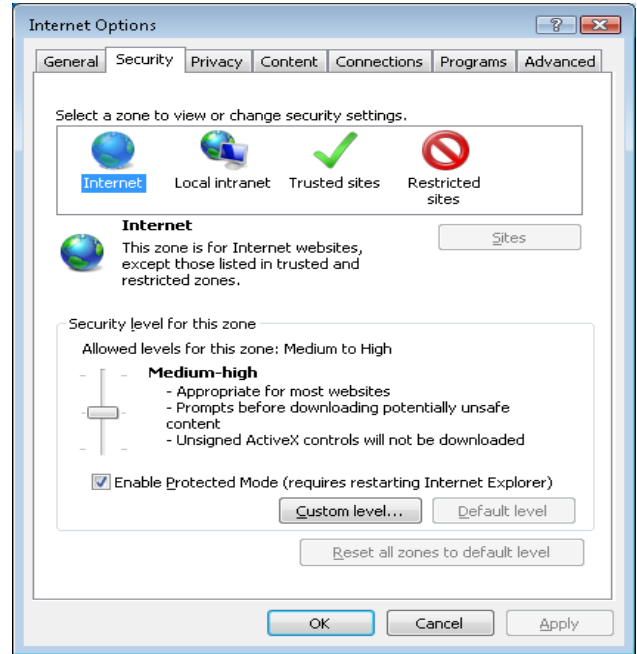


CompleteView Troubleshooting: Web Client Will Not Display Cameras

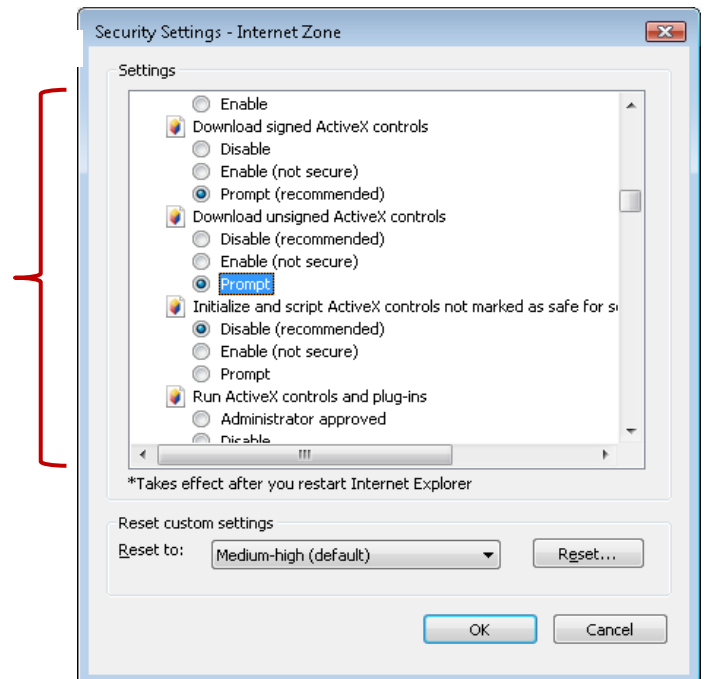
1. Confirm that the Internet Explorer Security Settings are configured for both Internet and Local Intranet on the client workstation.

CompleteView's Web Client uses an ActiveX control for the display of video. It may be necessary to modify the Internet Explorer security settings on the computers access CompleteView's Web Client to allow the ActiveX control.

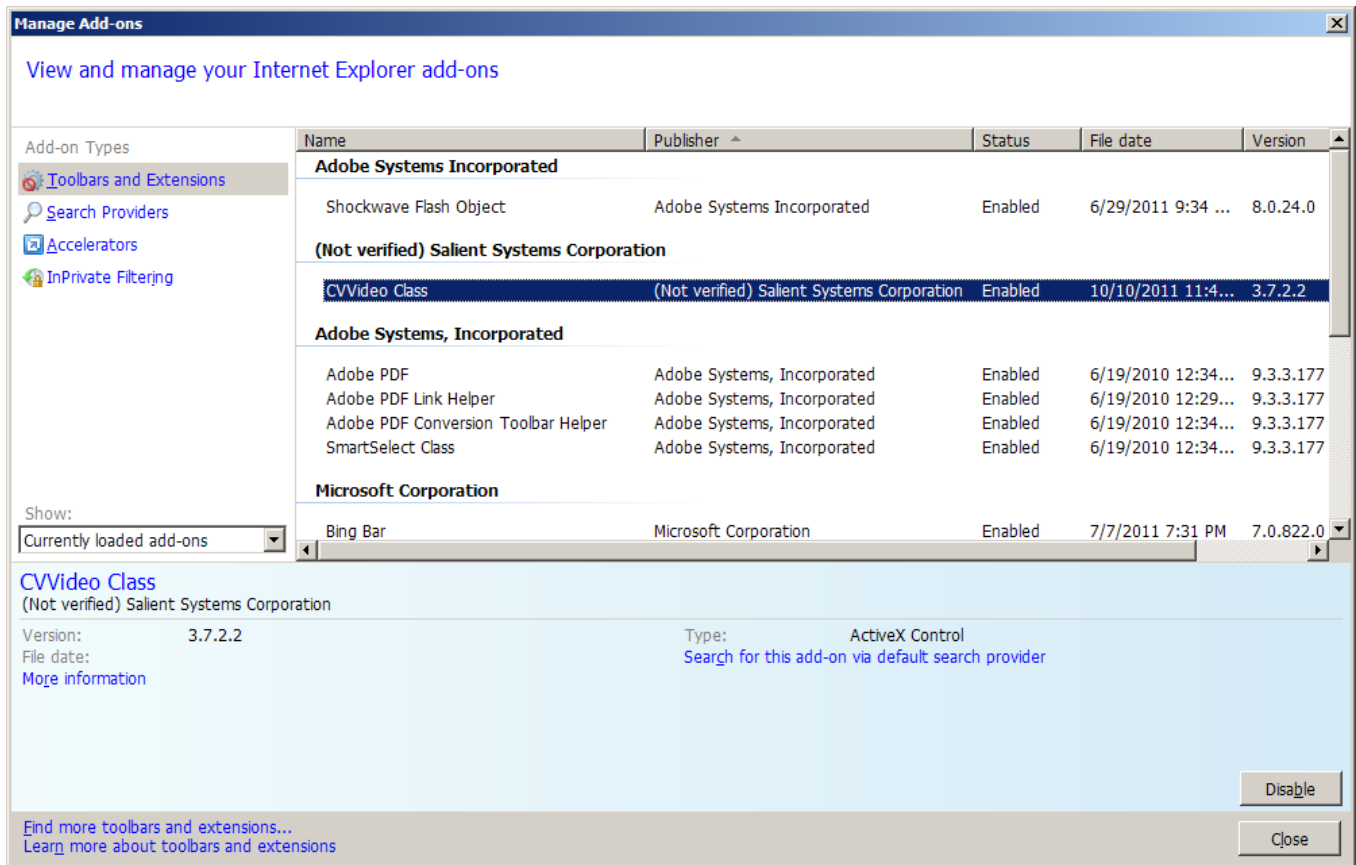
- Open *Microsoft Internet Explorer* Web browser.
- Click the **Tools** button or menu, and then select **Internet Options**.
- Click the **Security** tab.
- Select the **Internet** zone.
- Under the Security Level section, click Custom Level.
- Using the scroll bar, locate the settings shown in the table below and change to the correct setting listed. Click OK.
- Next, select the **local intranet** zone and run through the same settings to make sure they are configured as well.



