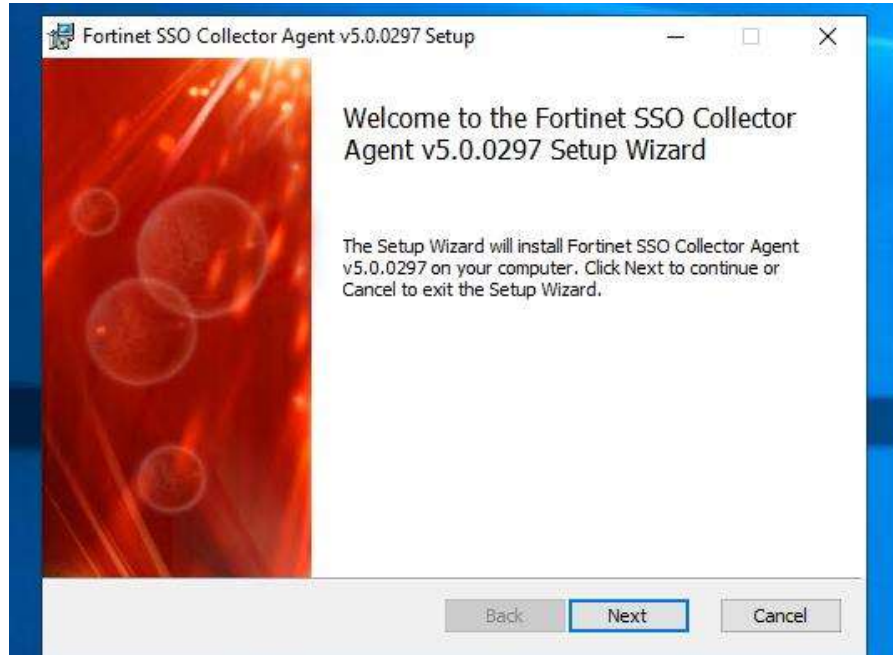


FSSO / DC Agent Guide

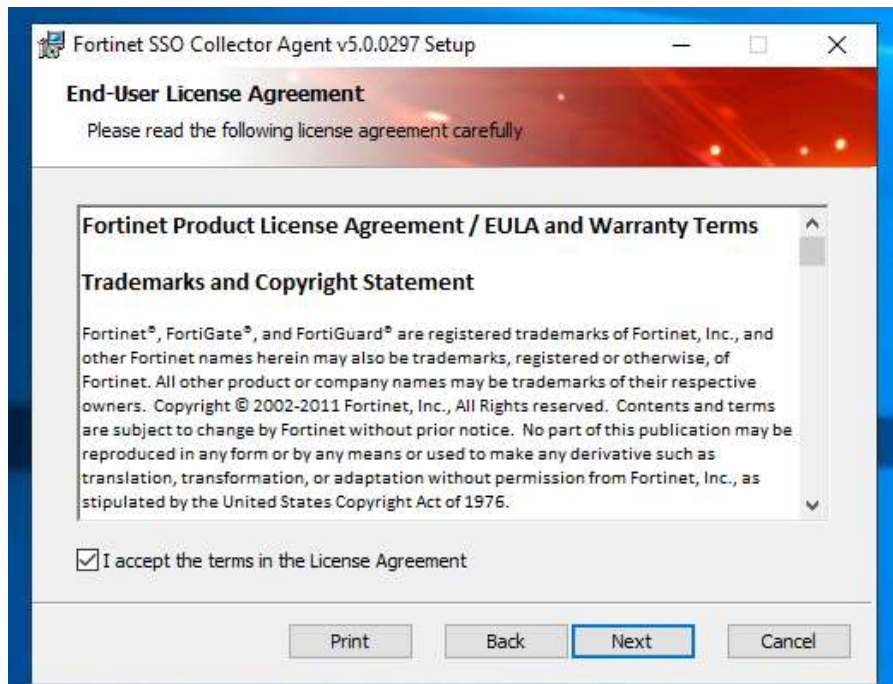


Instructions

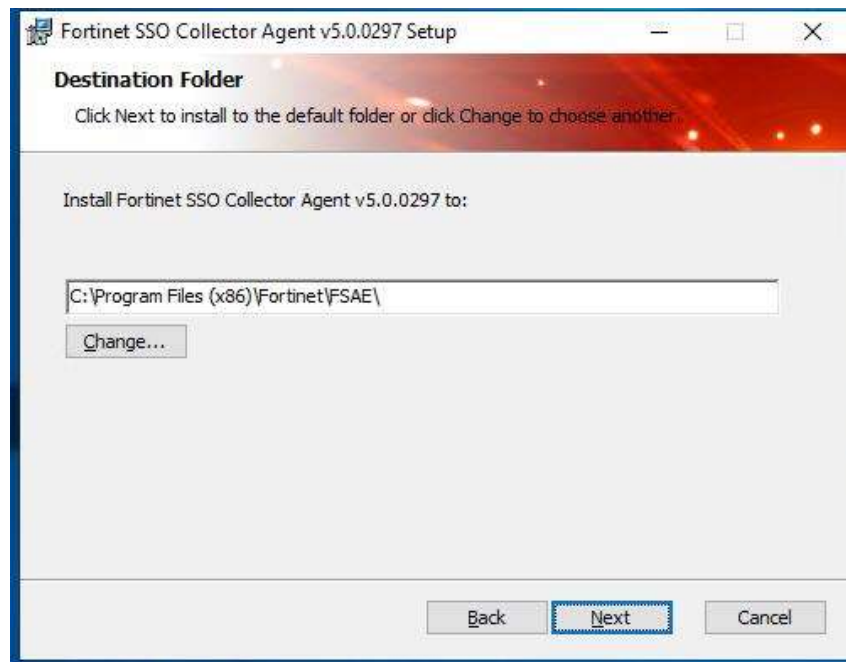
Run the FSSO software provided by Schools Broadband and click the next button



