16.3.2 Optional Lab: Configure Windows Vista Firewall

Print and complete this lab.

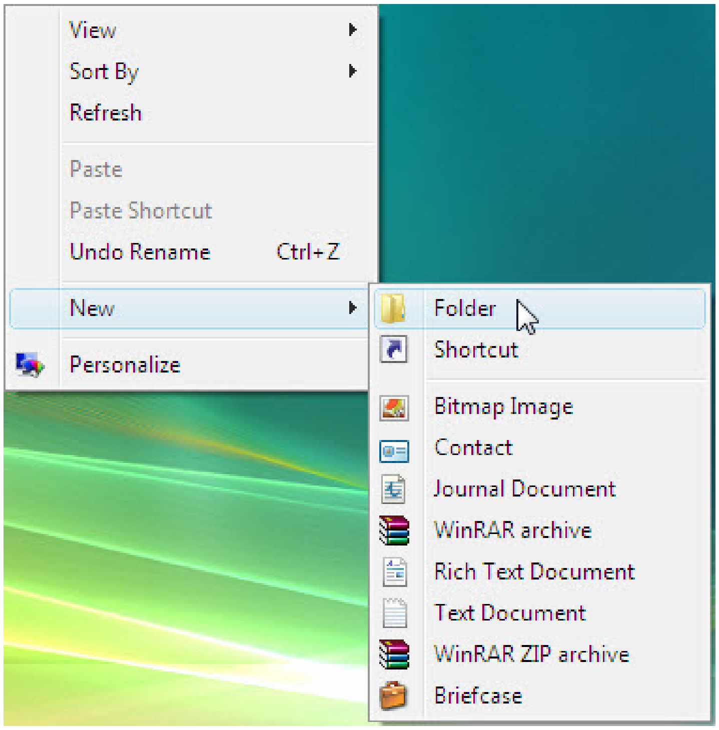
In this lab you will explore the Windows Vista Firewall and configure some advanced settings.

Recommended Equipment

- Two computers directly connected or connected through a hub or switch
- Windows Vista installed on both computers
- Computers are in the same workgroup and share the same subnet mask

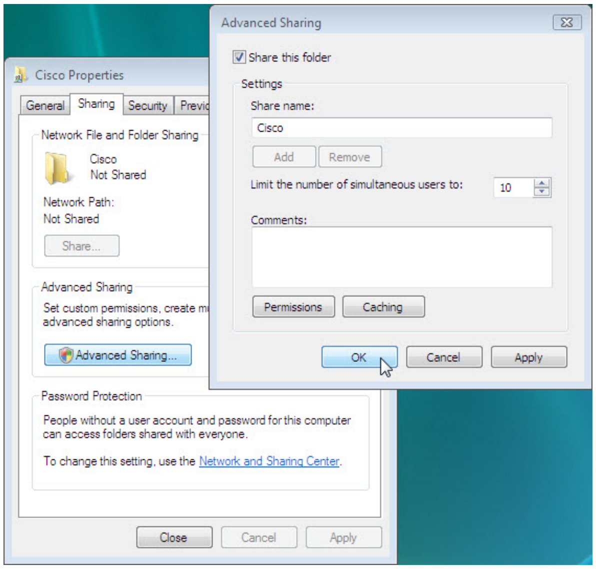
Step 1

For computer 1, right-click on the **desktop** select **New > Folder**. Name the folder Cisco.



Right-click on the Cisco folder then select **Share > Continue**.

Share the folder, use the default name Cisco.



Cisco
Not Shared

Network Path:
Not Shared

Set custom permissions, create m advanced sharing options.

People without a user account and password for this computer can access folders shared with everyone.

To change this setting, use the Network and Sharing Center.