Windows Security Setting Description	Correct Setting
Allow previously unused ActiveX controls to run without prompt	Enable
Allow Scriptlets	Enable
Display Video and animation on a webpage that does not use external medial player	Enable
Download signed ActiveX controls	Prompt
Download unsigned ActiveX controls	Prompt
Initialize and script ActiveX controls not marked as safe for scripting	Prompt
Run ActiveX controls and plug-ins	Enable



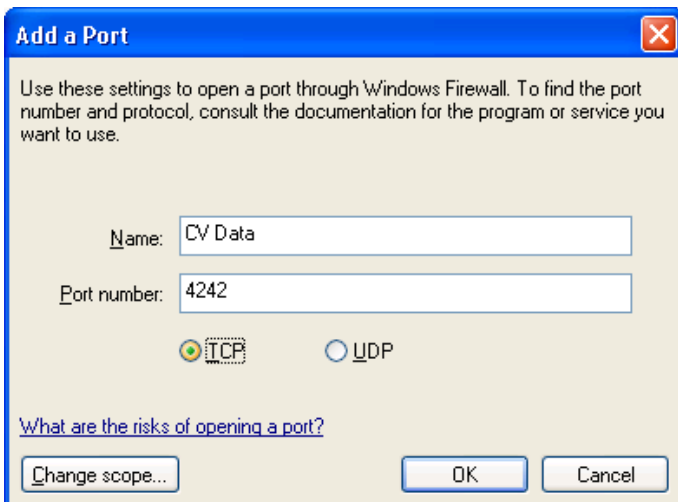
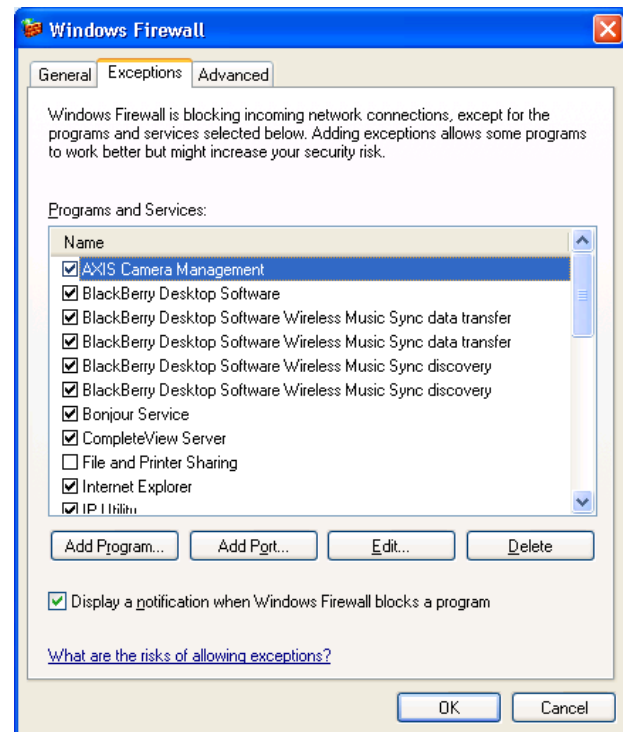
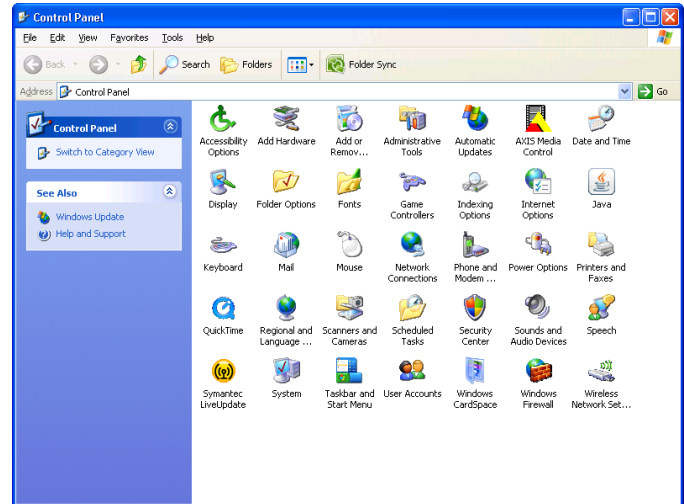
- Confirm that the Active X Control is installed properly. You can click on tools and manage add-ons to see if it is installed properly. You should have listed CVVideo Class and it should show the status as Enabled.



- If the Active X Control has been installed, confirm that port exceptions for CompleteView Web Client (default TCP 8080) and CompleteView Data Port (4242) have been added to any active firewall(s) on the CompleteView server that is recording video. Additional port exceptions for other CompleteView Applications can also be added, these ports are as follows: TCP 4243, 4250, and 4255. You can find the instructions to add exceptions to the Windows Firewall below.

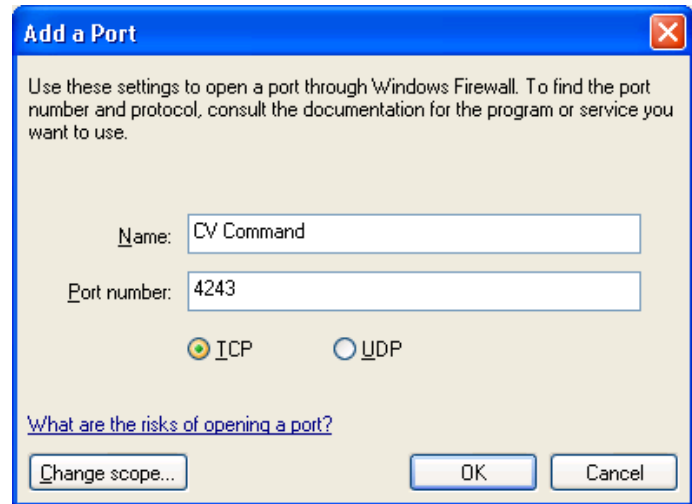
Windows XP Firewall Settings

- Open Control Panel by clicking *Start* then *Control Panel*.
- Click *Windows Firewall* to open the firewall settings.
- Select the *Exceptions* tab then click *Add Port* to add an exception.



- On the *Add a Port* dialog box enter "CV Data" as the *Name*; enter 4242 as the *Port Number*; set the *Protocol* to *TCP*. Click *OK* to add the port exception.