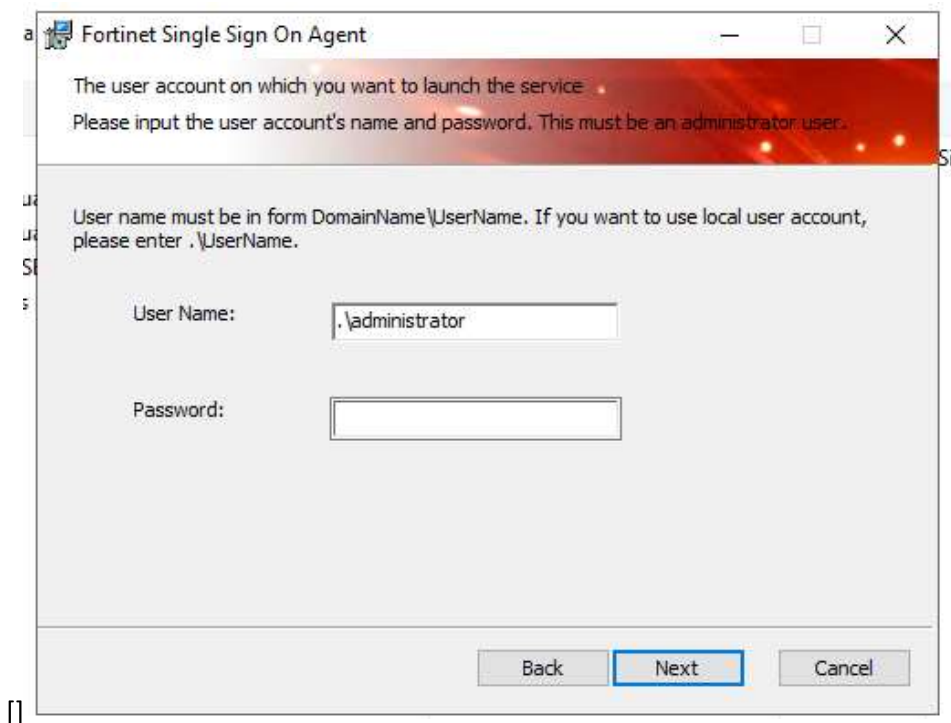
Accept the LA and click the next button



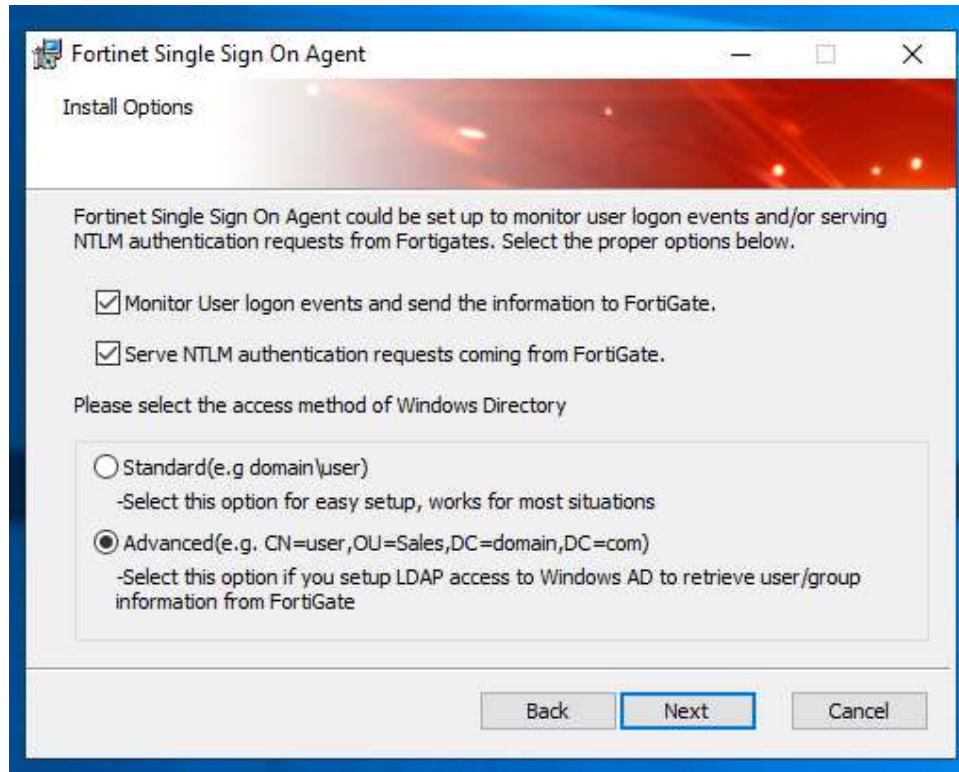
Confirm the installation path is correct and click next



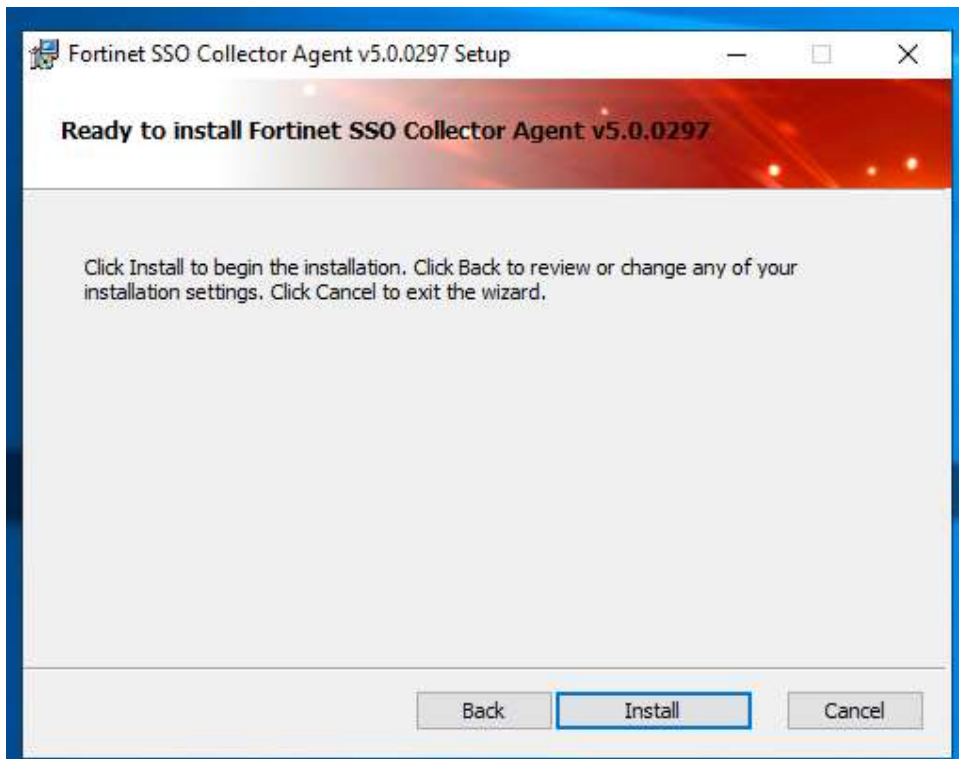
Enter a valid administrator account with its password and click next