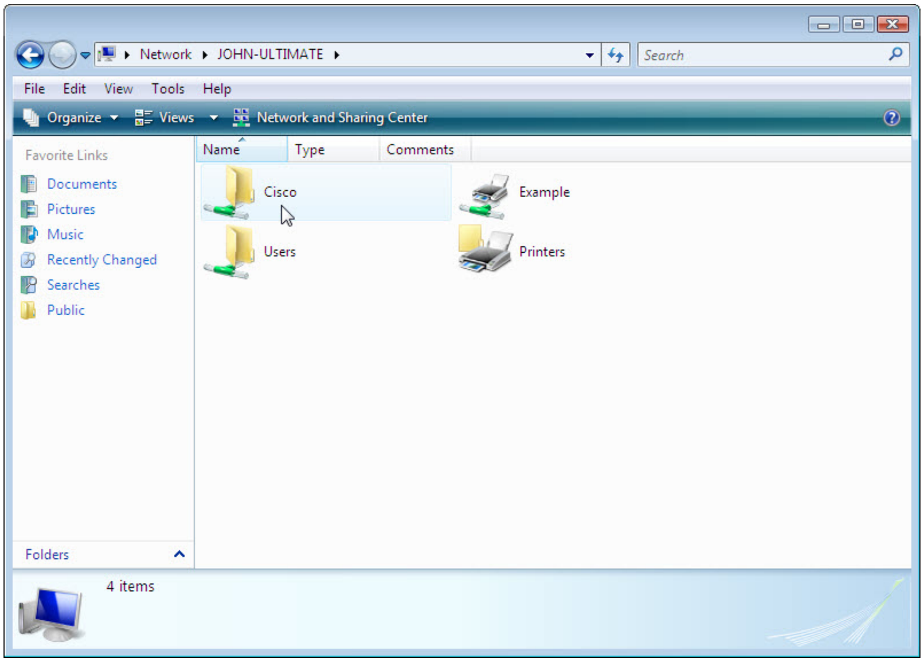
☑ Share this folder

Share name: Cisco

Limit the number of simultaneous users to: 10

Comments:

From computer 2 click **Start > Network** and try to connect to computer 1.



Can you see the shared folder Cisco?

Note: If you answered no, ask the instructor for help.

Close **Network**.

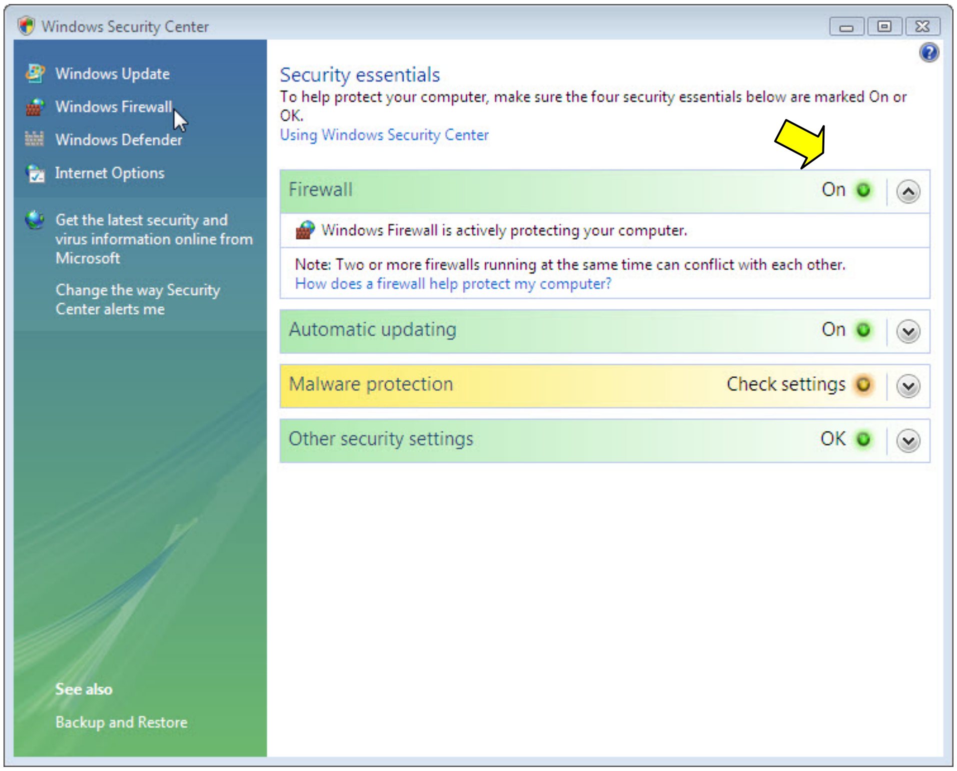
Note: Use computer 1 for the rest of the lab unless otherwise stated.

Step 2

Navigate to the Windows Vista Firewall:

Click **Start > Control Panel > Security Center**.

The Firewall indicator shows the status of the firewall. The normal setting is “ON”.



Security essentials

To help protect your computer, make sure the four security essentials below are marked On or OK.