- Click the Add Port button on the Windows Firewall Exceptions tab to add another port exception. On the *Add a Port* dialog box enter “CV Command” as the *Name*; enter 4243 as the *Port Number*; set the *Protocol* to *TCP*. Click *OK* to add the port exception.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: CV Command

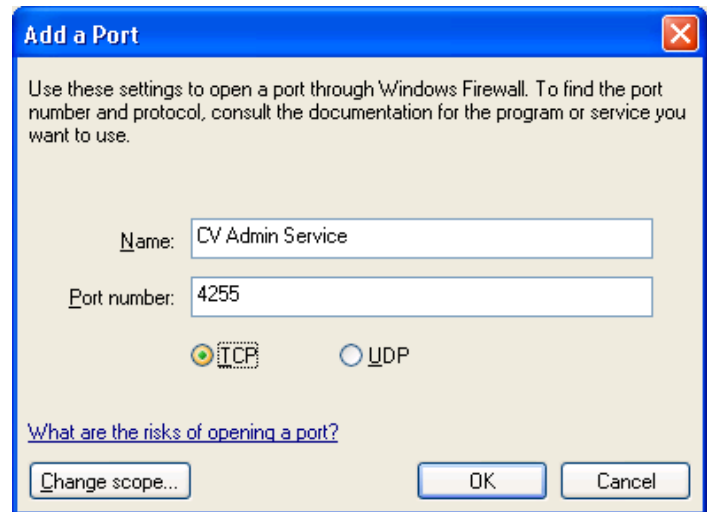
Port number: 4243

TCP UDP

[What are the risks of opening a port?](#)

Change scope... OK Cancel

- Click the Add Port button on the Windows Firewall Exceptions tab to add another port exception. On the *Add a Port* dialog box enter “CV Admin Service” as the *Name*; enter 4255 as the *Port Number*; set the *Protocol* to *TCP*. Click *OK* to add the port exception.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: CV Admin Service

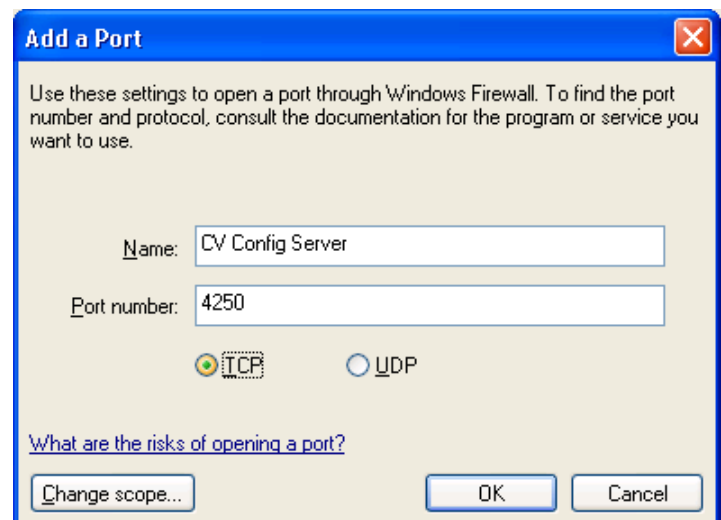
Port number: 4255

TCP UDP

[What are the risks of opening a port?](#)

Change scope... OK Cancel

- Click the Add Port button on the Windows Firewall Exceptions tab to add another port exception. On the *Add a Port* dialog box enter “CV Config Server” as the *Name*; enter 4250 as the *Port Number*; set the *Protocol* to *TCP*. Click *OK* to add the port exception.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: CV Config Server

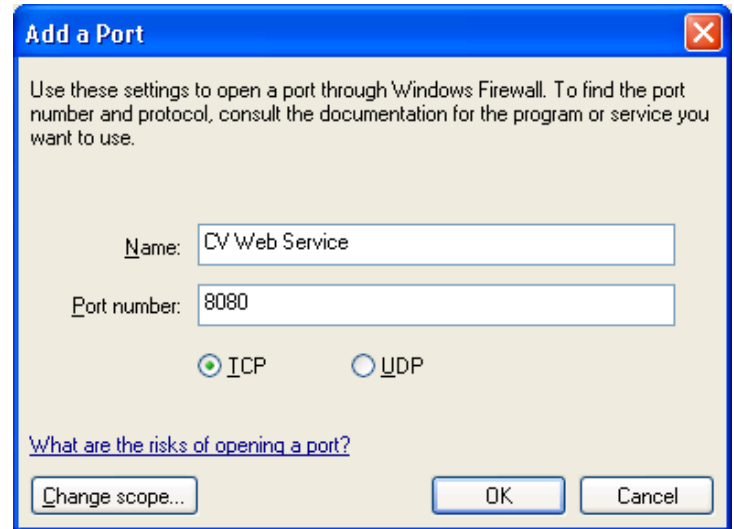
Port number: 4250

TCP UDP

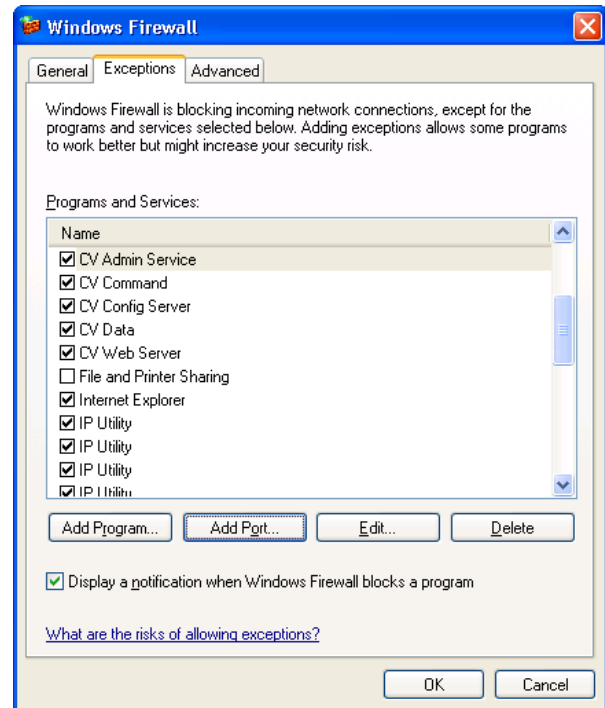
[What are the risks of opening a port?](#)

Change scope... OK Cancel

- Click the Add Port button on the Windows Firewall Exceptions tab to add another port exception. On the *Add a Port* dialog box enter “CV Web Service” as the *Name*; enter 8080 as the *Port Number*; set the *Protocol* to *TCP*. Click *OK* to add the port exception.



- Click *OK* on the *Windows Firewall* dialog to save the changes.