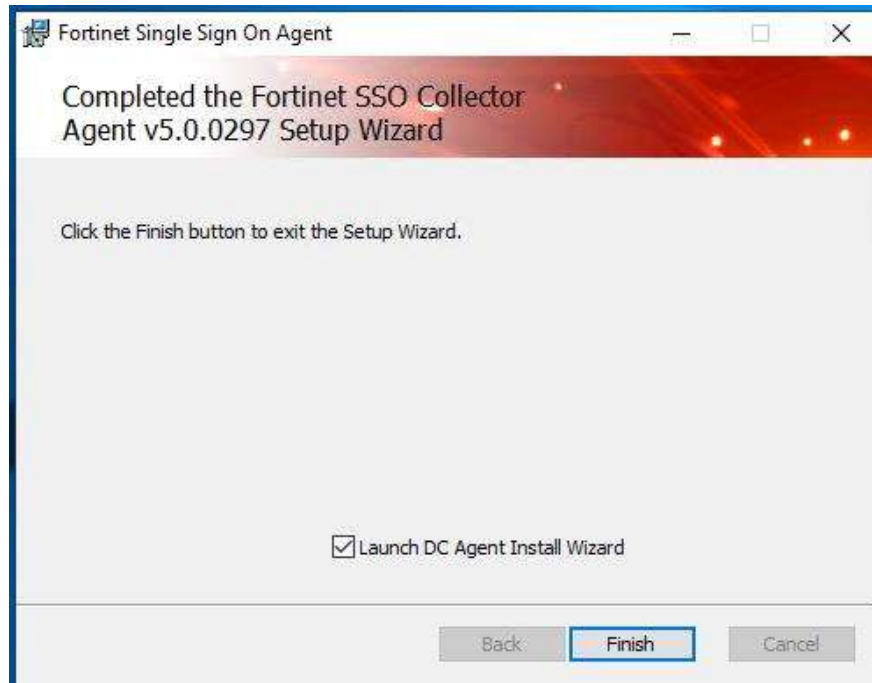
Ensure “Advanced” is selected (as per the below screenshot) and click next



