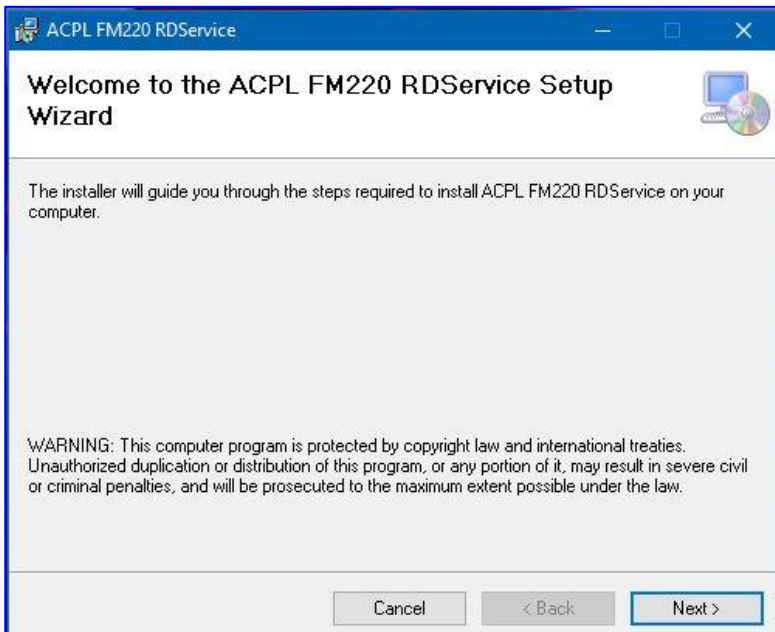


INSTALLATION GUIDE FOR ACPL FM220 RD WINDOWS APPLICATION

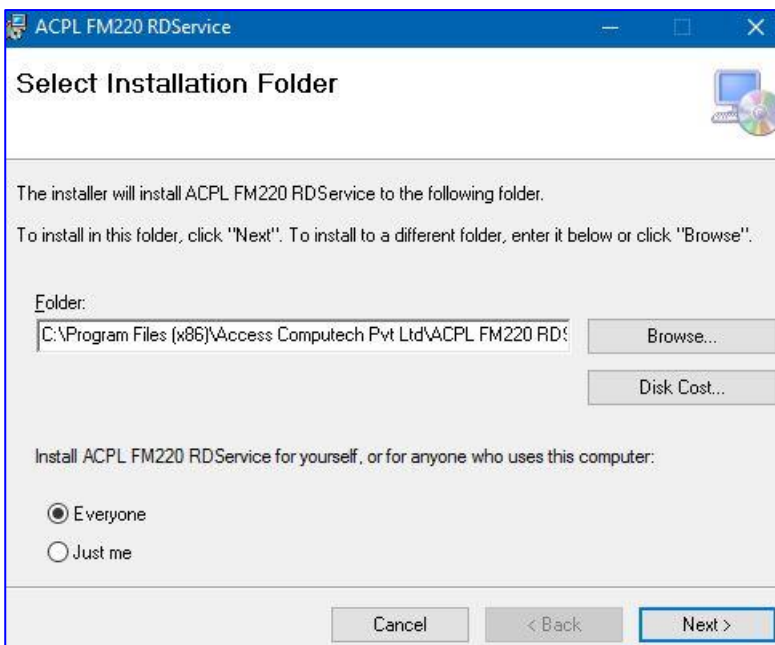
INDEX

CONTENT	PAGE No.
Setup FM220 RD Service	2
Setup FM220 RD Service Support Tool	5
Instructions to enable HTTPS in RD Service	8
RD Service troubleshooting for HTTPS	11
Instructions to configure proxy settings in RD Service	14
Basic functionality of RD Service	17
Allow RD Service communication in Antivirus Programs	20

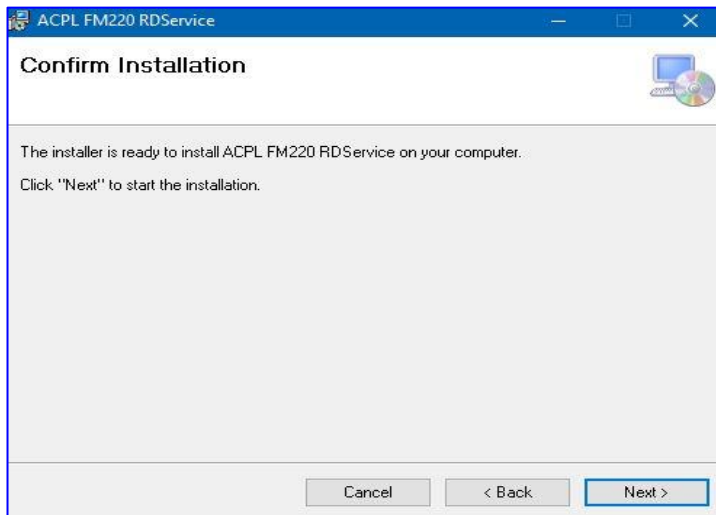
1. **SETUP FM220 RD SERVICE:**



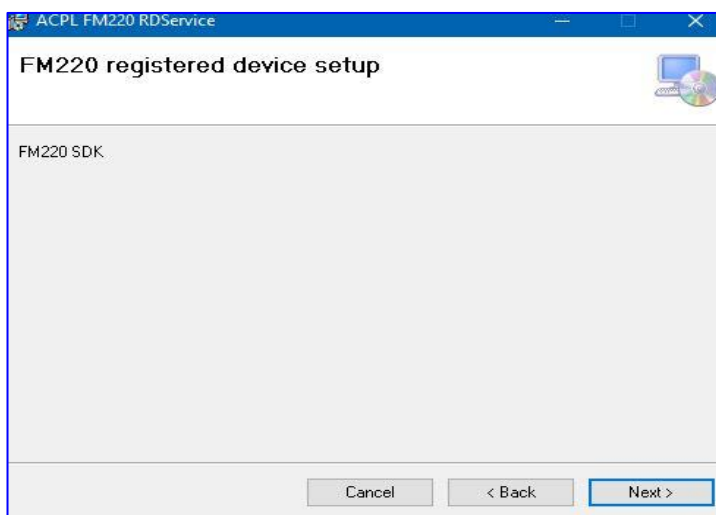
Download Windows Certified RD service from <http://acpl.in.net/RdService.html>? Link and download Windows Certified RD service



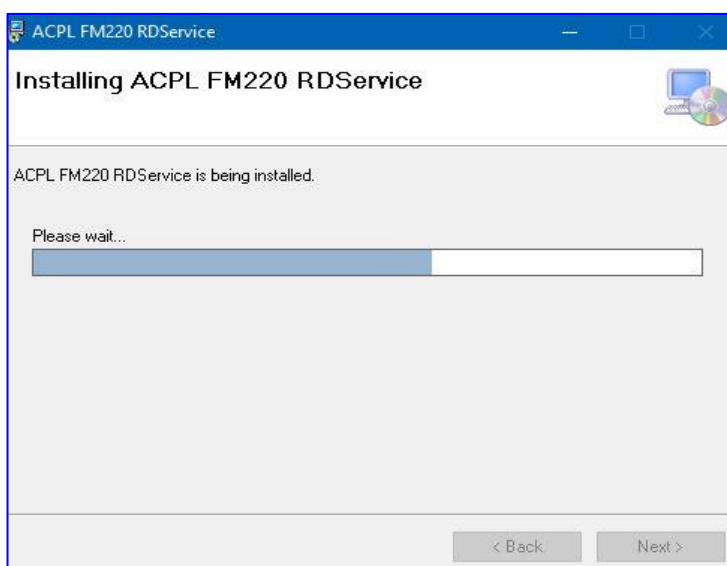
Click on Next and select installation folder.



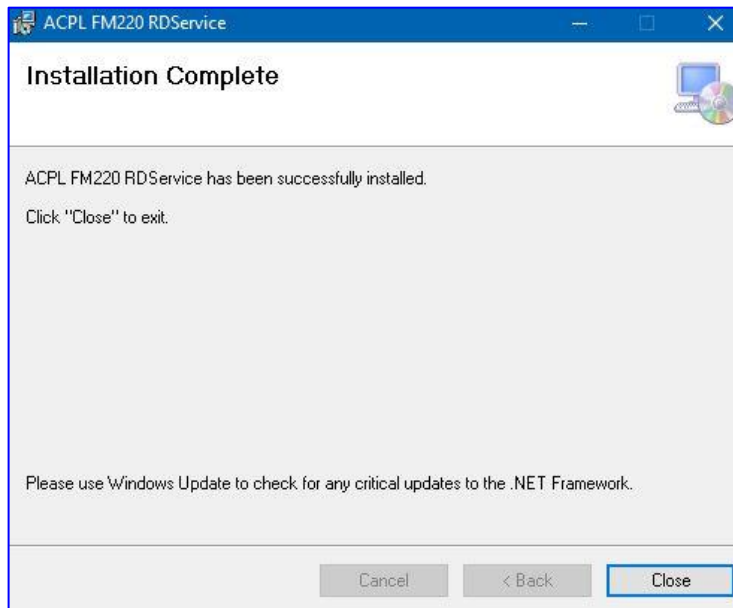
Click Next button for Confirm to Start Installation.



Click Next and wait for RD setup to start.

