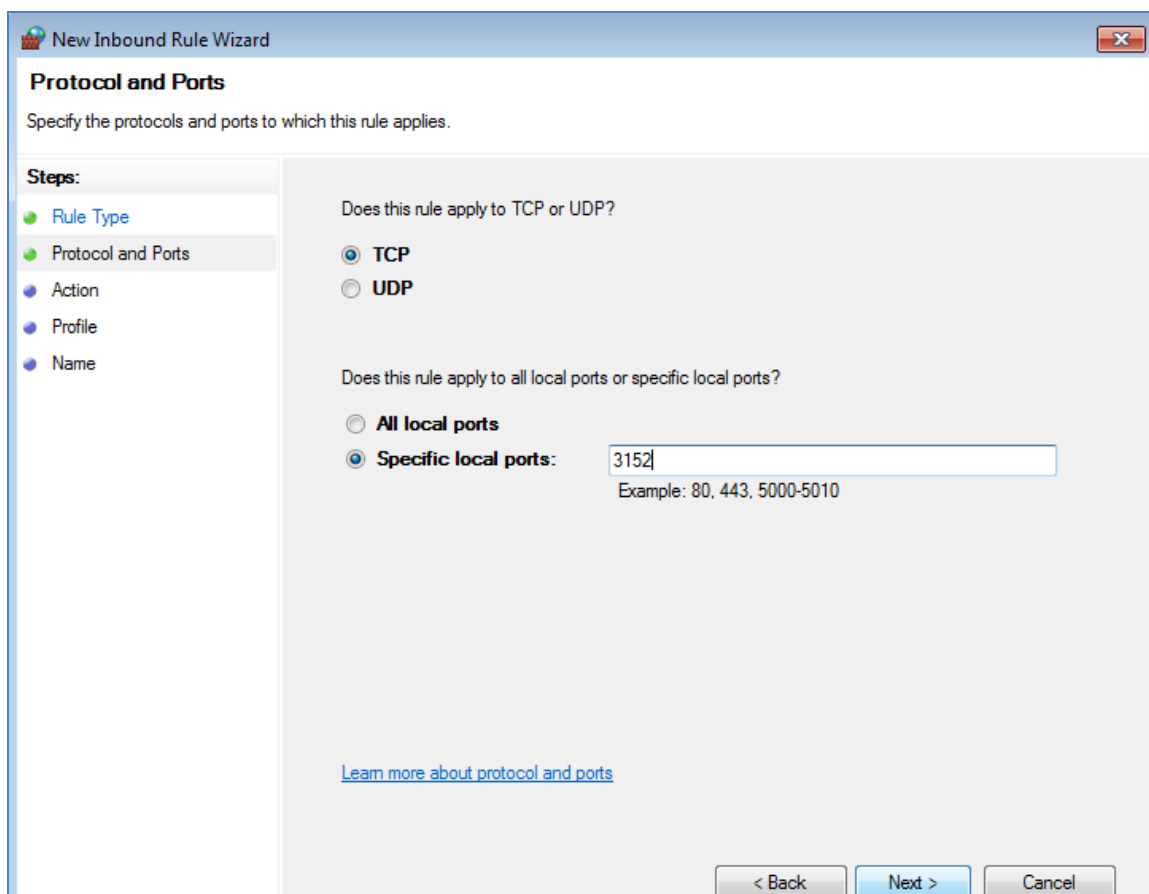


The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Rule Type' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps:' pane lists: Rule Type (selected), Protocol and Ports, Action, Profile, and Name. The main area asks 'What type of rule would you like to create?' and offers four options:

- ☐ **Program**: Rule that controls connections for a program.
- ☒ **Port**: Rule that controls connections for a TCP or UDP port.
- ☐ **Predefined:**: A dropdown menu shows 'Core Networking'. Description: Rule that controls connections for a Windows experience.
- ☐ **Custom**: Custom rule.

At the bottom, there is a link 'Learn more about rule types' and three buttons: '< Back', 'Next >', and 'Cancel'.