Using Windows Security Center

Firewall On

Windows Firewall is actively protecting your computer.

Note: Two or more firewalls running at the same time can conflict with each other.
How does a firewall help protect my computer?

Automatic updating On

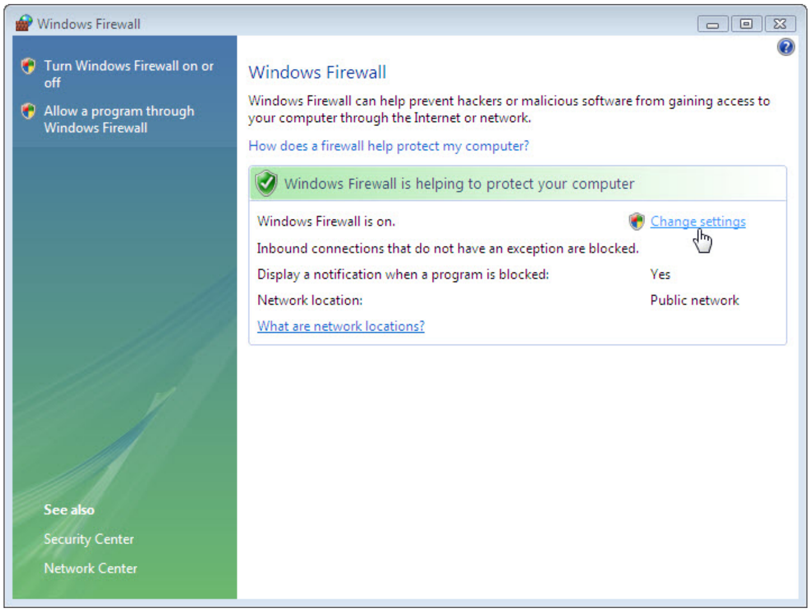
Malware protection Check settings

Other security settings OK

Access Windows firewall by clicking **Windows Firewall** at the right side of the window.

Step 3

Click **Change settings > Continue**.


Windows Firewall
Turn Windows Firewall on or off
Allow a program through Windows Firewall
See also
Security Center
Network Center

Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

How does a firewall help protect my computer?

Windows Firewall is helping to protect your computer

Windows Firewall is on. Change settings

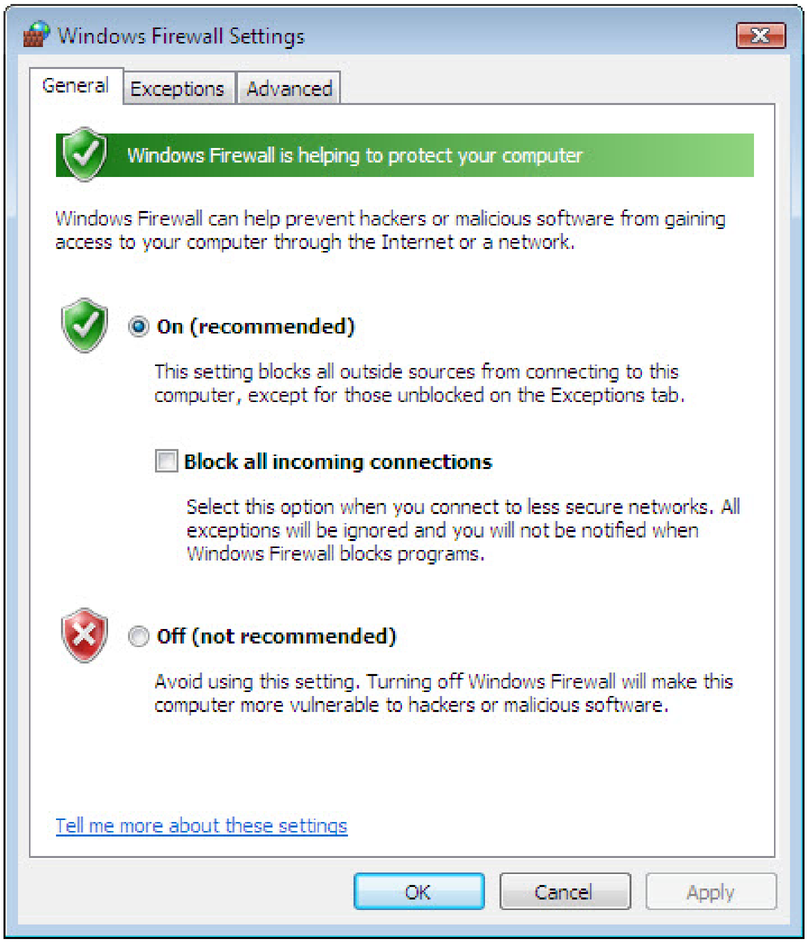
Inbound connections that do not have an exception are blocked.