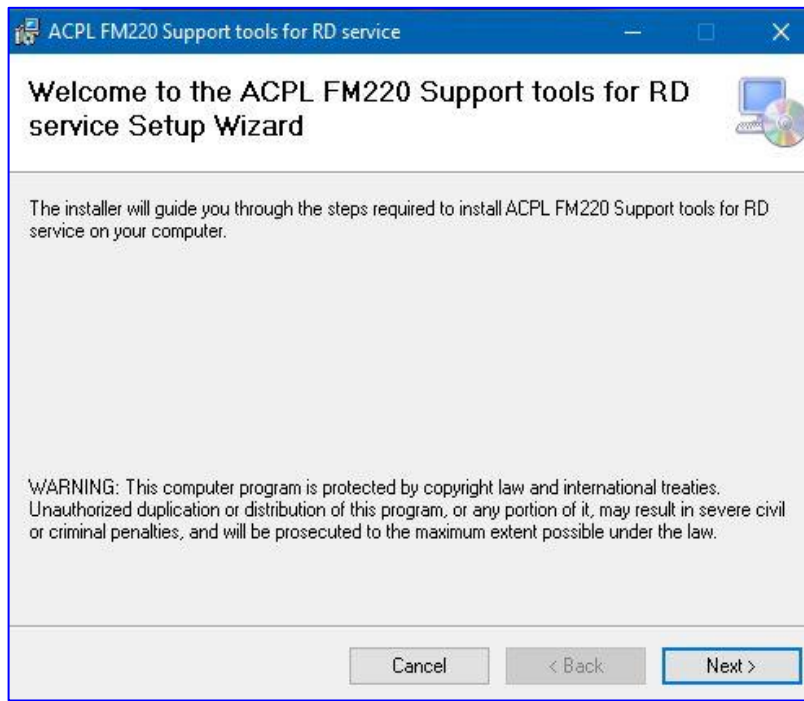


Wait to install all necessary files.

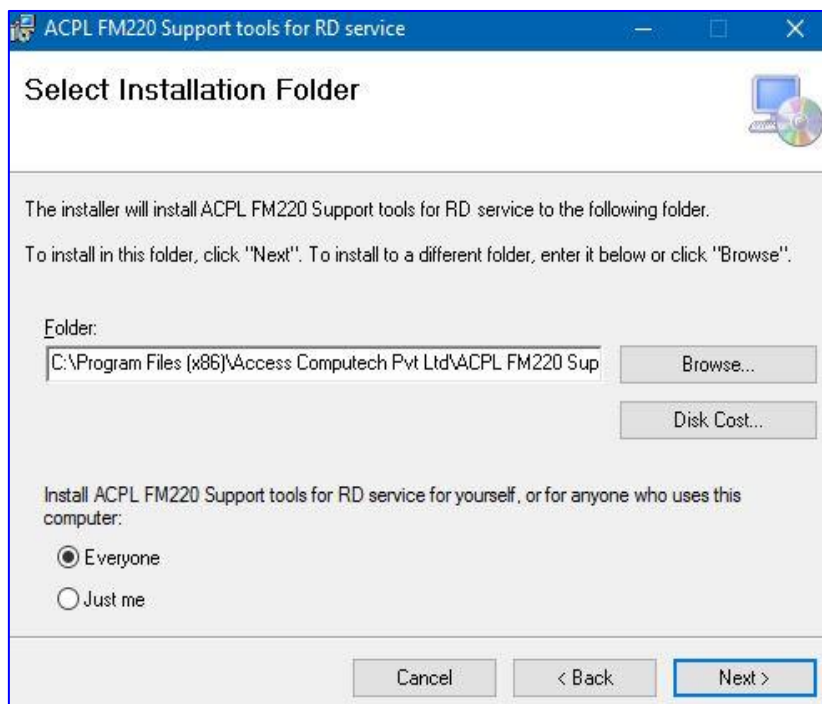


Click on Close button for Exit.

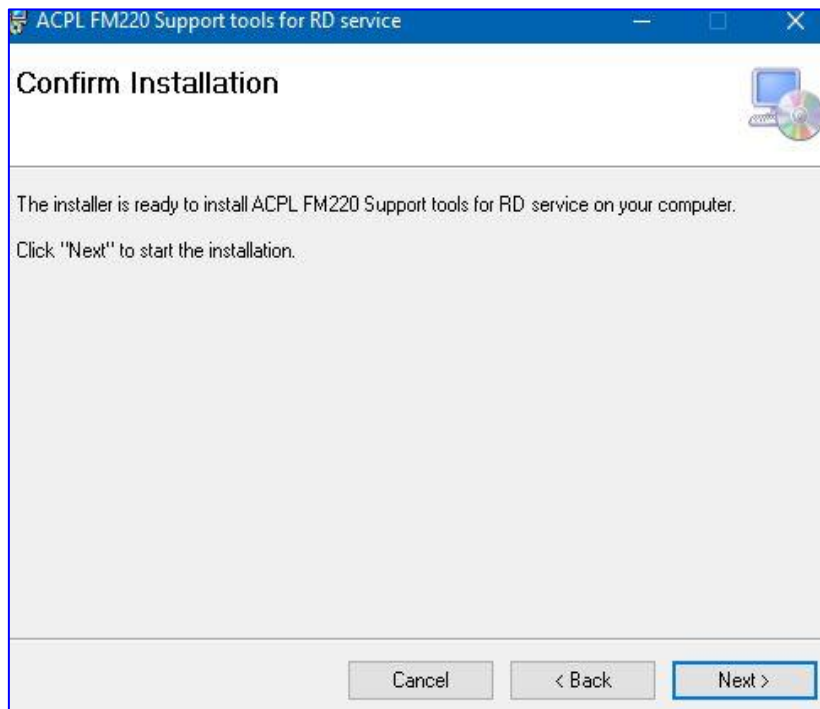
2. SETUP FM220 RD SERVICE SUPPORT TOOLS:



Download Windows Support Tools from <http://acpl.in.net/RdService.html?> Link and download Windows support tools



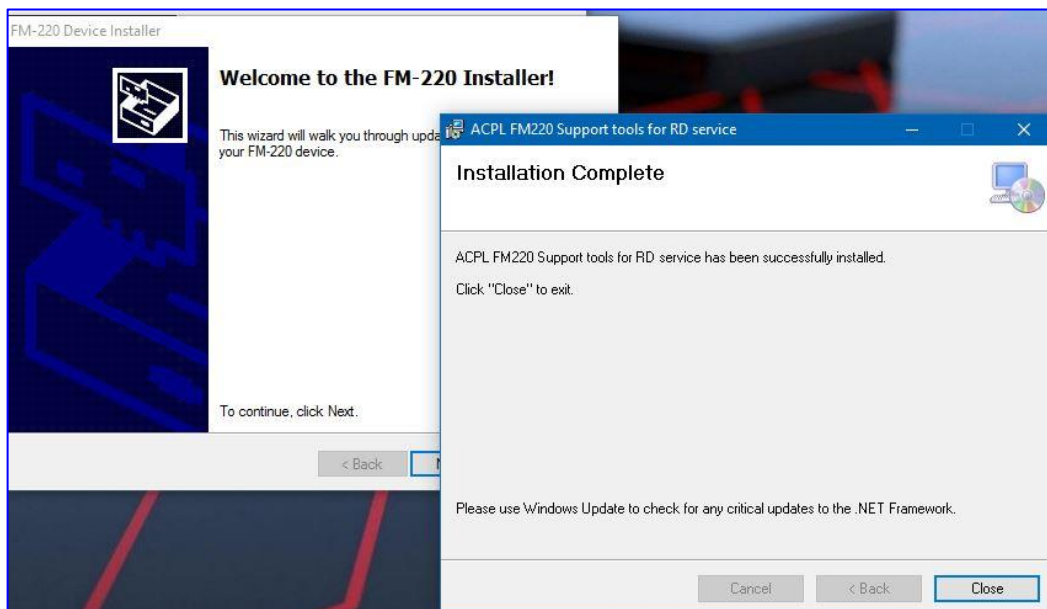
Click on Next button and Select installation folder. After selection, again click on Next button.



Confirm installation and click next to start further installation.

After clicking on next button, it will display message that your application is installed, click on close button for exit.

After installation, it will display automatic FM220 Device Installer.





Click on next and wait
For device drivers to
Install in your PC.



If drivers is successfully
installed in your PC,
then it will display
device status as
“Ready to use”.

If drives is not installing
In your PC, then it will
Display device status as
“Device driver Failed”.

3. INSTRUCTIONS TO ENABLE HTTPS IN RD SERVICE: **(Only if you want to use different port for HTTPS** **Otherwise it will support HTTPS on same port which is on** **HTTP)**

If you wanted to listen RD Service on HTTPS protocol, then please follow instructions described below.

If you want to check whether RD Service is listening through HTTPS protocol, then go to following link:

http://acpl.in.net/fm220_entry/RD_Service_Call_HTTP.aspx

If HTTPS is not configured in RD Service then follow instructions.

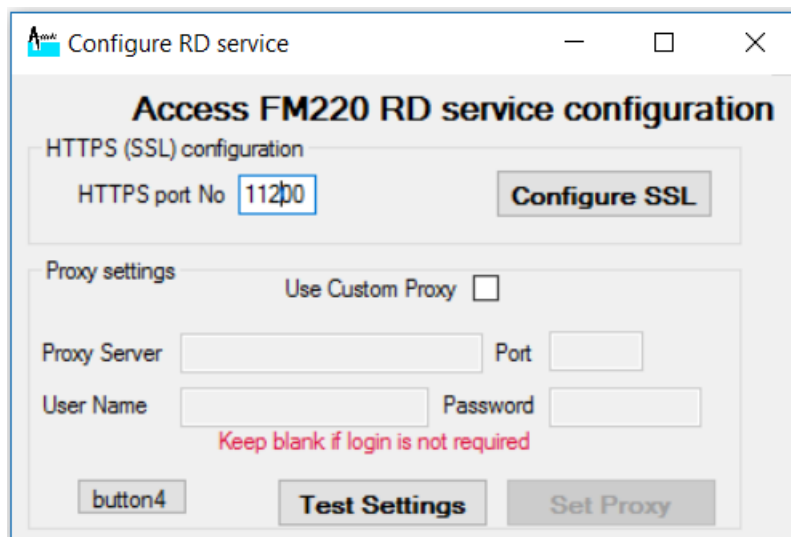
For enabling HTTPS in RD Service please go to following path and open application named “**Config ACPL RD service.exe**”. **Open this application as Administrator**. Follow instructions for further process:

PATH: `C:\Program Files (x86)\Access Computech Pvt Ltd\ACPL FM220 Support tools for RD service\`