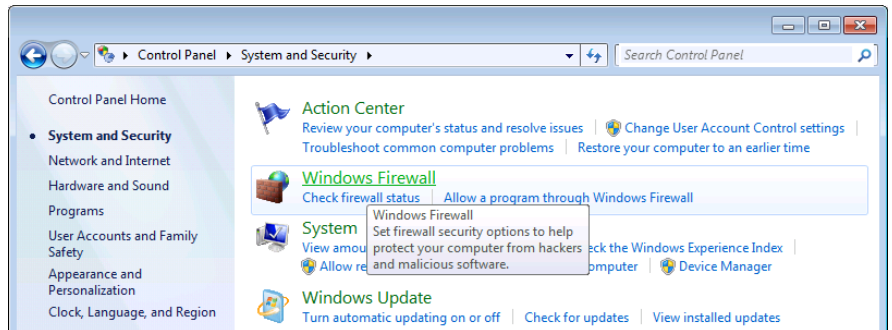


Configuration of Windows Firewall on Windows 7

- Open Control Panel by clicking *Start* then *Control Panel*.
- Open the Security options by clicking *System and Security*.



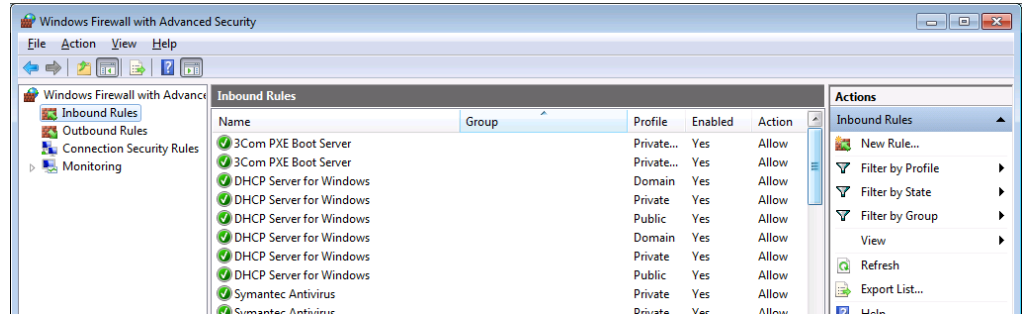
- Click *Windows Firewall*.



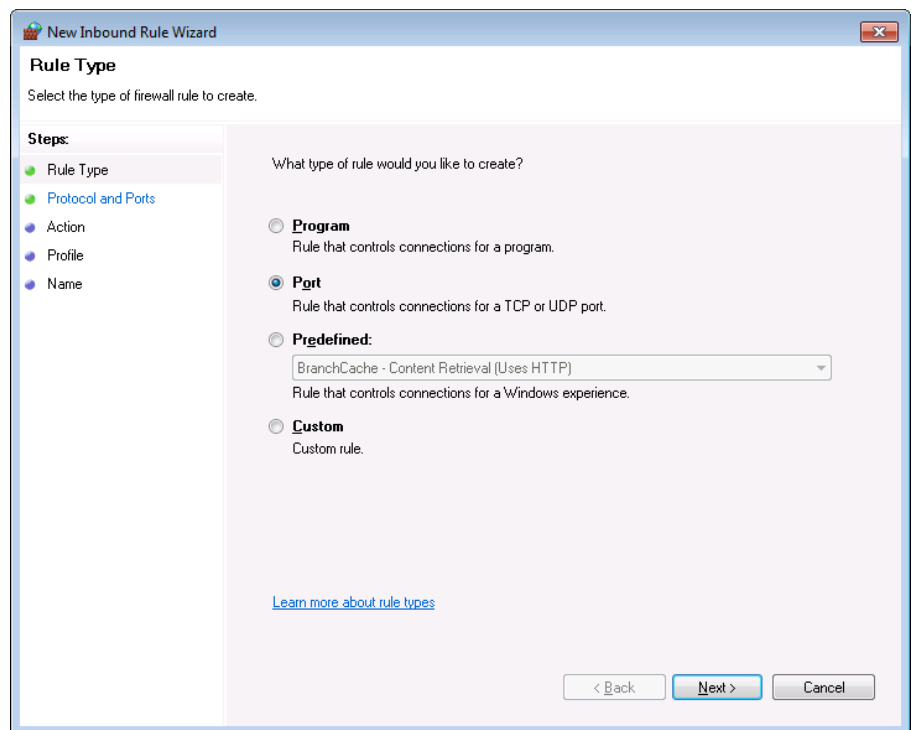
- Click *Advanced Settings*.



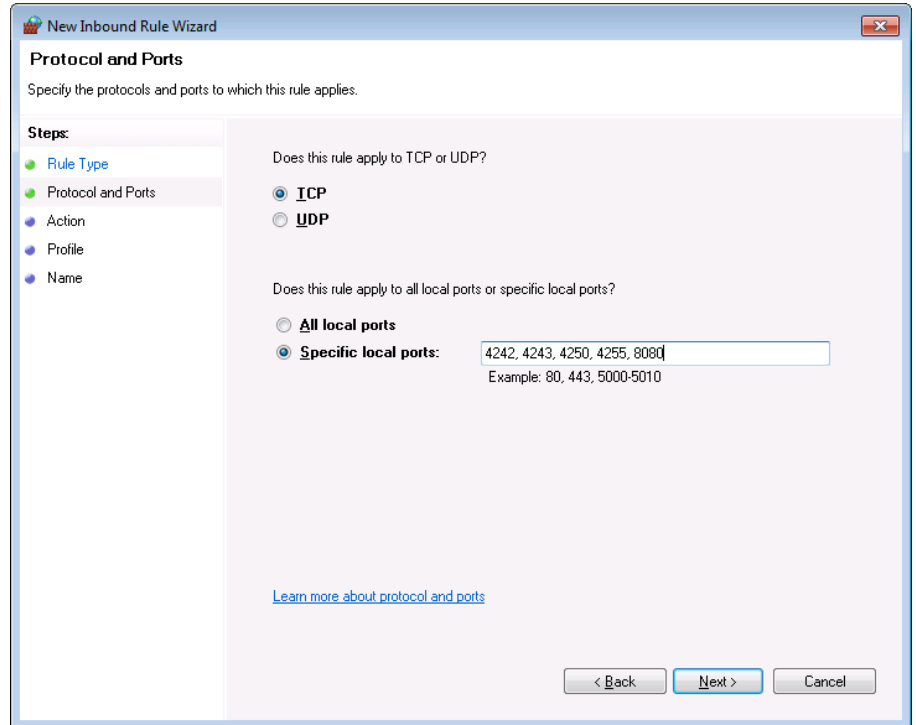
- Select *Inbound Rules*.
- Click *New Rule*.



- Select *Port* and click next.