Display a notification when a program is blocked: Yes

Network location: Public network

What are network locations?

The “Windows Firewall Settings” window opens.



Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● **On (recommended)**

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

☐ **Block all incoming connections**

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

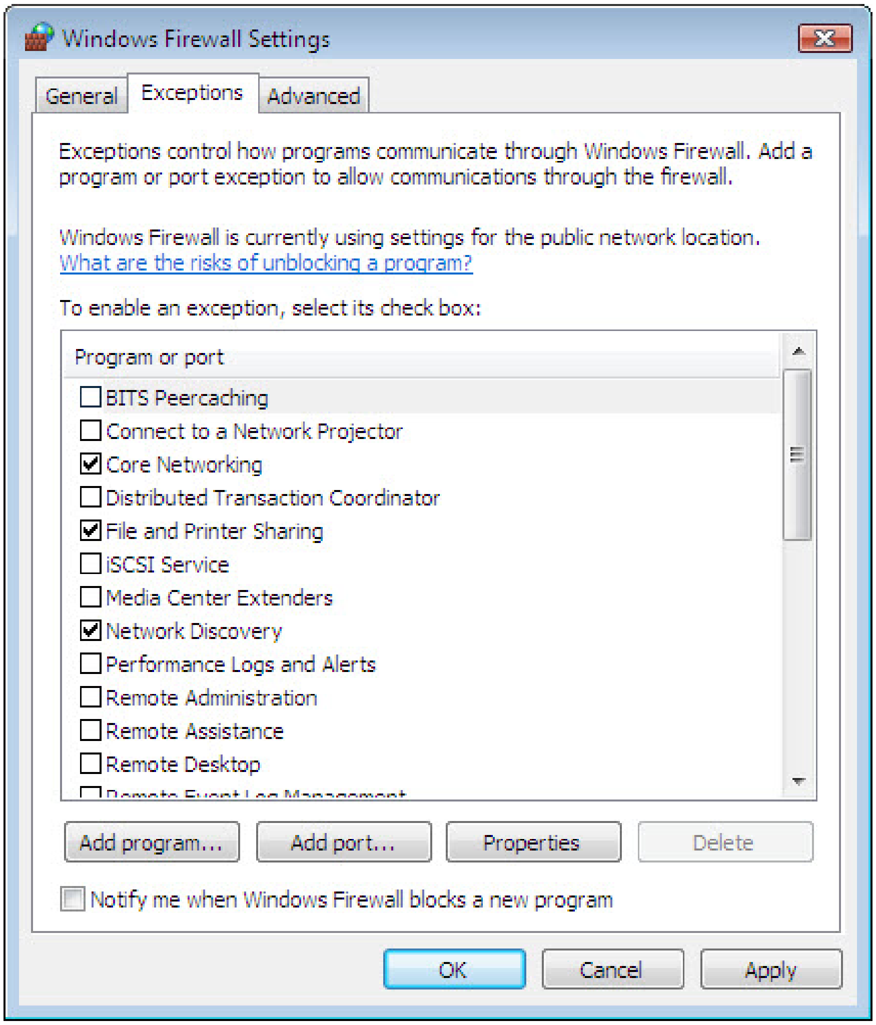
○ **Off (not recommended)**

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

In the space below, state why turning off the Windows Firewall is not advised.

Step 4

From the “Windows Firewall Settings” window select the **Exceptions** tab. Programs and services that Windows Firewall is not blocking will be listed with a checkmark.