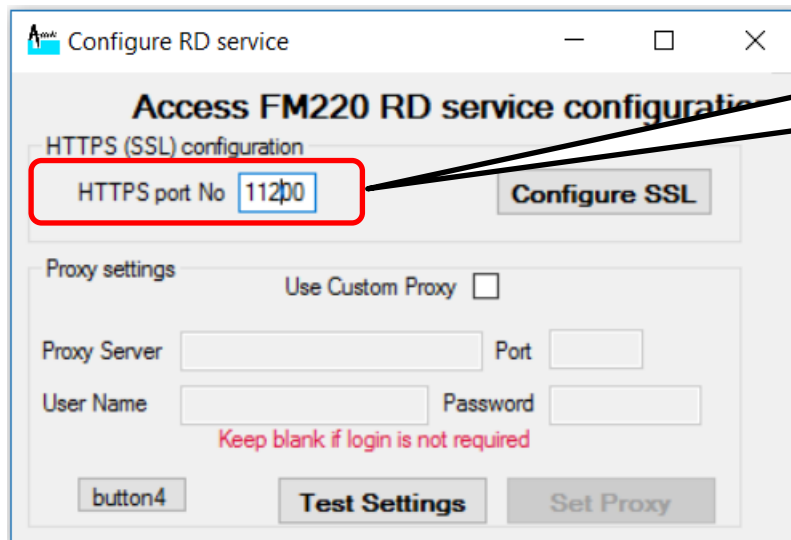
APP NAME: ` Config ACPL RD service.exe `

RUN MODE: `As Administrator

1. Application Console: -



2. Fill Port Number: -



Configure RD service

Access FM220 RD service configuration

HTTPS (SSL) configuration

HTTPS port No 11200 **Configure SSL**

Proxy settings Use Custom Proxy ☐

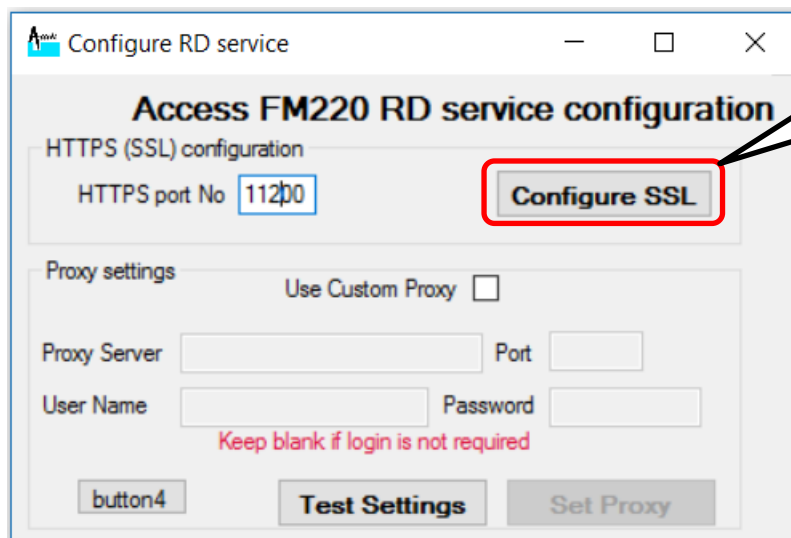
Proxy Server Port

User Name Password

Keep blank if login is not required

button4 **Test Settings** Set Proxy

3. Click on `Configure SSL` button: -



Configure RD service

Access FM220 RD service configuration

HTTPS (SSL) configuration

HTTPS port No 11200 **Configure SSL**

Proxy settings Use Custom Proxy ☐

Proxy Server Port

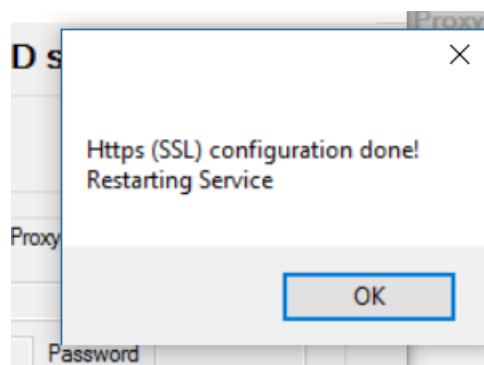
User Name Password

Keep blank if login is not required

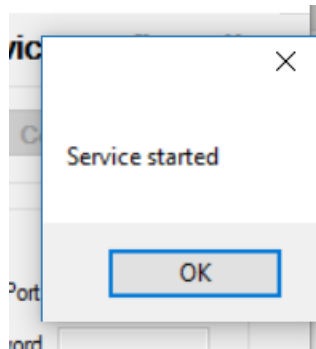
button4 **Test Settings** Set Proxy

4. Responses from application: -

➔ After clicking on `Configure SSL` button, it will show following response.



- ➔ **After above response, it will restart RD Service. So, please wait for restart and application response as following.**



4. RD SERVICE TROUBLESHOOTING WITH HTTPS:

➔ In case of WINDOWS 8.1, if operating system is not updated, then RD Service cannot be connected through HTTPS. So, to enable HTTPS in this OS please follow below instructions.

(These instructions are for 64-bit OS. You can search same for 32-bit.)

Please find links to download updates for enabling the HTTPS RD Calls into WIN 8.1 64 Bit version.

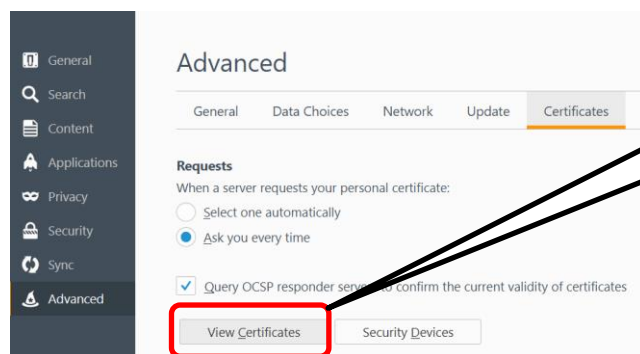
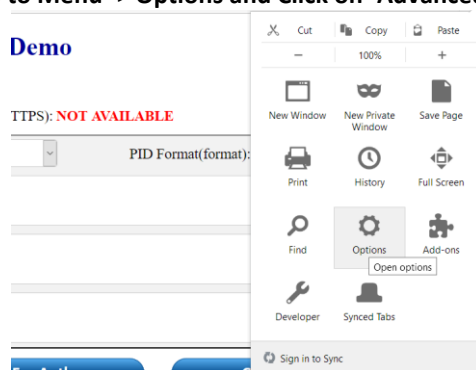
Please Install them in order shown below.

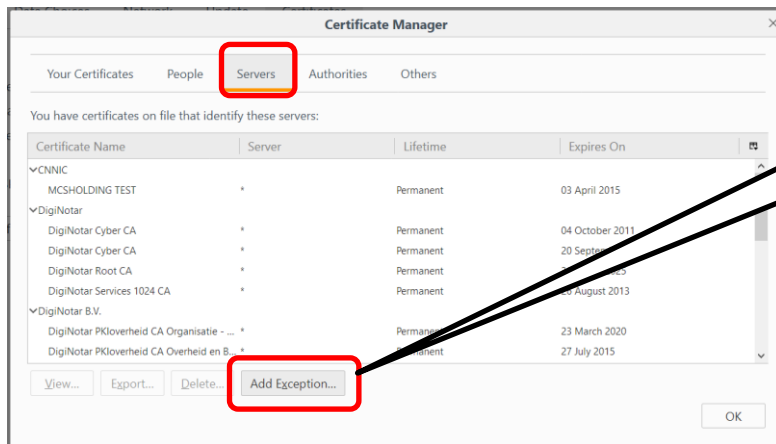
1. Please Download and Install UPDATE File: - **Windows8.1-KB3021910-x64.msu (NO RESTART)**
<https://www.microsoft.com/en-us/download/details.aspx?id=46809>
2. After 1st step and RESTART please download and install UPDATE File: -
Windows8.1-KB2919355-x64.msu (RESTART REQUIRED)
<https://www.microsoft.com/en-us/download/details.aspx?id=42335>
3. After 2nd step and RESTART please download and install UPDATE File: -
Windows8.1-KB3172614-x64.msu (RESTART REQUIRED)
<https://www.microsoft.com/en-us/download/details.aspx?id=53334>

➔ In case of Firefox browser, RD Service cannot be connected through HTTPS. So, to enable HTTPS in Firefox browser please follow below instructions.

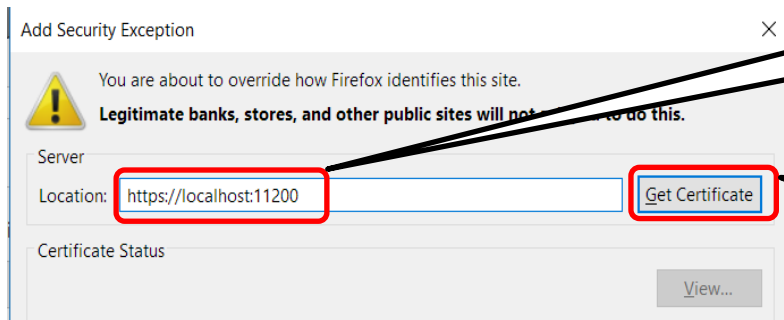
Open Firefox browser and follow below instructions:

Go to Menu -> Options and Click on 'Advanced' tab.