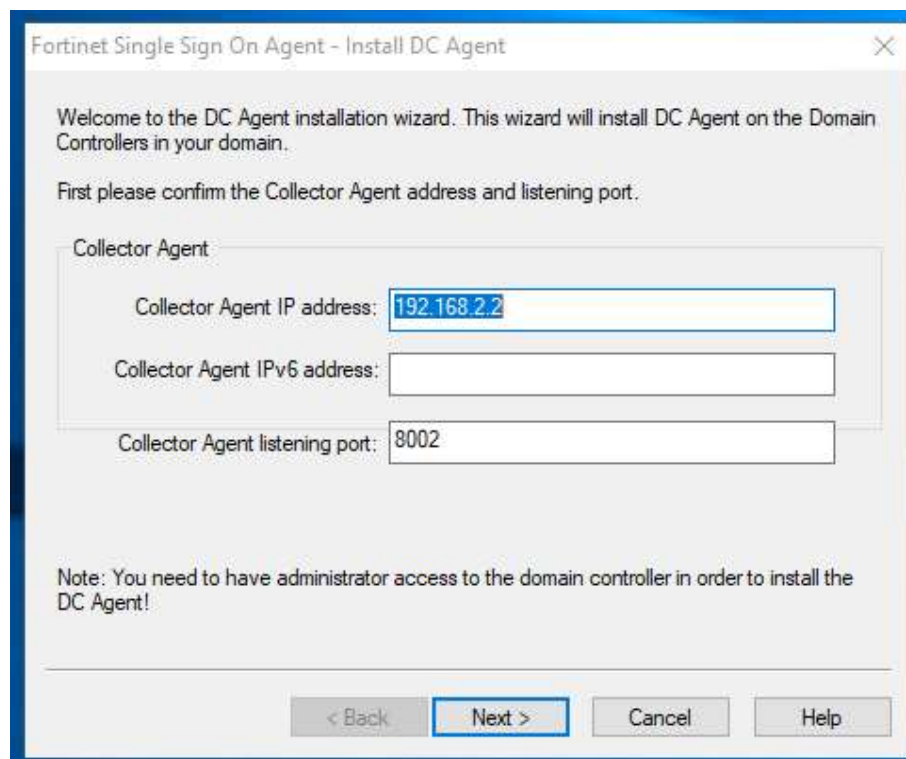
Click install



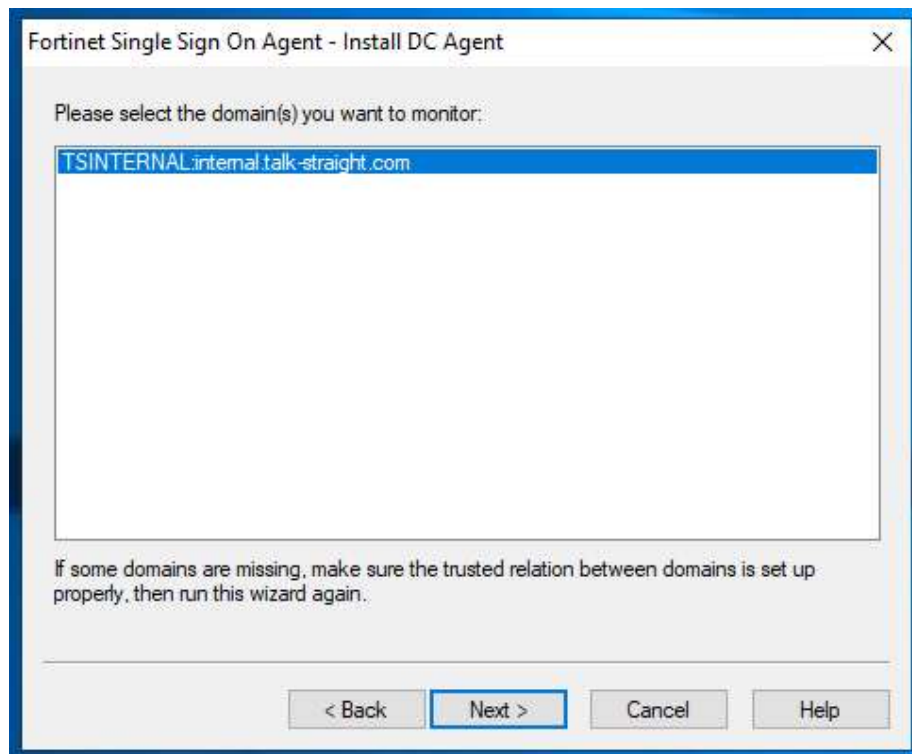
Ensure the box is ticked and click finish



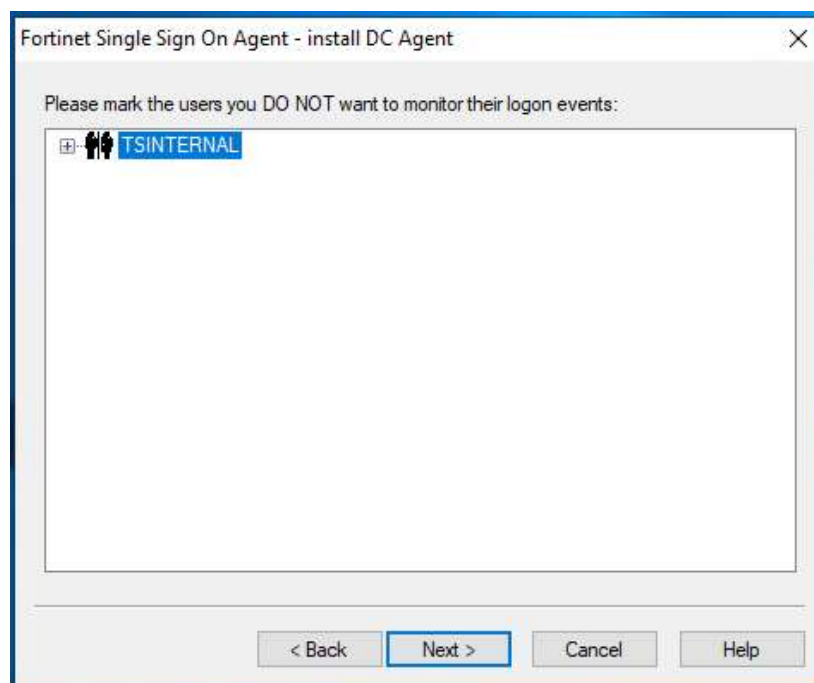
Confirm the IP address is correct and click next



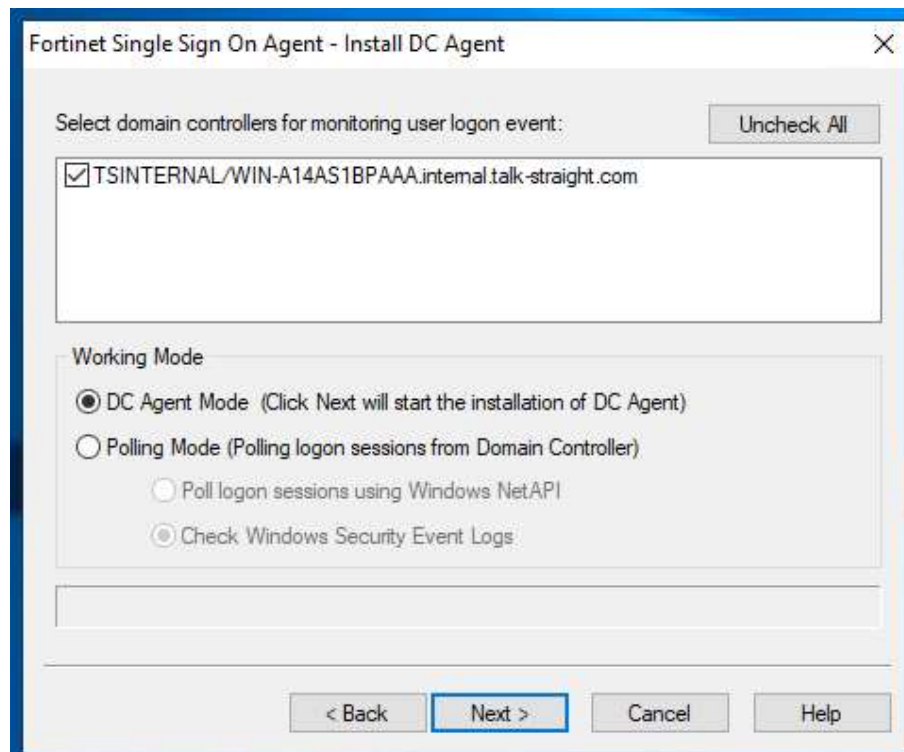
Select the domain so it is highlighted blue and click next