- Enter in the following ports as *Specific Local Ports* and click next.
 - a. 4242 – Data
 - b. 4243 – Command
 - c. 4250 – Config Server
 - d. 4255 – Admin Service
 - e. 8080 – Web Server*
*Optional

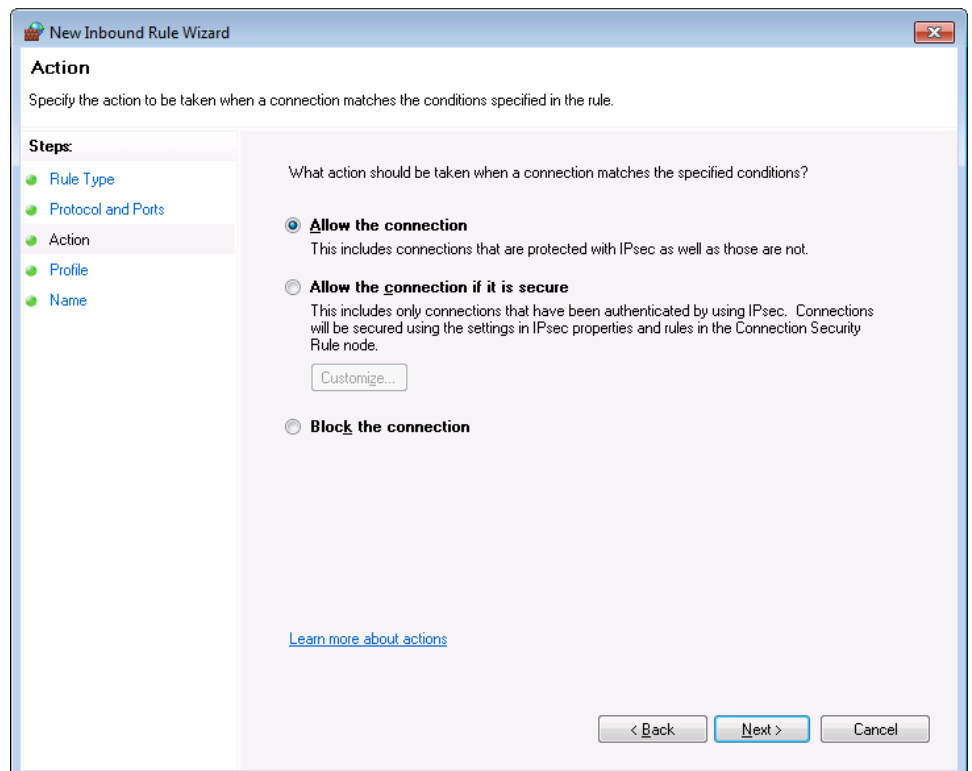


The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The 'Steps' pane on the left shows 'Protocol and Ports' as the current step. The main area contains two questions with radio button options:

- Does this rule apply to TCP or UDP?
 - ICP
 - UDP
- Does this rule apply to all local ports or specific local ports?
 - All local ports
 - Specific local ports:
Example: 80, 443, 5000-5010

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

- Select *Allow the connection and click next.*

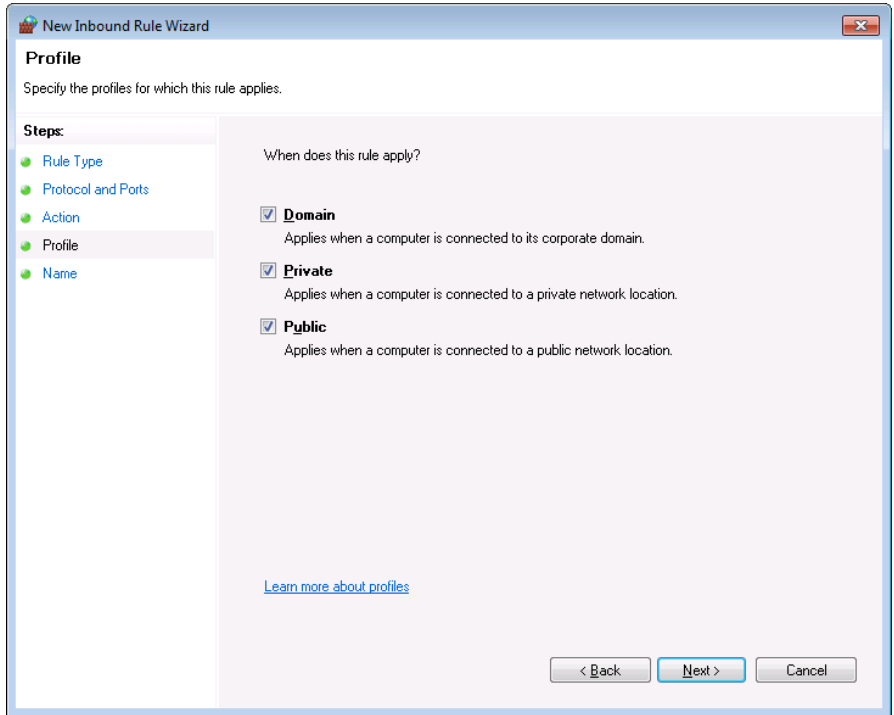


The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The 'Steps' pane on the left shows 'Action' as the current step. The main area contains a question with three radio button options:

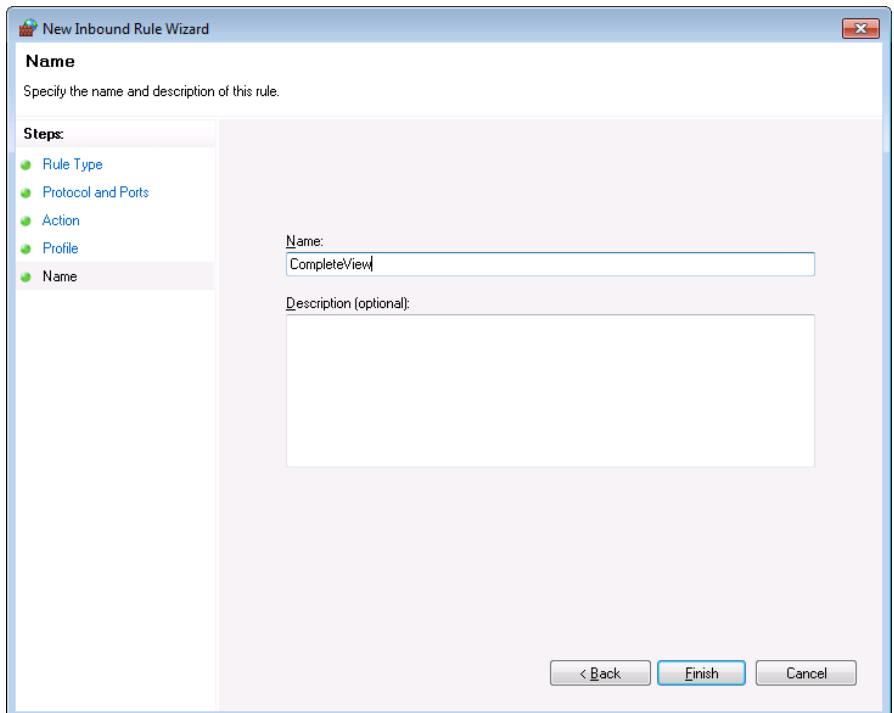
- What action should be taken when a connection matches the specified conditions?
 - Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
 - Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
 - Block the connection**

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A link 'Learn more about actions' is also present.

- Select which network types apply to this rule and click next. If you are not sure, select all.