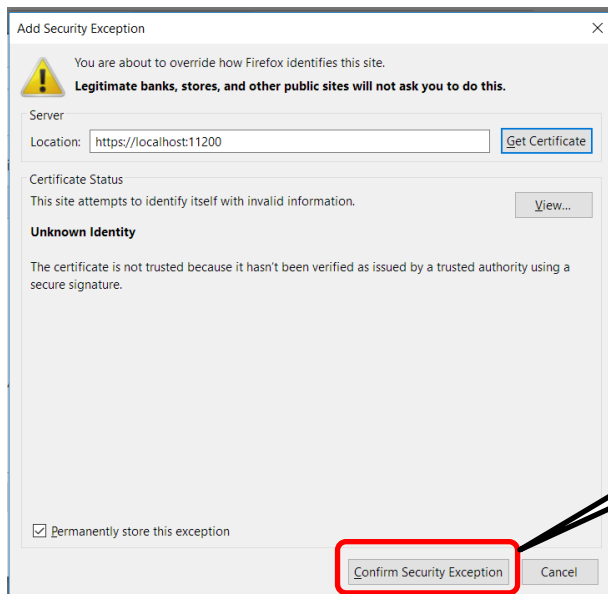


In 'Servers' Tab, click on 'Add Exception'



Default location of FM220 RD Service

Enter Location of RD Service and click on 'Get Certificate' button



Click on 'Confirm Security Exception' button

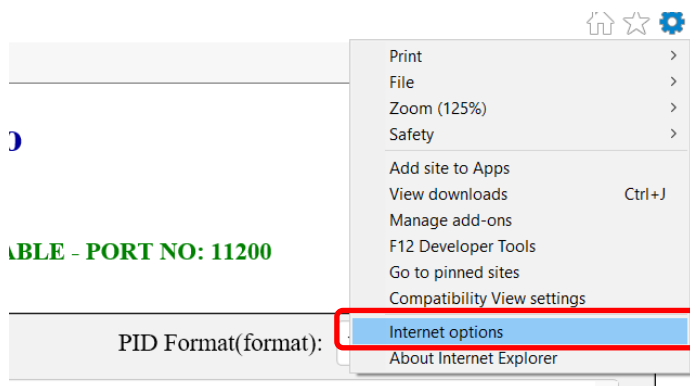
After all steps, you will be able to see the entry in 'server' tab



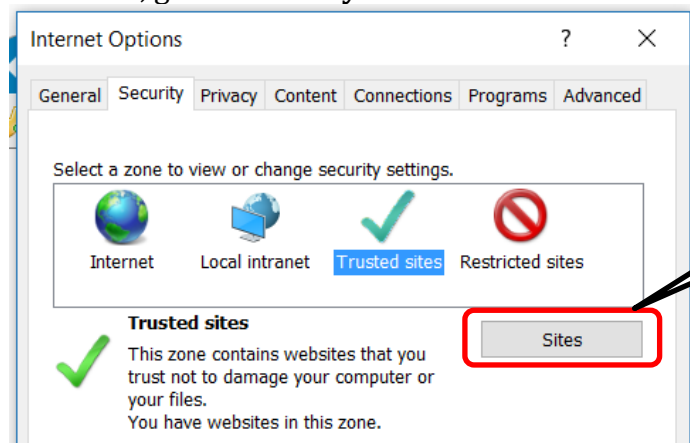
Refresh your web page from which you are calling RD Service.

➔ In case if HTTPS is also not working in IE, you can follow below instructions.

You can add your website into trusted web sites list to enable HTTPS.

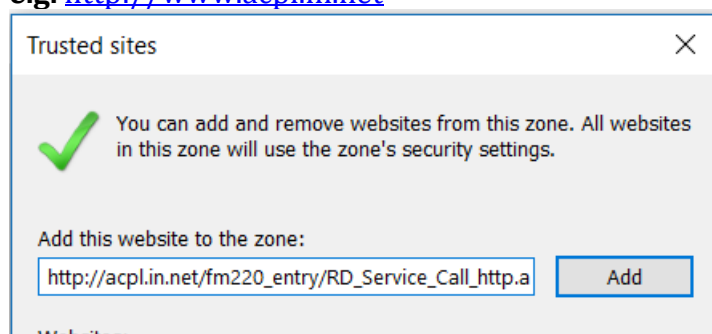


After that, go to `Security` tab and click on `Trusted Sites`.



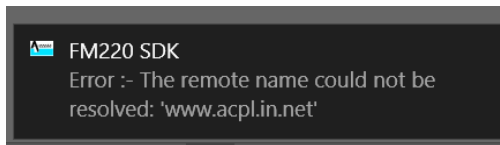
You can add your web site address from where you are going to call RD Service functionalities.

e.g. <http://www.acpl.in.net>

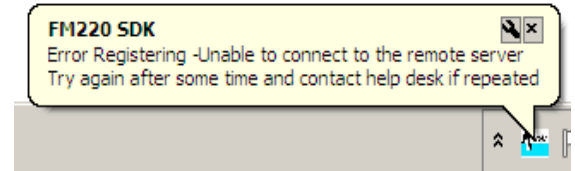


5. INSTRUCTIONS TO SET PROXY SETTINGS IN RD SERVICE:

If your internet running through proxy and you are getting following error while registering FM220 device in RD Service, then please follow instructions described below.



OR



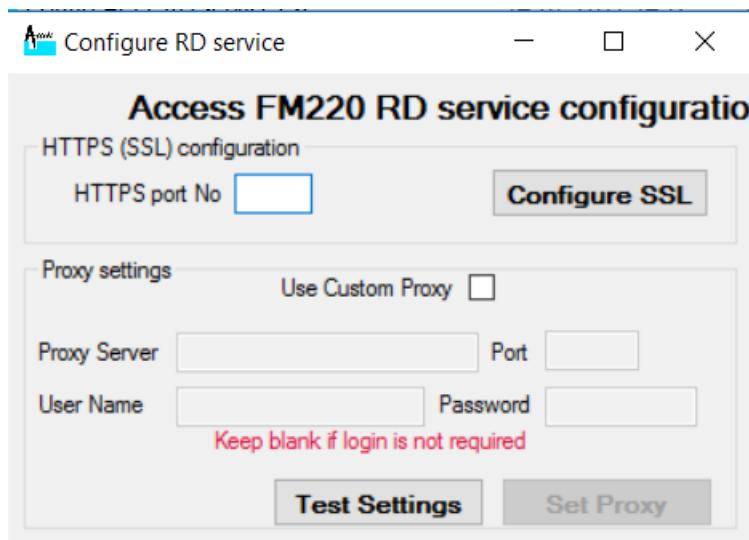
For enable proxy in RD Service please go to following path and open application named “**Config ACPL RD service.exe**”. **Open this application as Administrator**. Follow instructions for further process:

PATH: `C:\Program Files (x86)\Access Computech Pvt Ltd\ACPL FM220 Support tools for RD service\`

APP NAME: ` Config ACPL RD service.exe `

RUN MODE: `As Administrator`

1. Application Console: -



2. Fill Proxy Details: -

Configure RD service

Access FM220 RD service configuration

HTTPS (SSL) configuration

HTTPS port No **Configure SSL**

Proxy settings

Use Custom Proxy ☒

Proxy Server Port

User Name Password

Keep blank if login is not required

Test Settings **Set Proxy**

Check the box for
`Use Custom Proxy`

Enter Proxy Server
IP and Port Number

Enter Proxy Username and
Password if required.

3. Click on `Test Settings`: -

Configure RD service

Access FM220 RD service configuration

HTTPS (SSL) configuration

HTTPS port No **Configure SSL**

Proxy settings

Use Custom Proxy ☒

Proxy Server server ip Port port no.

User Name Password

Keep blank if login is not required

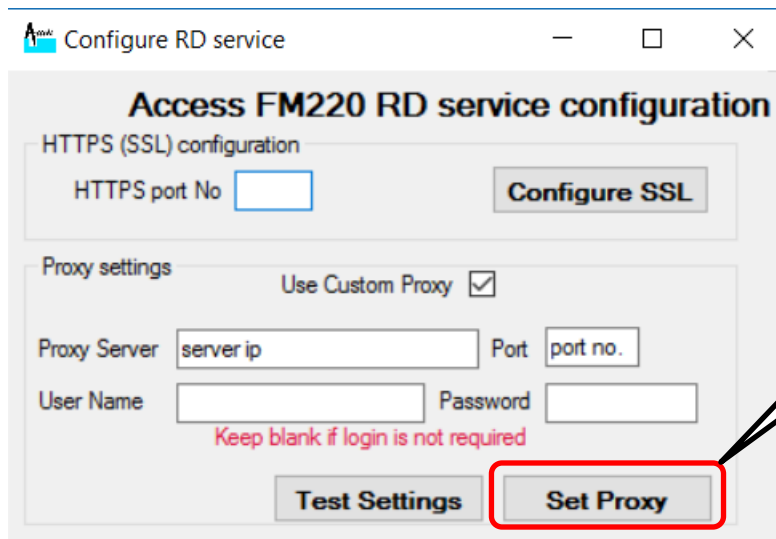
Test Settings **Set Proxy**

After inserting
details please click
on `Test Settings`

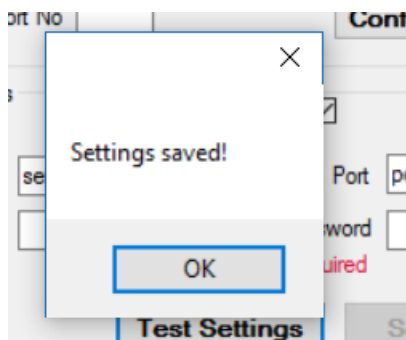
Success!

OK

4. Click on `Set Proxy`: -



After that please
click on `Set Proxy`



It will take some time to restart the service.

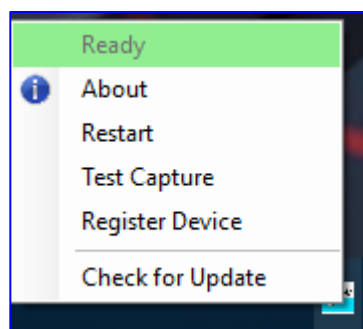
If any other error raises at time of registration, like `Device data not available` or `Device is blocked` or `Subscription Expired` etc., then please contact our support.

6. INSTRUCTIONS TO CHECK FOR ACPL FM220 REGISTERED DEVICE SERVICE: **(Basic Functionality)**

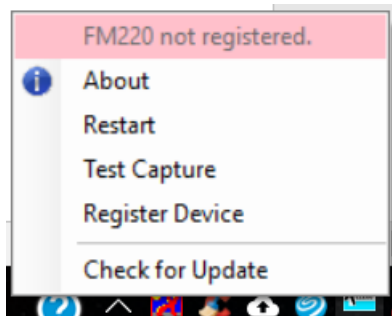
1. On your desktop, click Start > Run.
2. On the Open field, type **services.msc** and then click **OK**. The Services console pops up, listing all services that are installed on the computer.
3. Check for ACPL FM220 Registered Device service if it is started or not (Default Start)



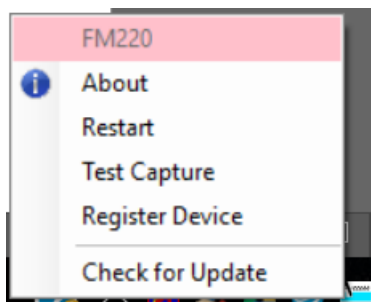
4. If service started then please check task bar for Icon
5. Right click on Icon and check if your device is ready or not.
6. If Service is running and device is connected and registered, then ready status will display with green colour.