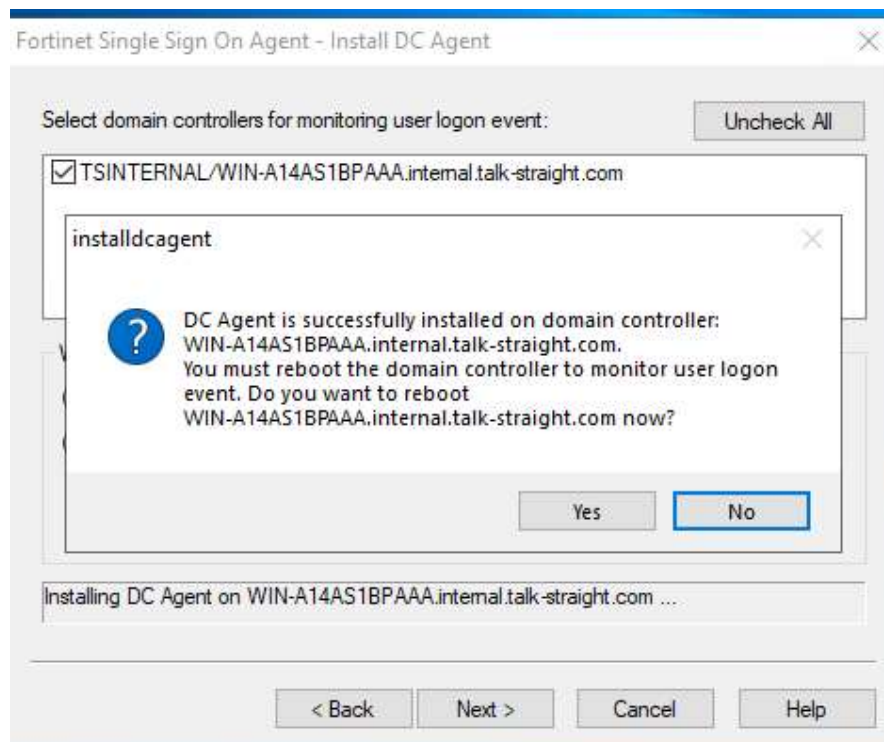
If you have any service accounts that you don't want to authenticate, expand the domain selector, and tick any users that don't need to authenticate. This would include service accounts etc. Click next



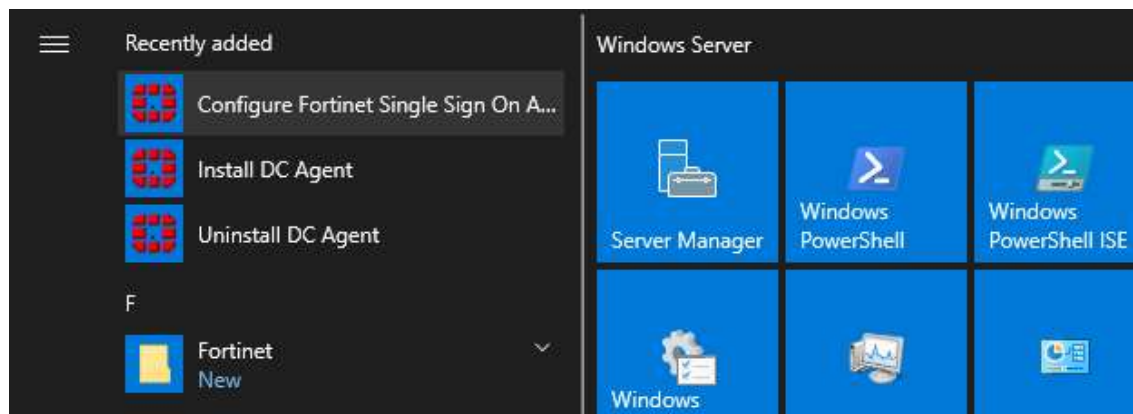
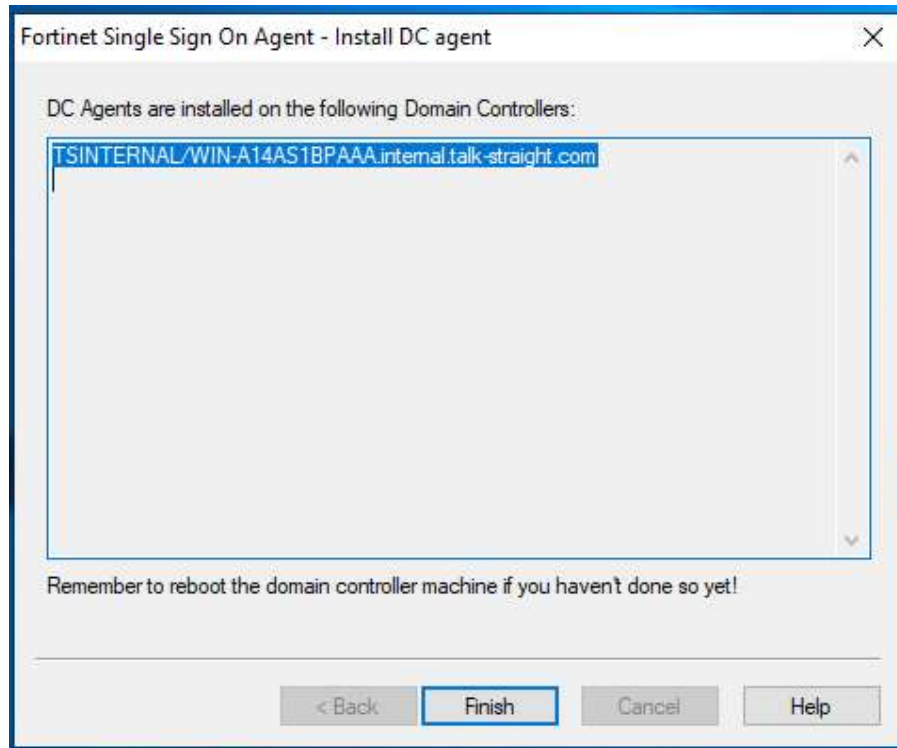
Ensure “DC Agent Mode” is selected and click next



Unless you are happy to reboot the server now, click no



Click finish

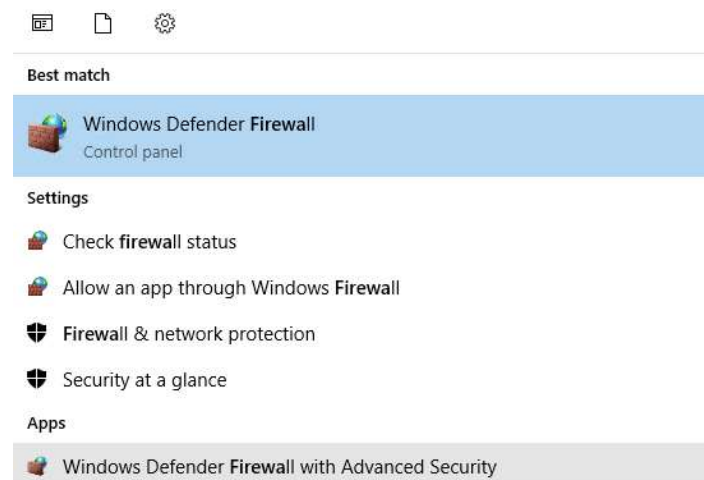


From the start bar find and click “Configure Fortinet Single Sign On Agent”