5. Select TCP and Specific local ports is 3152



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' pane lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area asks 'Does this rule apply to TCP or UDP?' with two options:

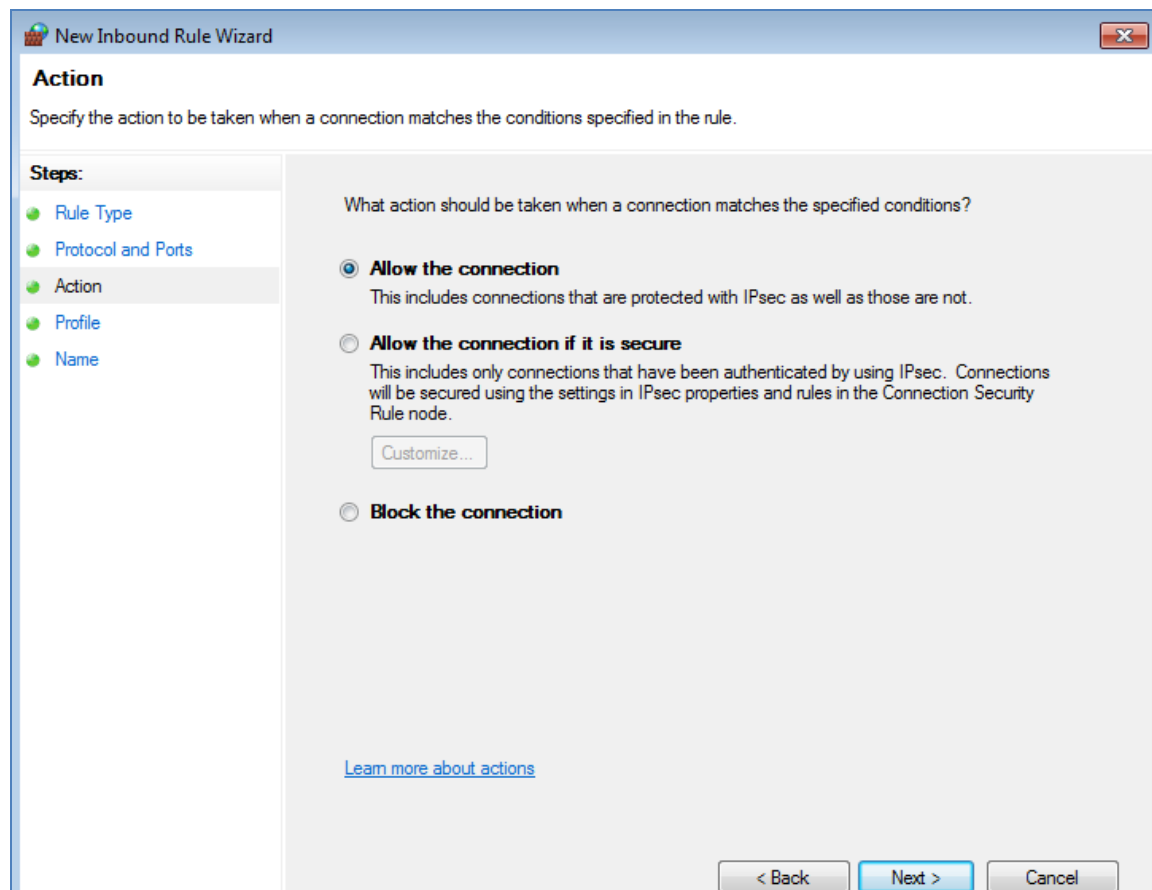
- ☒ **TCP**
- ☐ **UDP**

Below this, it asks 'Does this rule apply to all local ports or specific local ports?' with two options:

- ☐ **All local ports**
- ☒ **Specific local ports:** A text box contains '3152'. Below the text box is an example: 'Example: 80, 443, 5000-5010'.

At the bottom, there is a link 'Learn more about protocol and ports' and three buttons: '< Back', 'Next >', and 'Cancel'.

6. Select Allow the connection option



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action', followed by the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action' (highlighted), 'Profile', and 'Name'. The main area asks 'What action should be taken when a connection matches the specified conditions?' and offers three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. Descriptive text is provided for each option. A 'Customize...' button is next to the 'Allow the connection if it is secure' option. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons. A link 'Learn more about actions' is at the bottom left.

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.