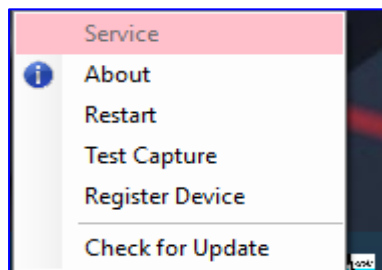
7. If Service is running, Device is connected but, Device is not registered, then following status will be displayed.



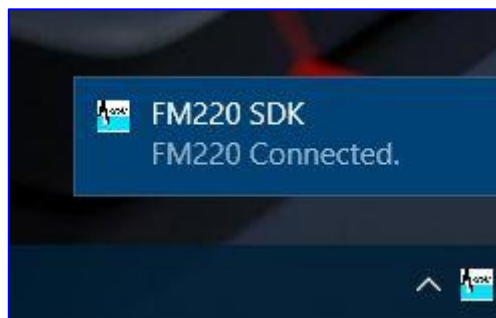
8. If Service is running and device is not connected then following status will be displayed.



9. If Service is stopped, then it will display in Red colour.



10. Whenever FM220 Device is connected to PC, it will display notification



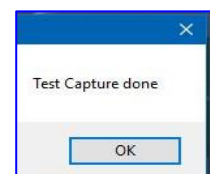
11. Now click on “Test Capture” option from menu to test device. It will display image as below



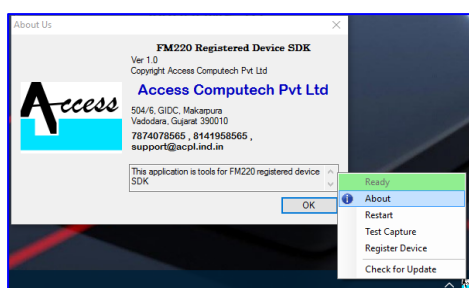
Now, click on “Capture Finger” button and put your finger on device for fingerprint. After taking fingerprint, click on submit button and again capture another finger in same manner.



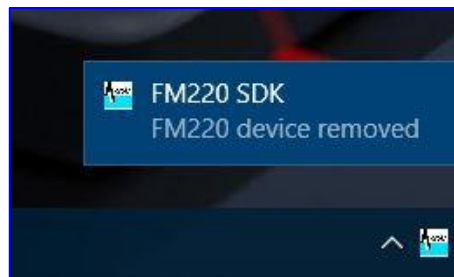
12. After successful enrolment of finger print, it will display message :



13. Click on “About” option from menu for information about application.



14. Whenever you remove FM220 Device from your PC, it will display Notification as

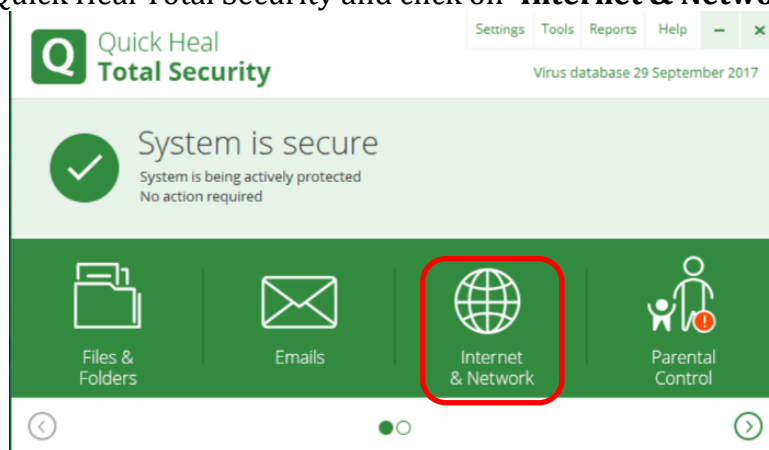


7. ALLOW RD SERVICE COMMUNICATION IN ANTIVIRUS PROGRAMS:

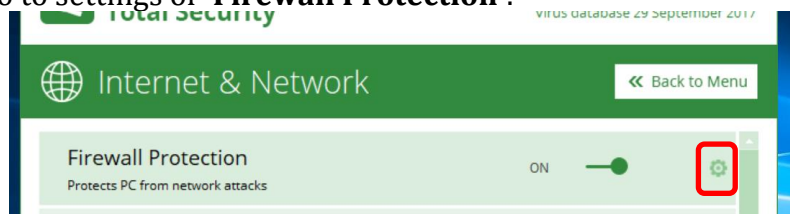
→ Quick Heal:

i. Enable ports for HTTP:

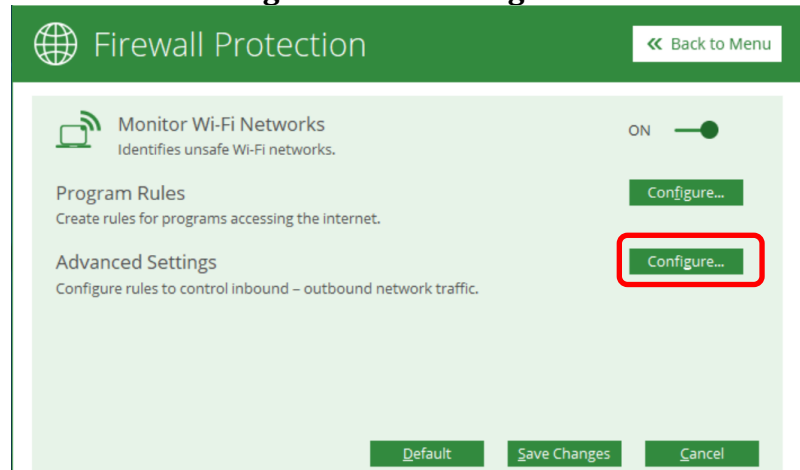
Open Quick Heal Total Security and click on '**Internet & Network**'.



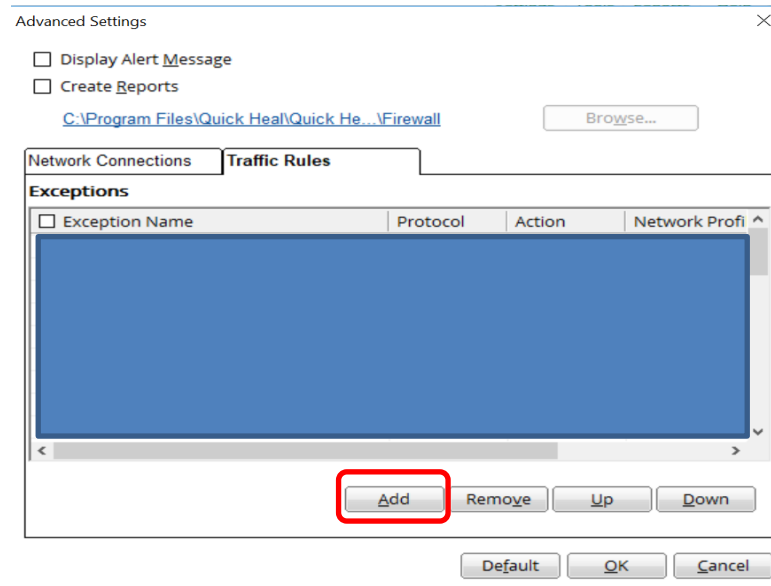
Now go to settings of '**Firewall Protection**'.



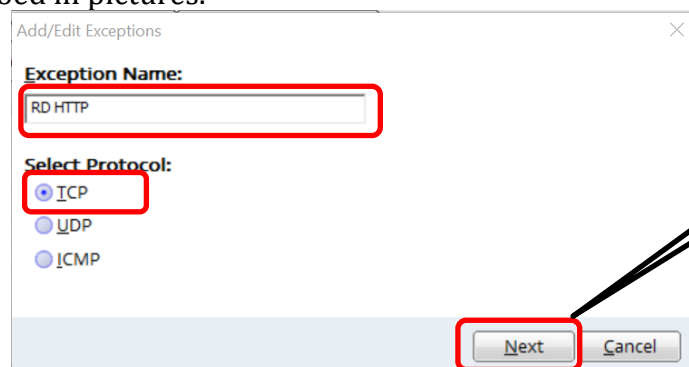
Now in **'Advanced Settings'** click on **'Configure'**.



Now in **'Traffic Rules'** click on **'Add'**.



Now follow described steps below as pictures and enter values same as described in pictures.



Add/Edit Exceptions

Local IP Address:

☒ Any IP Address:

☐ IP Address: . . .

☐ IP Address Range

Start IP Address: . . .

End IP Address: . . .

Back Next Cancel

Click 'Next'

Add/Edit Exceptions

Local TCP/UDP Port:

☐ All Ports

☐ Specific Port(s): Use comma (,) in between to enter multiple ports.

☒ Port Range

Start Port: 11100

End Port: 11120

Back Next Cancel

Click 'Next'

Add/Edit Exceptions

Remote IP Address:

☒ Any IP Address:

☐ IP Address: . . .

☐ IP Address Range

Start IP Address: . . .

End IP Address: . . .

Back Next Cancel

Click 'Next'

Add/Edit Exceptions

Remote TCP/UDP Port:

☐ All Ports

☐ Specific Port(s): Use comma (,) in between to enter multiple ports.