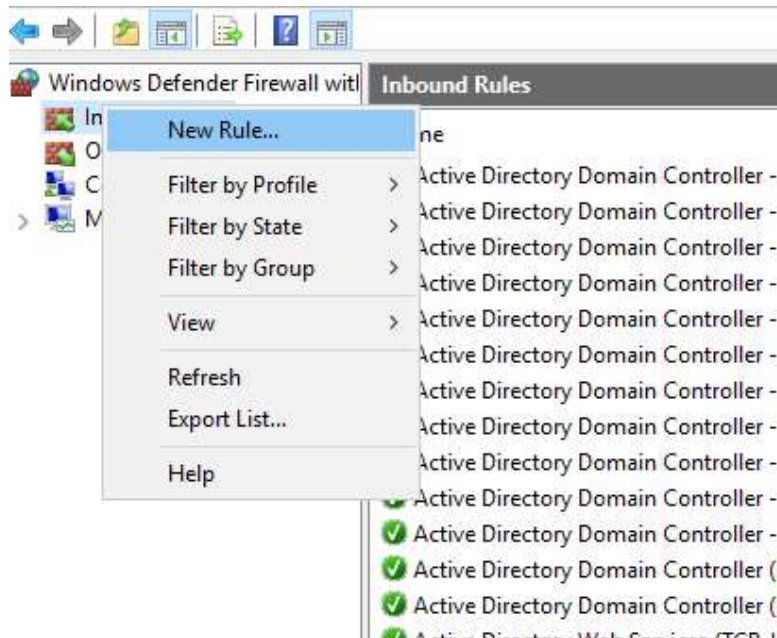
Leave all settings as default except the password, change this to F0rtinet22! Click Save & close

You must ensure the certain ports are allowed inbound to the server, the following example uses Windows Advanced Firewall

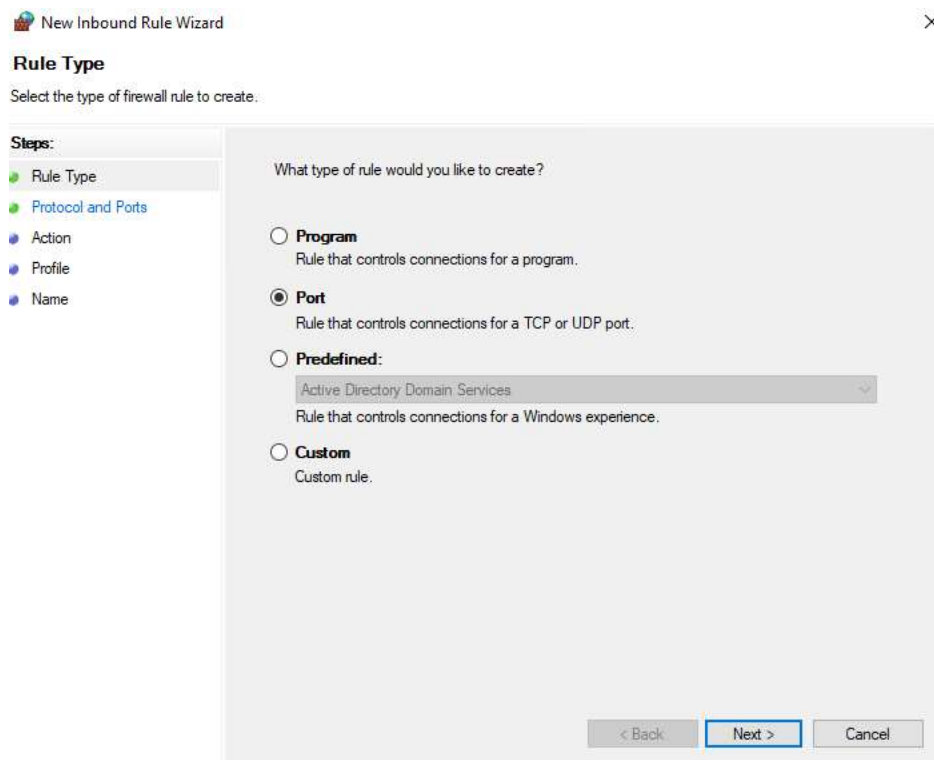
Open Windows Defender Firewall with Advanced Security



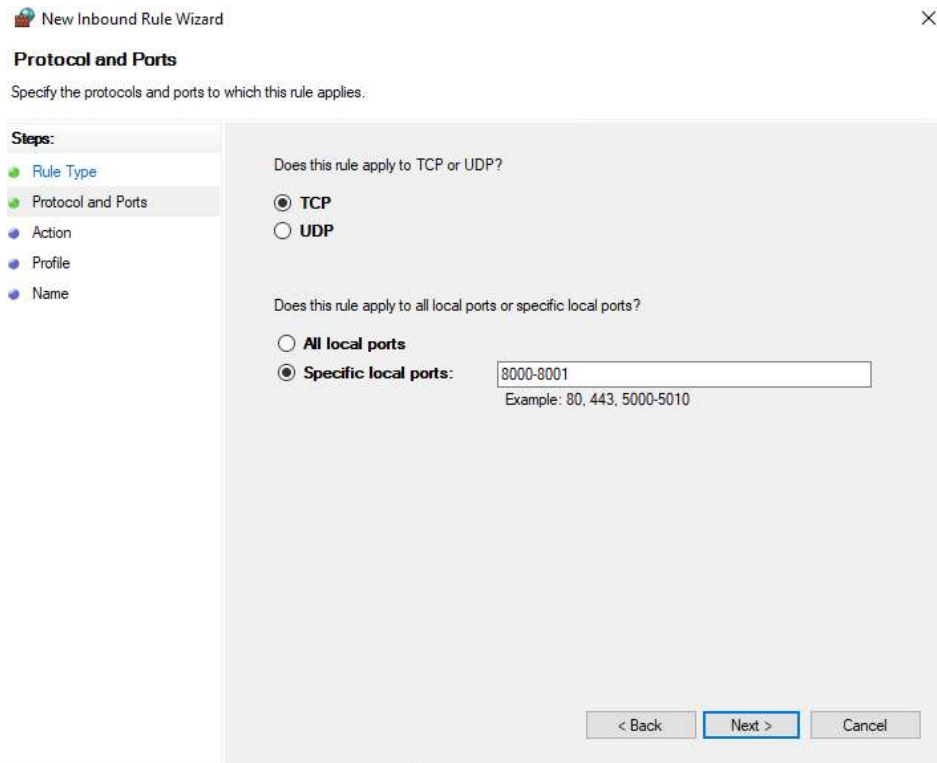
Right click Inbound Rules and click New Rule...