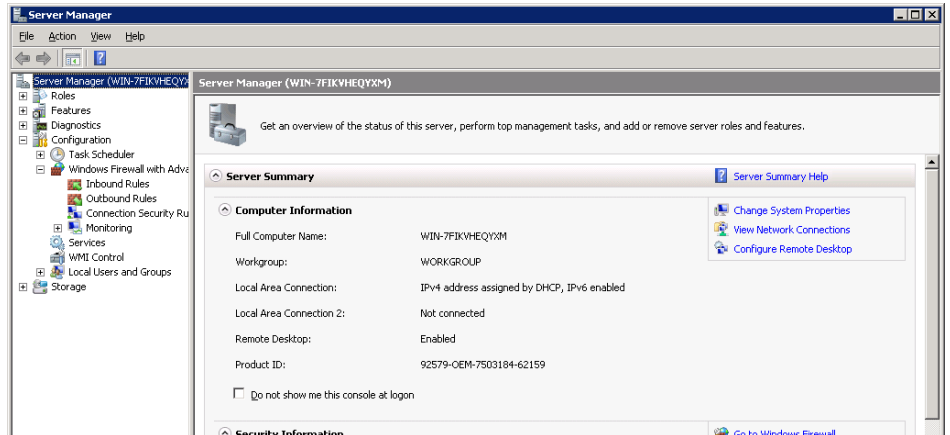


- Name the rule CompleteView and click Finish.

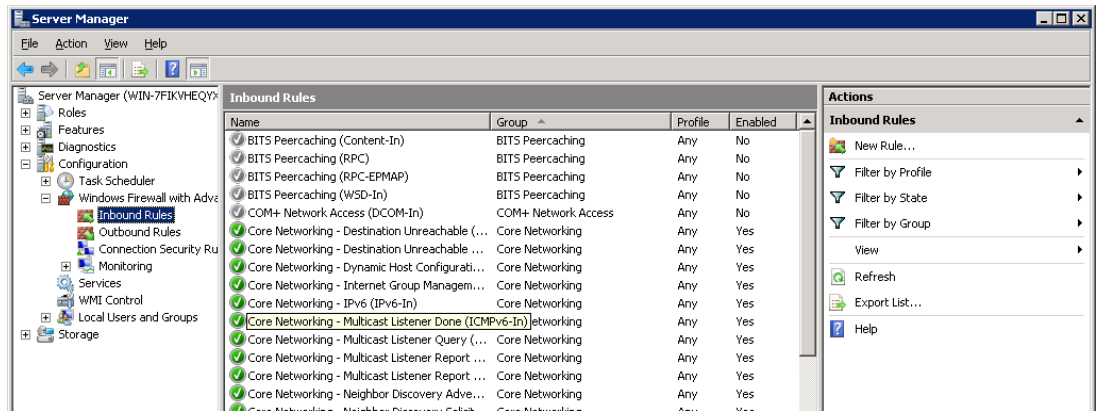


Configuration of Windows Firewall on Windows Server 2008

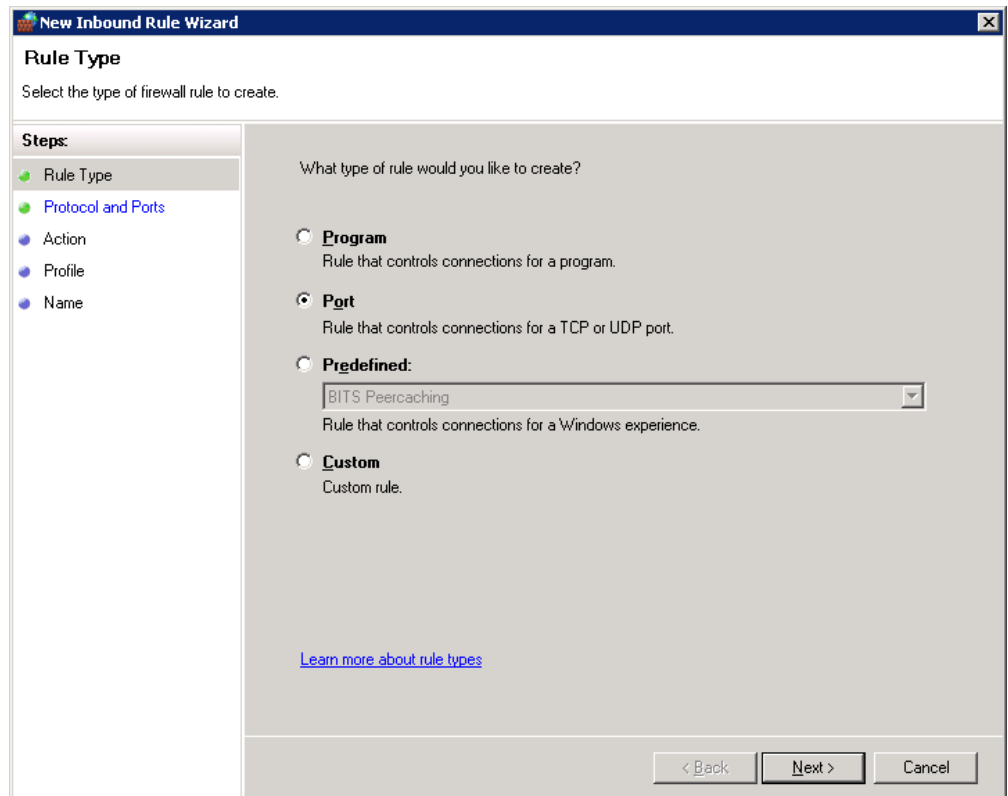
- Right click on My Computer and select Manage.
- Expand Configuration to see Windows Firewall with Advance Settings.
- Expand Windows Firewall with Advance Settings to see Inbound Rules.



- Select *Inbound Rules*.
- Click *New Rule*.