☒ Port Range

Start Port: 11100

End Port: 11120

Back Next Cancel

Click 'Next'

Add/Edit Exceptions

Select Action:

☒ Allow

☐ Deny

Network Profile:

☒ Home ☒ Public

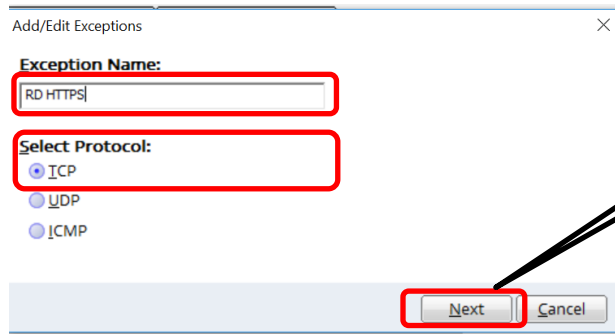
☒ Work ☒ Restricted

Back Finish Cancel

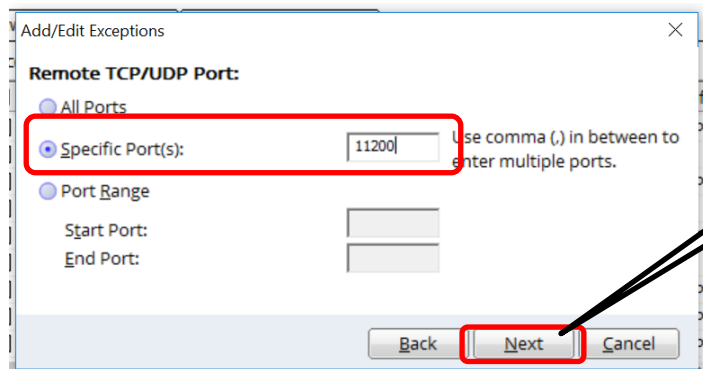
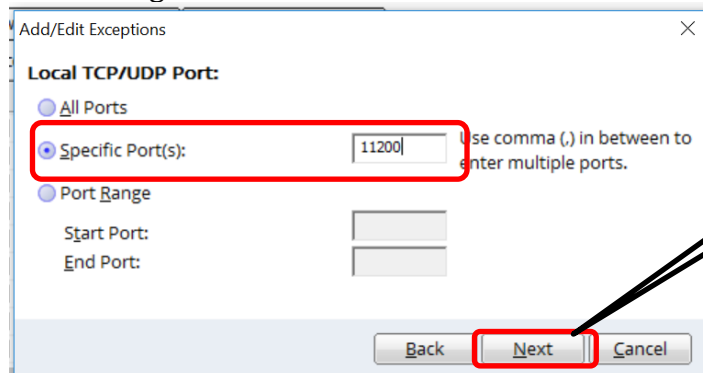
Click 'Finish'

ii. Enable port for HTTPS:

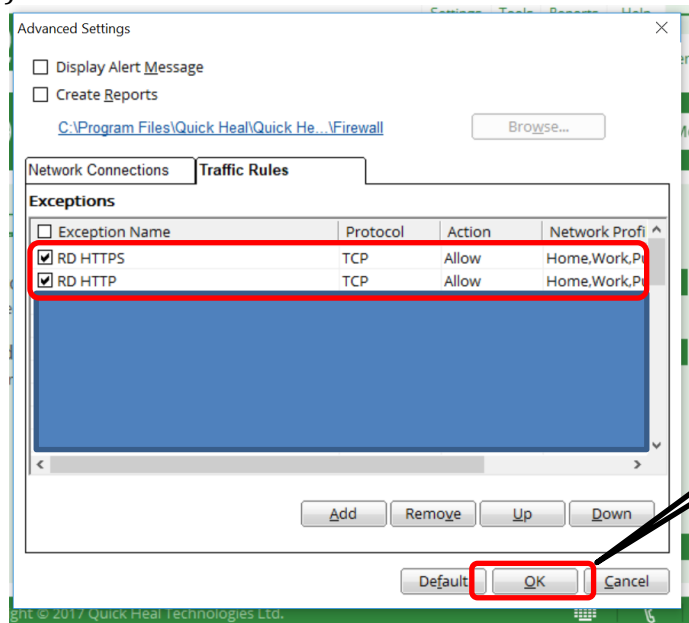
Enabling of HTTPS port is same as enabling of port in HTTP, described above. There is only change in rule name and port number please follow instructions as described in pictures.



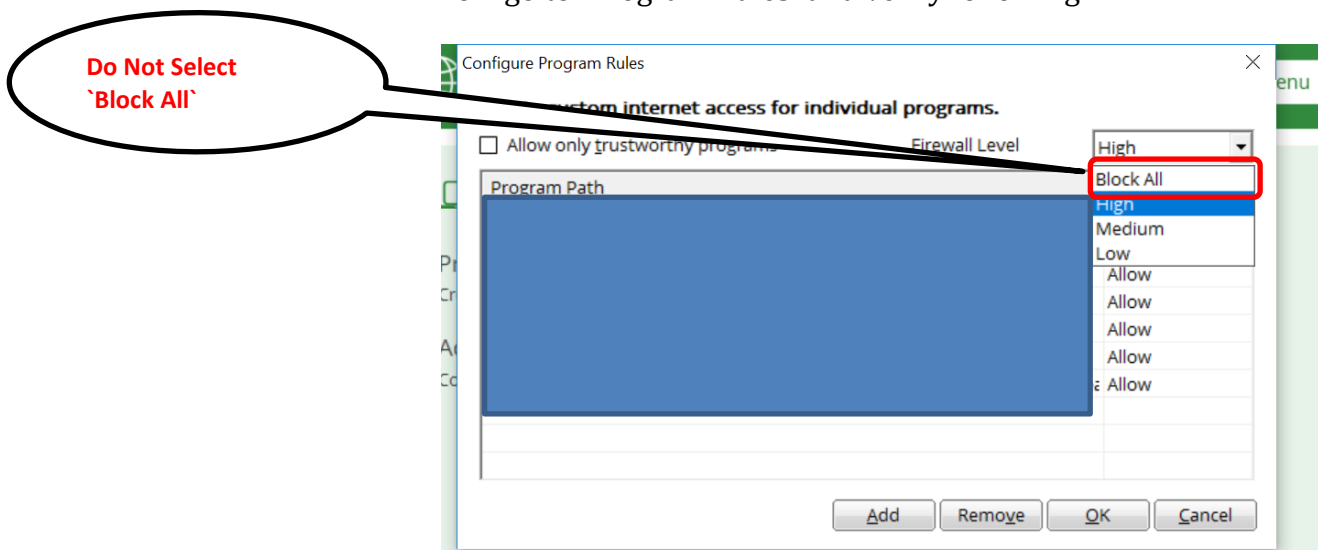
Other steps are same as above HTTP configuration. Only port number will change.



After completion of all steps you will be able to see all rules (HTTP and HTTPS).

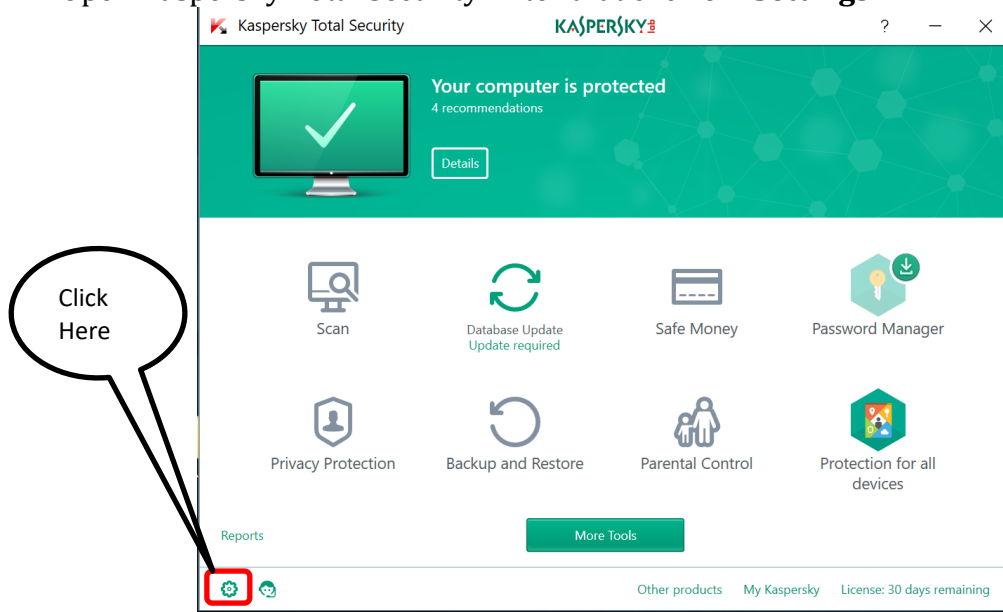


Now go to 'Program Rules' and verify following

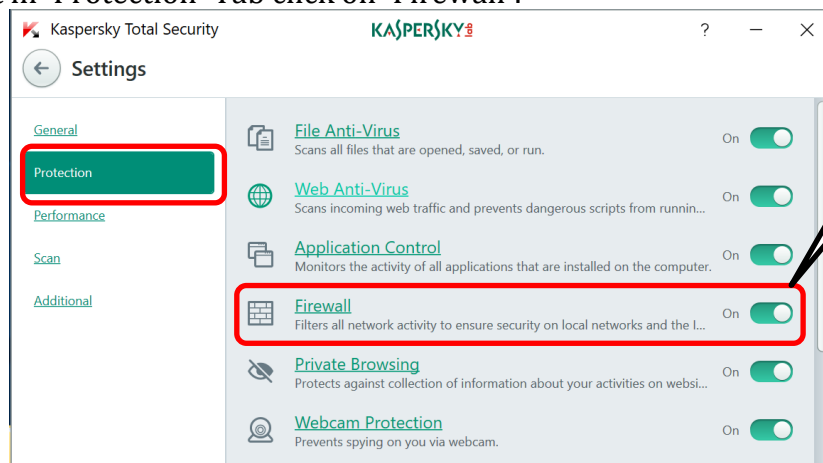


→ **Kaspersky:**

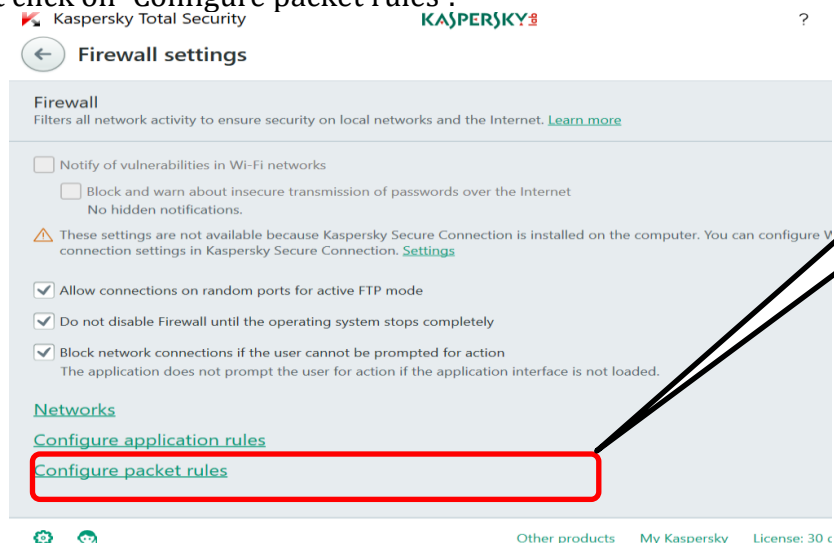
Open Kaspersky Total Security. After that click on `Settings`.