Select Port and click next



Select TCP, and specify 8000-8001 as the local ports, click next



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?

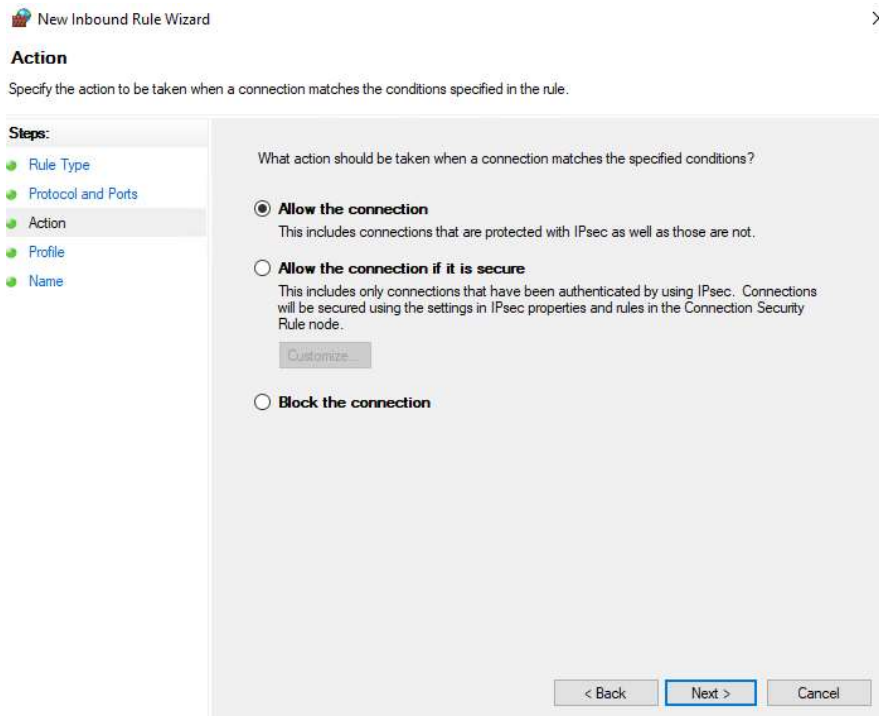
☐ **All local ports**

☒ **Specific local ports:**

Example: 80, 443, 5000-5010

< Back **Next >** Cancel

Ensure the connection is allowed and click next



New Inbound 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.

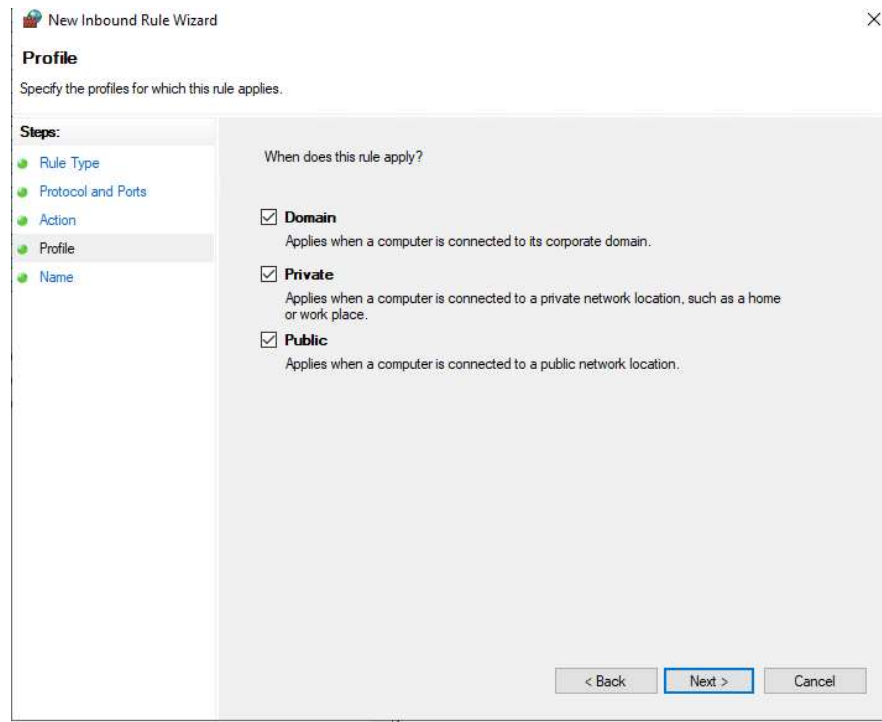
☐ **Allow the connection if it is secure**

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**

< Back **Next >** Cancel

Select all the profiles and click next



New Inbound Rule Wizard

Profile
Specify the profiles for which this rule applies.