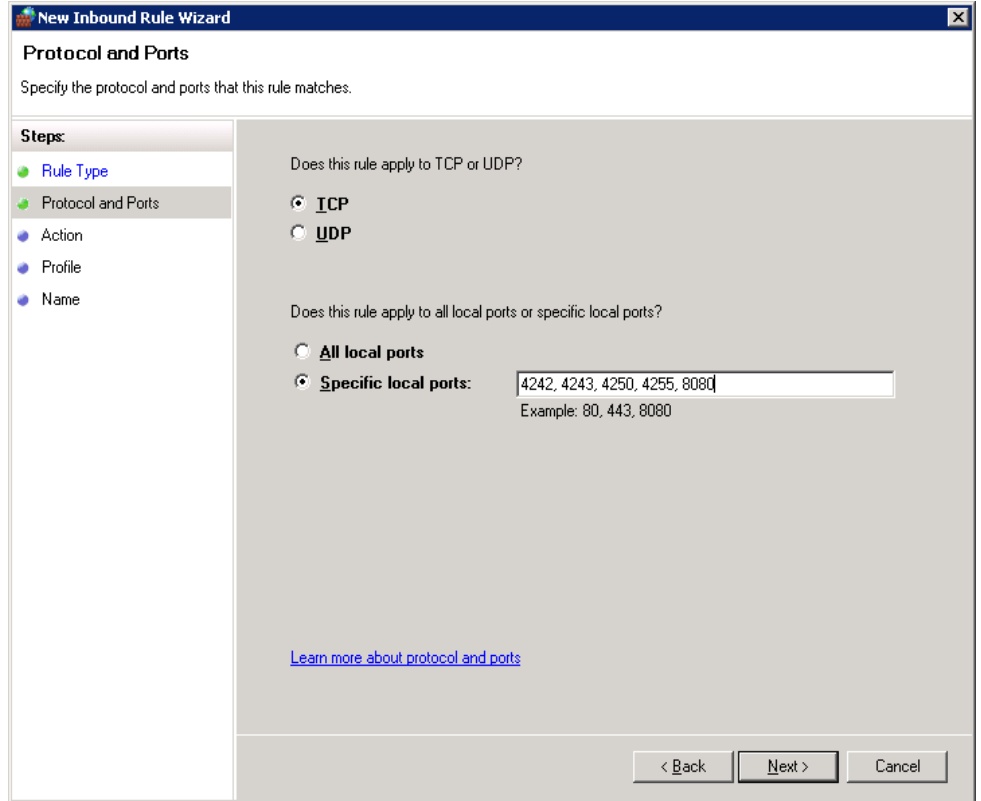


- Select *Port* and click next.

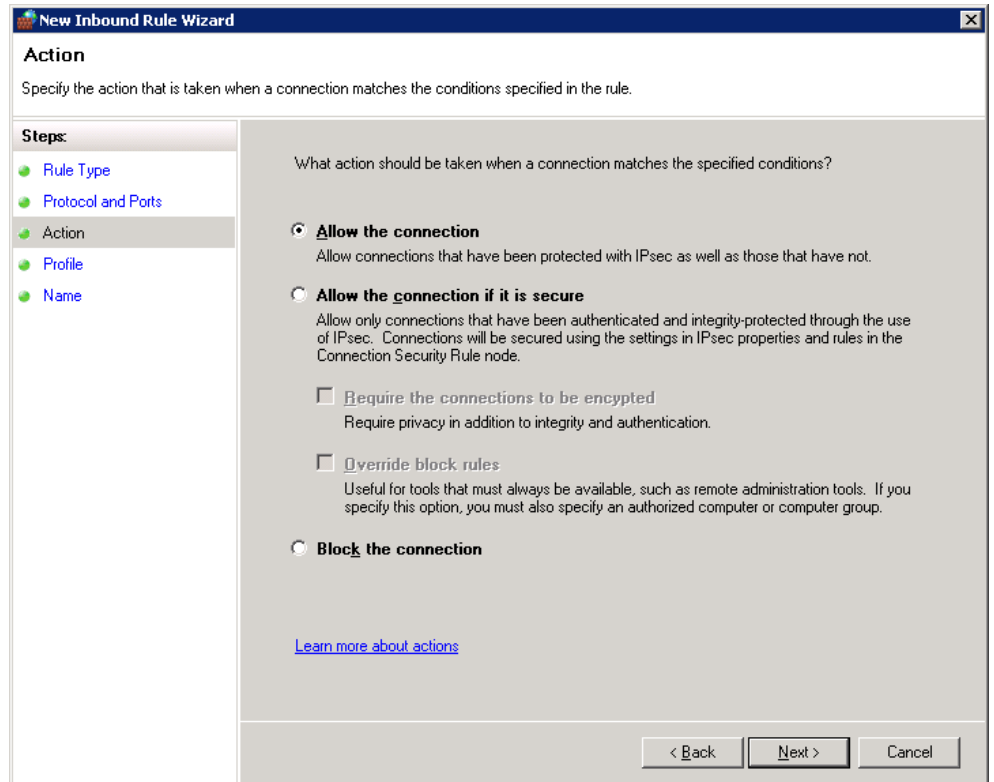


- Enter in the following ports as *Specific Local Ports* and click next.
 - a. 4242 – Data
 - b. 4243 –Command
 - c. 4250 – Config Server
 - d. 4255 – Admin Service
 - e. 8080 – Web Server*