After that in `Protection` Tab click on `Firewall`.



After that click on `Configure packet rules`.



Now we will see, how to enable ports for HTTP and HTTPS.

i. Enable ports for HTTP & HTTPS:

In 'Packet Rules' windows click on 'Add'.

The screenshot shows the 'Packet rules' window. A table lists existing rules with columns for Name, Direction, Protocol, Action, and Status. The 'Add' button at the bottom right is highlighted with a red box and a callout bubble saying 'Click Here'.

Below the table, the 'Add' rule configuration form is shown with several fields highlighted by red boxes and callout bubbles:

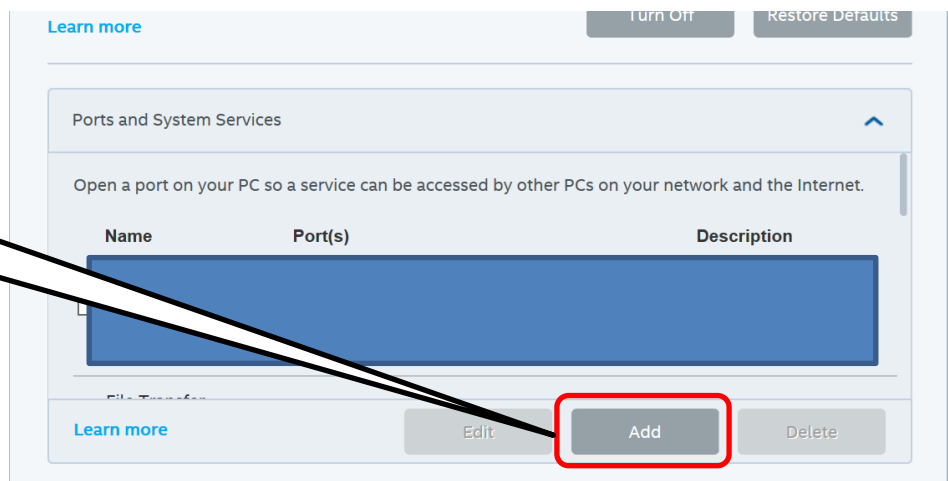
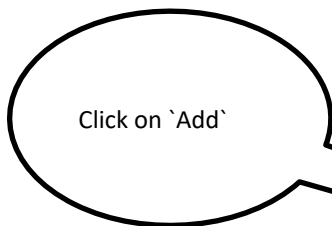
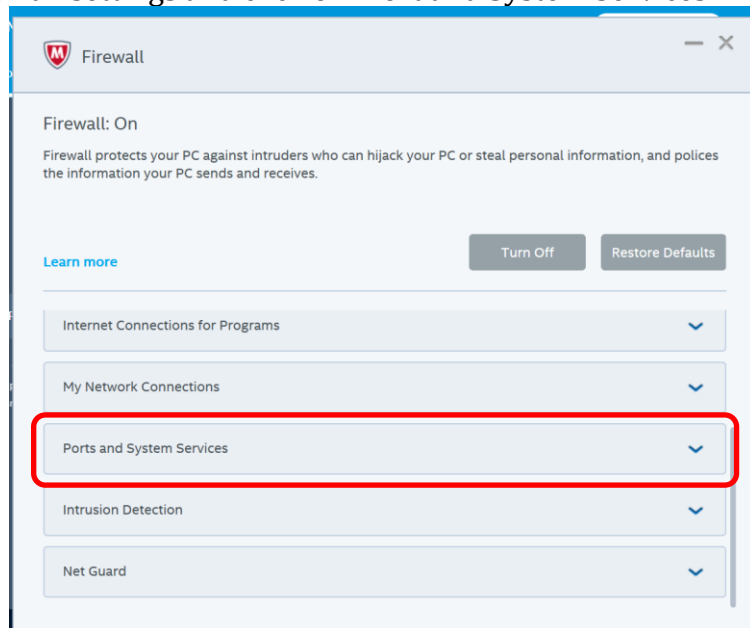
- Action:** Set to 'Allow'. Callout: 'Keep `Allow`'.
- Name:** Set to 'RD SERVICE HTTP'. Callout: 'Name for Rule. Different name in case of HTTPS'.
- Direction:** Set to 'Inbound/Outbound'. Callout: 'Keep direction both Inbound/Outbound'.
- Protocol:** Set to 'TCP'. Callout: 'Keep `TCP` protocol'.
- Remote ports:** Empty field.
- Local ports:** Set to '11100-11120'. Callout: 'Here HTTP Ports: `11100 – 11120` FOR HTTPS CHANGE IT TO: `11200`'.
- Address:** Set to 'Any address'.
- Status:** Radio buttons for 'Active' (selected), 'Inactive', and a checkbox for 'Log events'.

At the bottom, the 'Save' button is highlighted with a red box and a callout bubble saying 'After setting all values click on `Save`'.

→ **MCAFEE:**

Open McAFEE security program.

Go to Firewall settings and click on 'Port and System Services'.



Now we will see how to configure HTTP and HTTPS ports.

Description for Rules.
Different in case of HTTPS

i. **Enable ports for HTTP & HTTPS:**

Ports and System Services

Open a port on your PC so a service can be accessed by other PCs on your network and the internet.

Add System Service Port

System Service Name: :PL FM220 Registered Device Service

System Service Category: RD Service Authentication

Service Description: This rule enable client to connect with RD Service through HTTP

[Learn more](#) **Save** Cancel

Click on 'Save'

Ports and System Services

4000-5000:

Local TCP/IP Ports: 11100-11120

Local UDP Ports:

Open ports to: All PCs

Forward activity to ☐ Yes

[Learn more](#) **Save** Cancel

Here HTTP Ports: `11100 – 11120`
FOR HTTPS CHANGE IT TO: `11200`

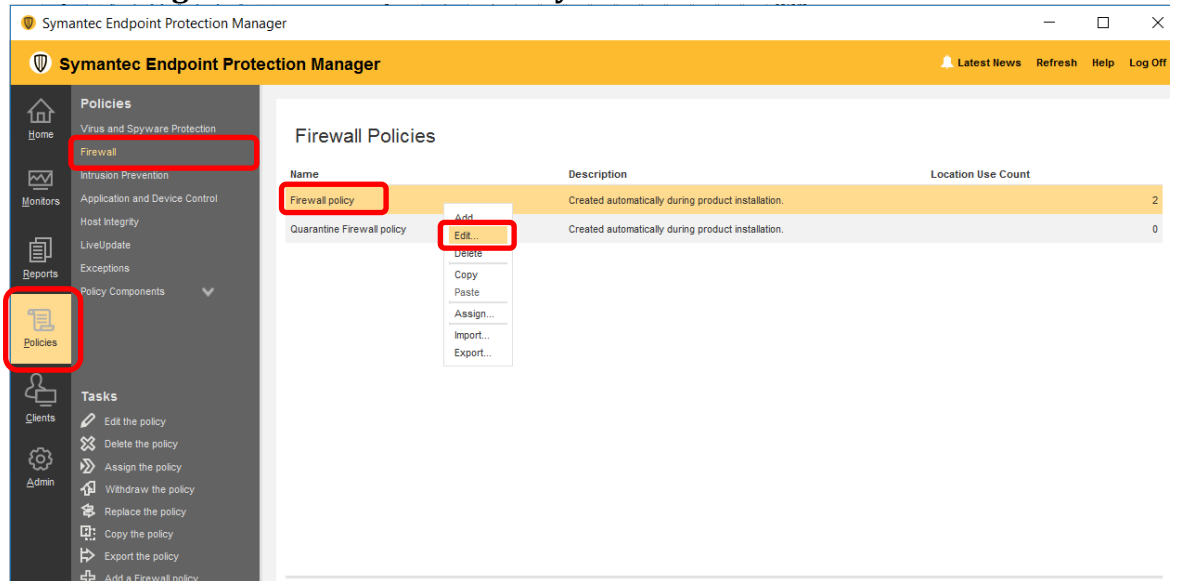
Click on 'Save'

➔ **Symantec Endpoint Protection:**

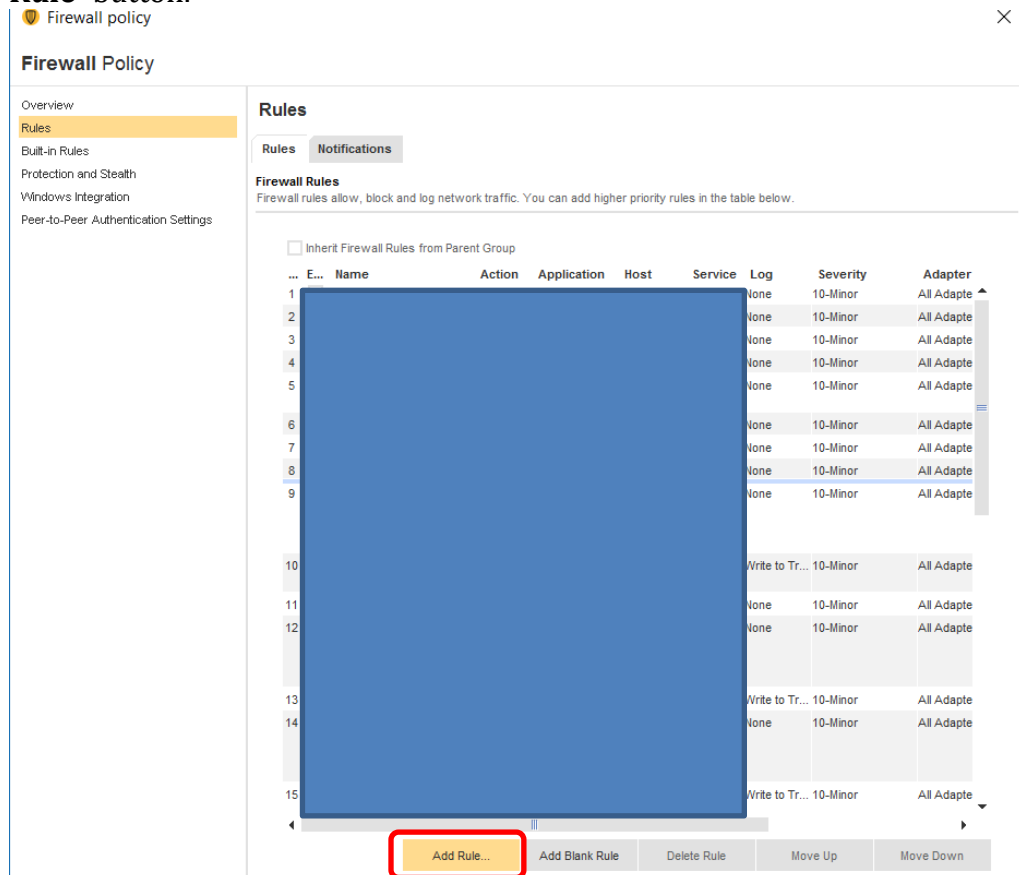
Open Symantec Endpoint Protection.