Steps:

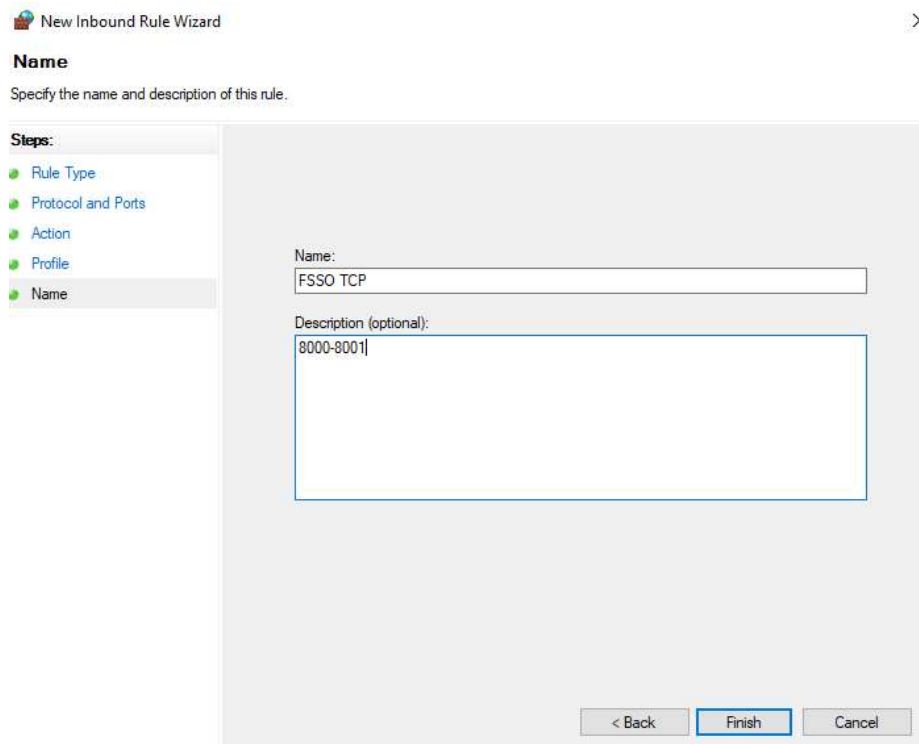
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

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

< Back **Next >** Cancel

Give the rule and appropriate name and click Finish



New Inbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

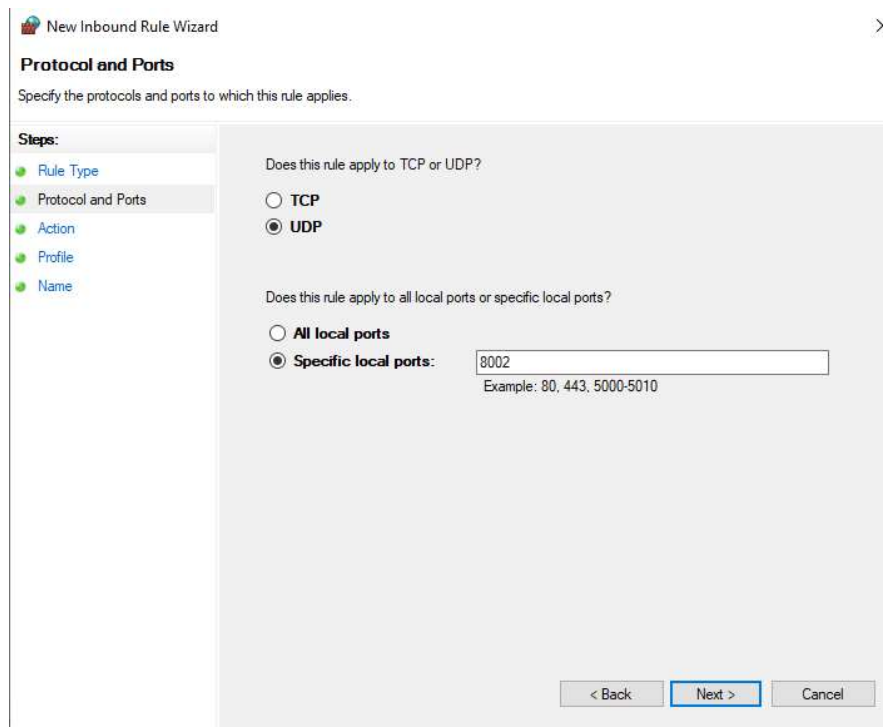
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
FSSO TCP

Description (optional):
8000-8001

< Back **Finish** Cancel

Repeat the firewall steps again this time adding UDP Port 8002, see screenshots below.



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

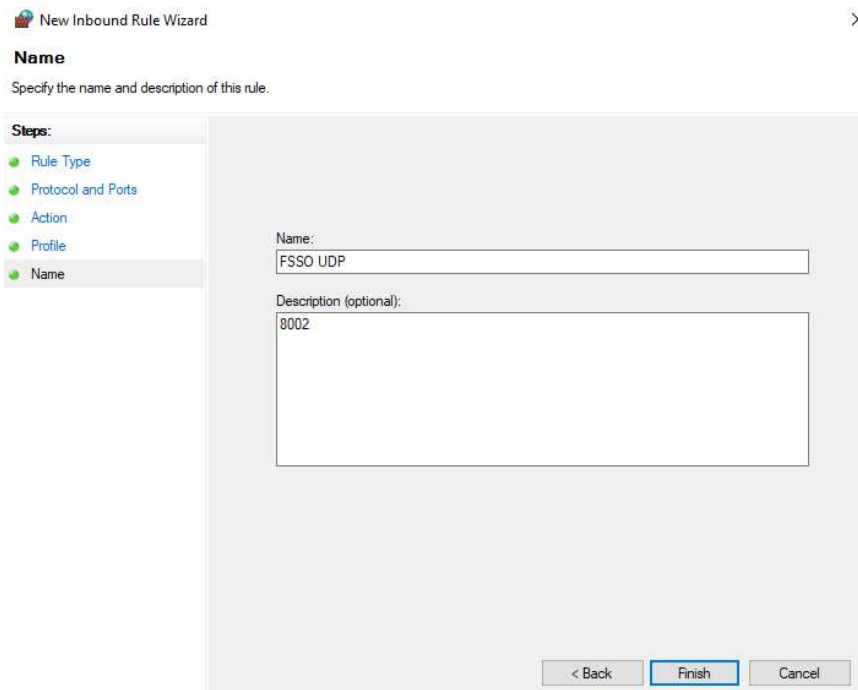
Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

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

Name:

Description (optional):

< Back Finish Cancel

Repeat these steps on ALL domain controllers and ensure that the domain controllers are rebooted before the software is used

If in doubt please do wait for your go live date, when our engineers will be able to assist