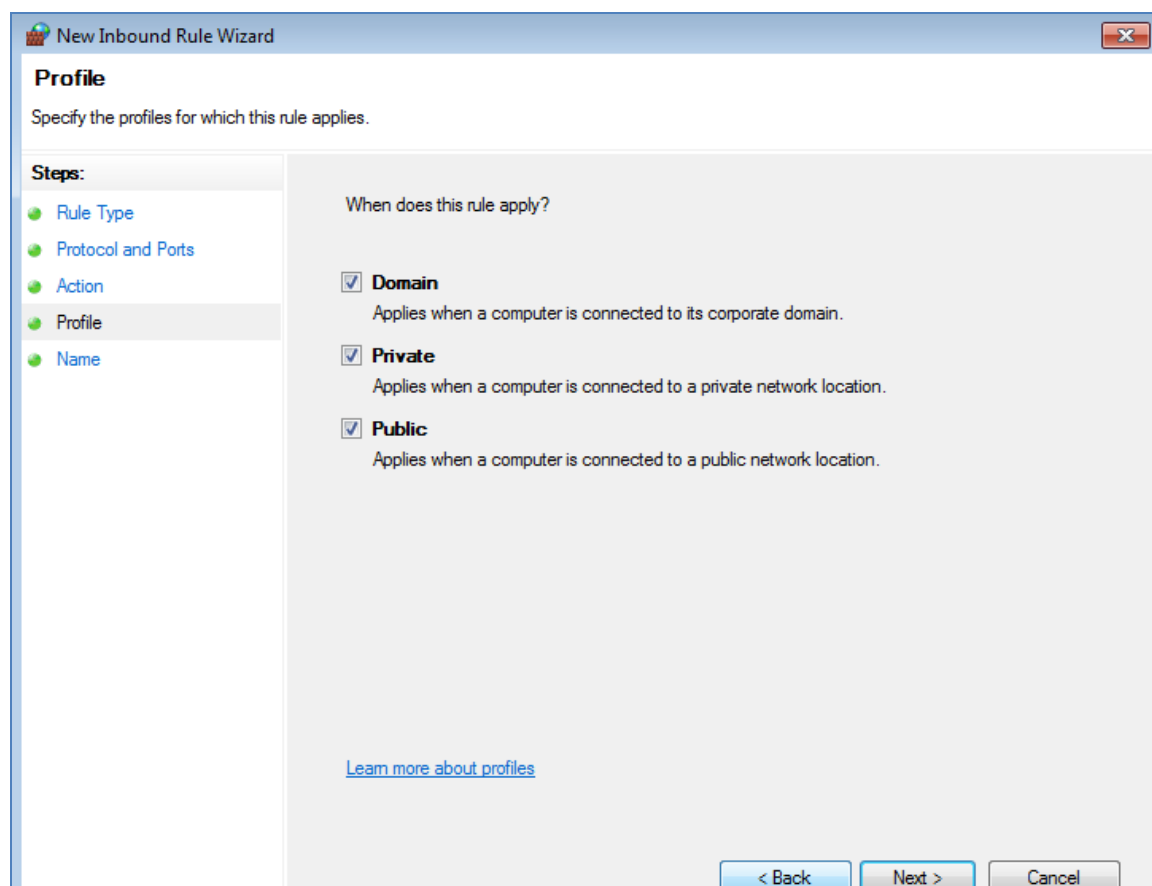
☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

[Learn more about actions](#)

< Back Next > Cancel

7. Apply all Rules



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile', followed by the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile' (highlighted), and 'Name'. The main area asks 'When does this rule apply?' and offers three checked checkbox options: 'Domain', 'Private', and 'Public'. Descriptive text is provided for each option. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons. A link 'Learn more about profiles' is at the bottom left.

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- 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.

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

[Learn more about profiles](#)

< Back Next > Cancel

8. Set the Name as Aplus Keylock

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

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

Name:
Aplus Keylock

Description (optional):

< Back Finish Cancel

Remark: In Windows 7 have to add Inbound Rules UDP, Outbound Rules TCP and Outbound Rules UDP also follow the steps above.

If any third party Antivirus or Firewall program installed, please open the 3152 TCP and UDP port for NetRocky4ND Services and set all permission for the Aplus program.

Clicfg.ini File Setting

In usually case, this file is setting well by default.

Clicfg.ini is a configuration file for the NetRockey4ND keylock. (No effect to the Rockey2 keylock)

1. Enable

This option must set equal to Y.

2. Time Out

Time frame to seek for NetRockey4ND keylock on LAN. Default value is 2, for slow computer recommended set to 4.