Go to **'Policies'** tab and click on **'Firewall'**.

After that **right click** on **'Firewall Policy'** and select **'Edit'**.



After that into **'Firewall Policy'** window select **'Rules'** tab and click on **'Add Rule'** button.



Now we will see how to configure ports for HTTP and HTTPS.

i. Enable ports for HTTP & HTTPS:

Add Firewall Rule Wizard

Welcome to the Add Firewall Rule Wizard

This wizard helps you to add a new firewall rule.

What do you want to name this firewall rule?

Rule name: **RD HTTP**

To continue, click Next.

Symantec

< Back **Next >** Cancel

Enter Rule name
**Different for
HTTPS and HTTP**

Click `Next`

Allow all
connections

Add Firewall Rule Wizard

Select the Action for the Rule

Select whether the firewall should allow or block or ask connections.

Symantec

Do you want this firewall rule to allow or block or ask connections?

Allow connections

Block connections

Ask connections

< Back **Next >** Cancel

Click `Next`

Allow all
Applications

Add Firewall Rule Wizard

Select the Rule Applications

Select the applications this rule should match.

Symantec

Do you want this firewall rule to apply to all applications, or only specific applications?

All Applications

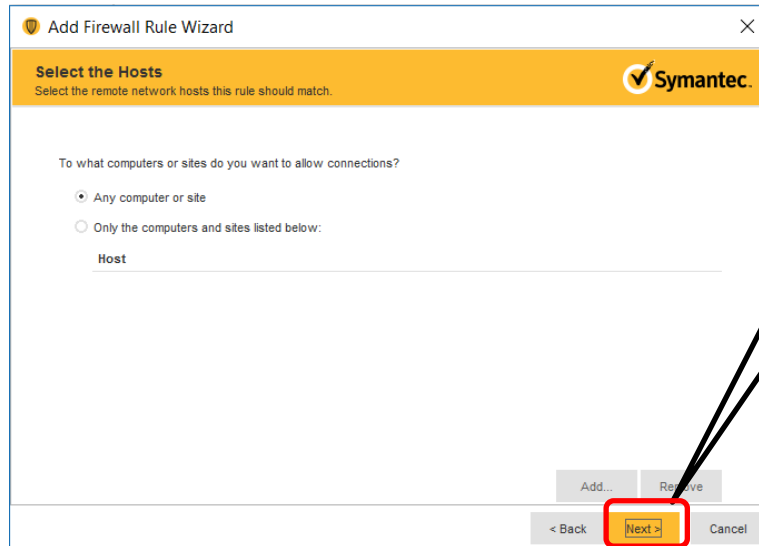
Only the applications listed below.

Application	Description
-------------	-------------

Add... Remove

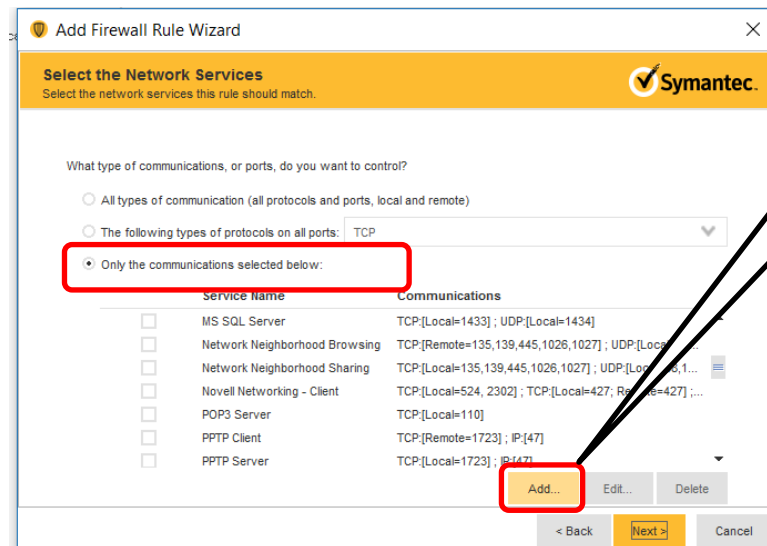
< Back **Next >** Cancel

Click `Next`



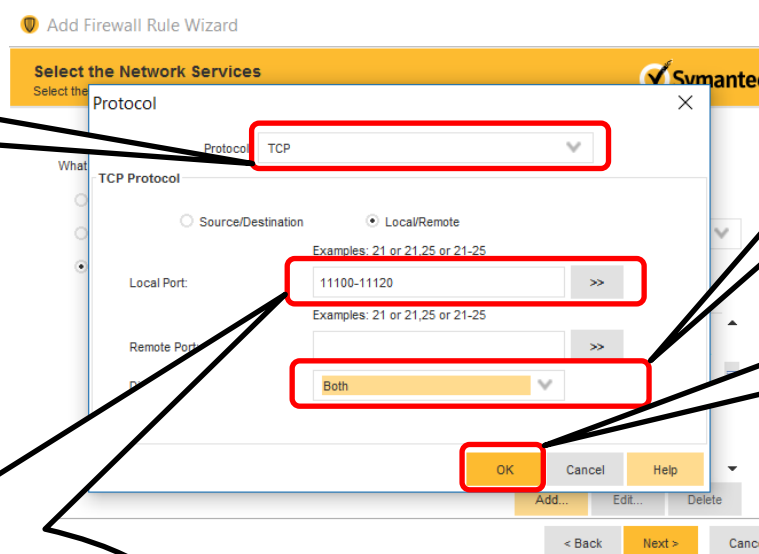
The screenshot shows the 'Add Firewall Rule Wizard' window, Symantec brand. The title bar says 'Add Firewall Rule Wizard'. The main heading is 'Select the Hosts' with the instruction 'Select the remote network hosts this rule should match.' Below this, it asks 'To what computers or sites do you want to allow connections?'. There are two radio buttons: 'Any computer or site' (selected) and 'Only the computers and sites listed below:'. Below the second option is a 'Host' label and an empty text box. At the bottom right, there are buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Click 'Next'



The screenshot shows the 'Add Firewall Rule Wizard' window, Symantec brand. The title bar says 'Add Firewall Rule Wizard'. The main heading is 'Select the Network Services' with the instruction 'Select the network services this rule should match.' Below this, it asks 'What type of communications, or ports, do you want to control?'. There are three radio buttons: 'All types of communication (all protocols and ports, local and remote)', 'The following types of protocols on all ports: TCP', and 'Only the communications selected below:'. The third option is selected and highlighted with a red box. Below this is a table with two columns: 'Service Name' and 'Communications'. The table lists several services with checkboxes. At the bottom right, there are buttons: '< Back', 'Next >', and 'Cancel'. The 'Add...' button is highlighted with a red box.

Click 'Add'



The screenshot shows the 'Add Firewall Rule Wizard' window, Symantec brand. The title bar says 'Add Firewall Rule Wizard'. The main heading is 'Select the Network Services' with the instruction 'Select the network services this rule should match.' Below this, it asks 'What type of communications, or ports, do you want to control?'. There are three radio buttons: 'All types of communication (all protocols and ports, local and remote)', 'The following types of protocols on all ports: TCP', and 'Only the communications selected below:'. The second option is selected. Below this is a table with two columns: 'Service Name' and 'Communications'. The table lists several services with checkboxes. At the bottom right, there are buttons: '< Back', 'Next >', and 'Cancel'. The 'Add...' button is highlighted with a red box.

Select 'TCP' as protocol

Select Direction 'Both'

Click 'OK'

Here HTTP Ports: '11100 - 11120'
FOR HTTPS CHANGE IT TO: '11200'

Add Firewall Rule Wizard

Select the Network Services
Select the network services this rule should match.

What type of communications, or ports, do you want to control?

☐ All types of communication (all protocols and ports, local and remote)

☐ The following types of protocols on all ports: TCP

☒ Only the communications selected below:

Service Name	Communications
<input checked="" type="checkbox"/>	TCP:[Local=11100-11120]
<input type="checkbox"/> DHCP Server	UDP:[Local=67,68; Remote=67,68]
<input type="checkbox"/> DNS Server	TCP:[Local=53; Remote=53] ; UDP:[Local=53]
<input type="checkbox"/> FTP Server	TCP:[Local=21; Incoming] ; TCP:[Local=20; Outgoing]
<input type="checkbox"/> HTTP Server	TCP:[Local=80,443]
<input type="checkbox"/> IMAP Server	TCP:[Local=143]
<input type="checkbox"/> LDAP Server	TCP:[Local=389]

Click 'Next'

Add Firewall Rule Wizard

Select a Log Action
Select the logging settings for this rule.

Do you want to create a log entry when this rule is matched?

☐ Yes

☒ No

Click Finish to create this firewall rule.

Click 'Finish'