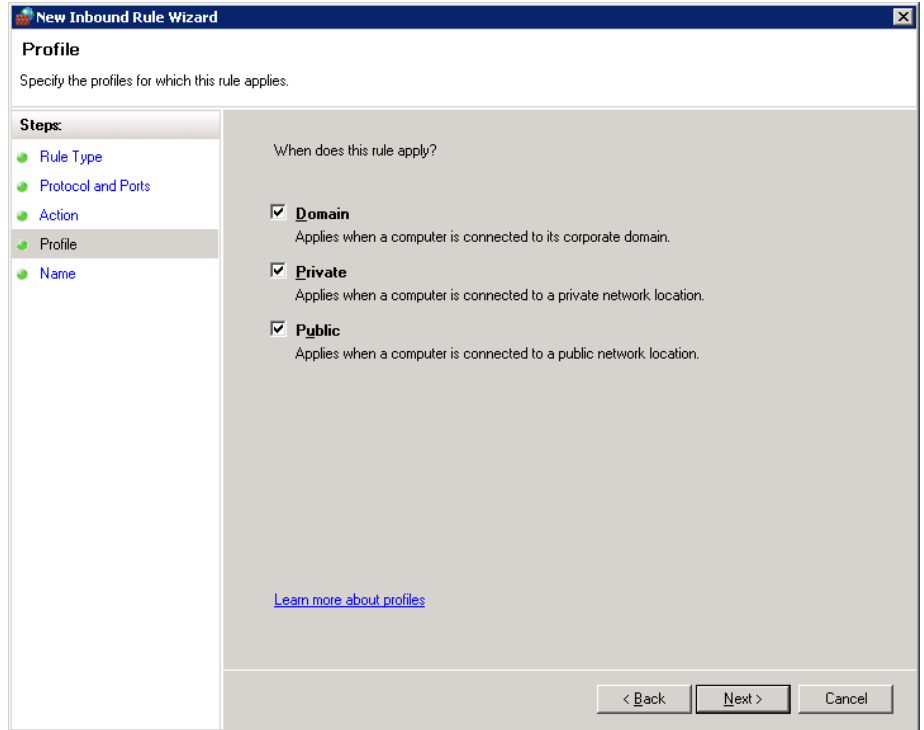
*Optional



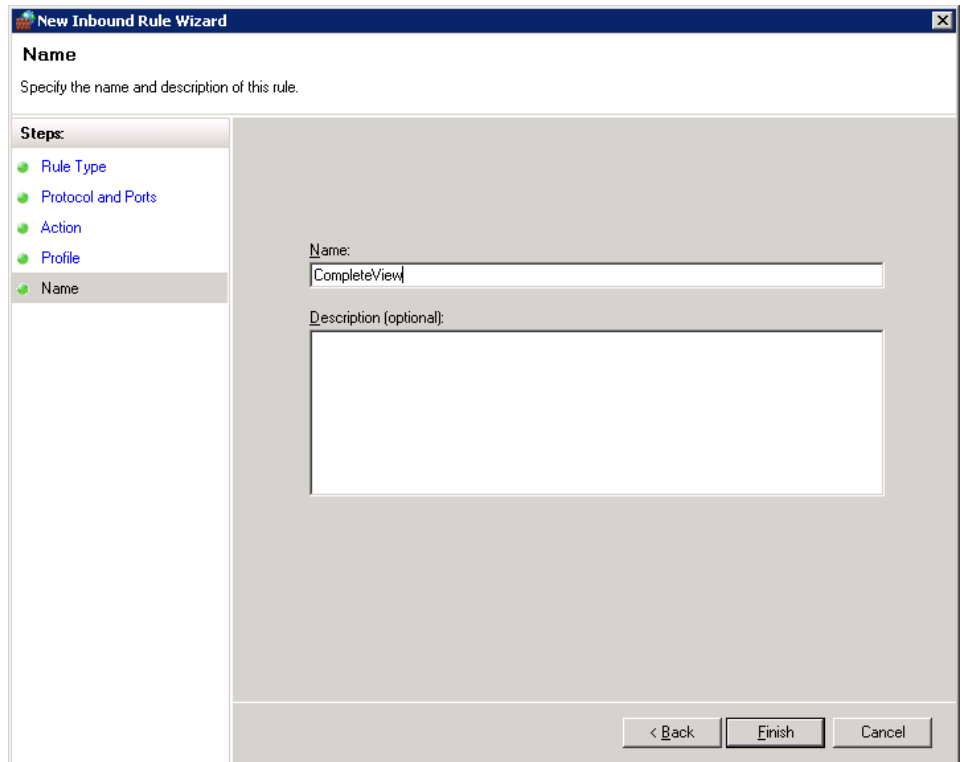
- Select *Allow the connection and click Next.*



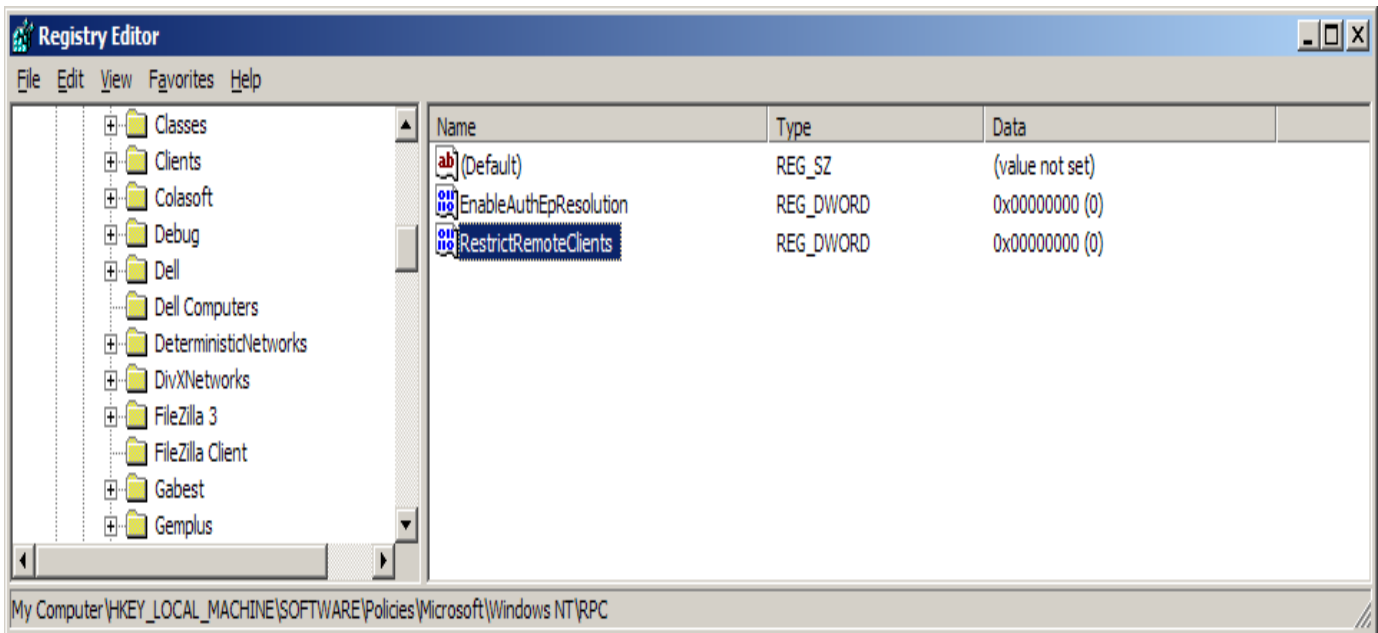
- Select which network types apply to this rule and click next. If you are not sure, select all.



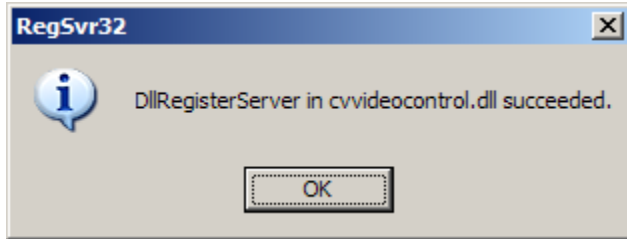
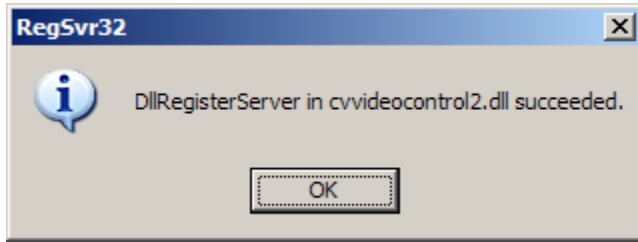
- Name the rule CompleteView and click Finish.



4. If you are still not able to connect to the Web Client, check the following Registry settings on the server.
 - a. Click on the *Windows Start Button*, select run, and type **regedit**.
 - b. Navigate to HKeyLocalMachine/software/Policies/Microsoft/Windows NT/RPC
 - c. If RPC is present, confirm the following words are listed:
 EnableAuthEpResolution
 RestrictRemoteClients
 - d. If they are not present, please add them by clicking on edit and selecting new key value.
 - e. If they are present, confirm they have a value of 0.
 - f. If they are not present, please add them by clicking on edit and selecting new dword value. Once they are added, confirm that both words have a value of 0.
 - g. Once you have confirmed the registry settings, please try and reconnect to the web client and reinstall the Active X Control.



5. If you are still not able to connect to the Web Client from a separate workstation, you can copy two files from the server to the client machine.
 - a. These two files are located in `C:\Program Files\CompleteView\WebClient`, on the server. The two files you need to copy are:
 - i. **CVVideocontrol.dll**
 - ii. **CVVideocontrol2.dll**
 - b. Once you have copied both of these files, create a folder on the workstation named WebClient in the `C:\Program Files\CompleteView` directory and copy two .dll files into this folder.
 - c. Next, right click on the .dll files and select Open with. Navigate to `C:\Windows\System32\` and select `regsvr32.exe`.
 - d. Double click on the .dlls and you will see the following messages.



6. If you can still not connect to the web client, please contact Salient Support via email at support@salientsys.com.