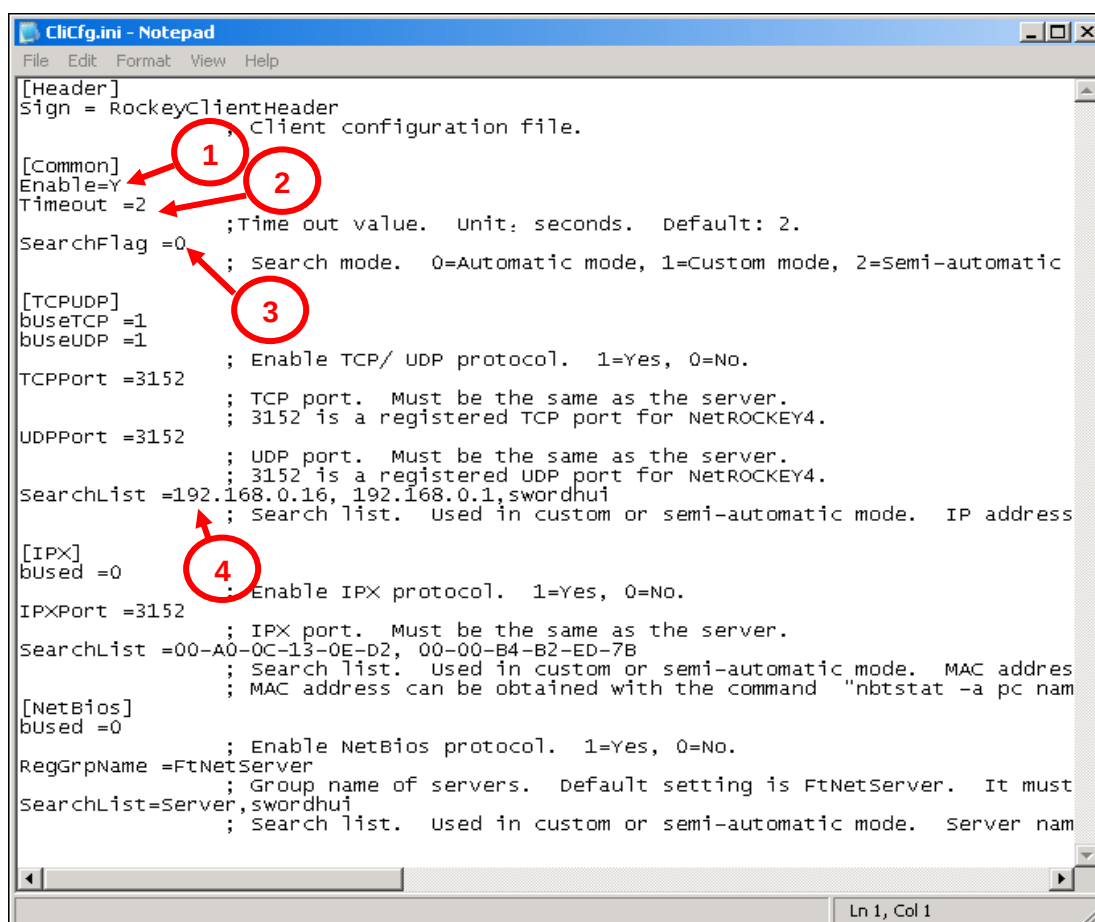
3. SearchFlag

Setting to set searching mode. Default is 0. (Automatic mode)

Set to 1 for custom mode, user must define the IP address of computer are connected the NetRockey4ND keylock at the search list.

4. SearchList

Set the Main computer IP here for custom SearchFlag mode.



```
[Header]
Sign = RockeyClientHeader
; Client configuration file.

[Common]
Enable=Y
Timeout =2
SearchFlag =0
; Time out value. Unit: seconds. Default: 2.
; Search mode. 0=Automatic mode, 1=Custom mode, 2=Semi-automatic

[TCPUDP]
buseTCP =1
buseUDP =1
; Enable TCP/ UDP protocol. 1=Yes, 0=No.
TCPPort =3152
; TCP port. Must be the same as the server.
; 3152 is a registered TCP port for NetROCKEY4.
UDPPort =3152
; UDP port. Must be the same as the server.
; 3152 is a registered UDP port for NetROCKEY4.
SearchList =192.168.0.16, 192.168.0.1, swordhui
; Search list. Used in custom or semi-automatic mode. IP address

[IPX]
bUsed =0
; Enable IPX protocol. 1=Yes, 0=No.
IPXPort =3152
; IPX port. Must be the same as the server.
SearchList =00-A0-0C-13-0E-D2, 00-00-B4-B2-ED-7B
; Search list. Used in custom or semi-automatic mode. MAC address
; MAC address can be obtained with the command "nbtstat -a pc nam

[NetBios]
bused =0
; Enable NetBios protocol. 1=Yes, 0=No.
RegGrpName =FtNetServer
; Group name of servers. Default setting is FtNetServer. It must
SearchList=Server, swordhui
; Search list. Used in custom or semi-automatic mode. Server nam
```

The screenshot shows the Clicfg.ini file in Notepad. Four red circles with numbers 1 through 4 are placed over the file, with arrows pointing to specific settings: 1 points to 'Enable=Y', 2 points to 'Timeout =2', 3 points to 'SearchFlag =0', and 4 points to 'SearchList =192.168.0.16, 192.168.0.1, swordhui'.