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

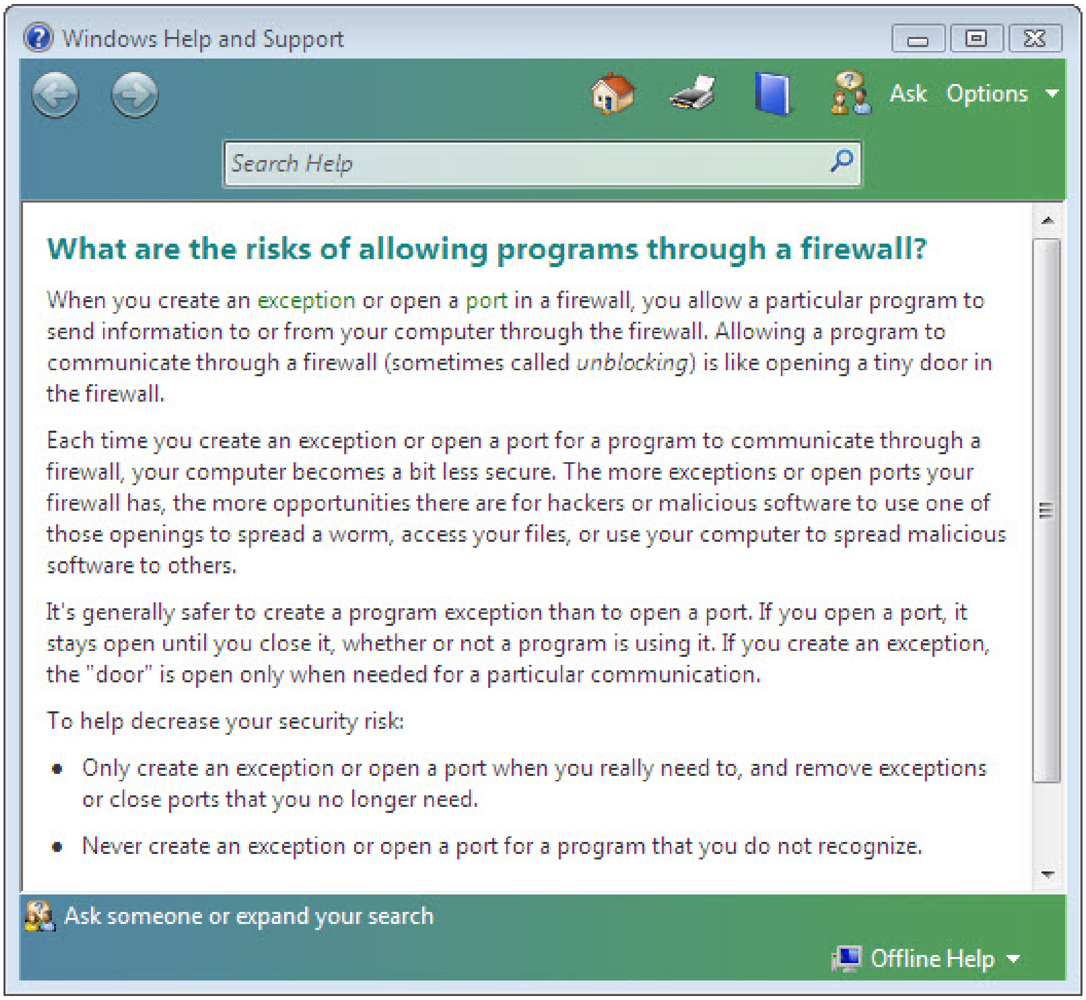
Program or port

- □ BITS Peercaching
- □ Connect to a Network Projector
- ☑ Core Networking
- □ Distributed Transaction Coordinator
- ☑ File and Printer Sharing
- □ iSCSI Service
- □ Media Center Extenders
- ☑ Network Discovery
- □ Performance Logs and Alerts
- □ Remote Administration
- □ Remote Assistance
- □ Remote Desktop
- □ Remote Event Log Management

□ Notify me when Windows Firewall blocks a new program

You can add applications to this list. This may be necessary if your customer has an application that requires outside communications but for some reason the Windows Firewall cannot perform the configuration automatically. You must be logged on to this computer as an administrator to complete this procedure.

Click **What are the risks of unblocking a program**?



What are the risks of allowing programs through a firewall?

When you create an exception or open a port in a firewall, you allow a particular program to send information to or from your computer through the firewall. Allowing a program to communicate through a firewall (sometimes called *unblocking*) is like opening a tiny door in the firewall.

Each time you create an exception or open a port for a program to communicate through a firewall, your computer becomes a bit less secure. The more exceptions or open ports your firewall has, the more opportunities there are for hackers or malicious software to use one of those openings to spread a worm, access your files, or use your computer to spread malicious software to others.

It's generally safer to create a program exception than to open a port. If you open a port, it stays open until you close it, whether or not a program is using it. If you create an exception, the "door" is open only when needed for a particular communication.

To help decrease your security risk:

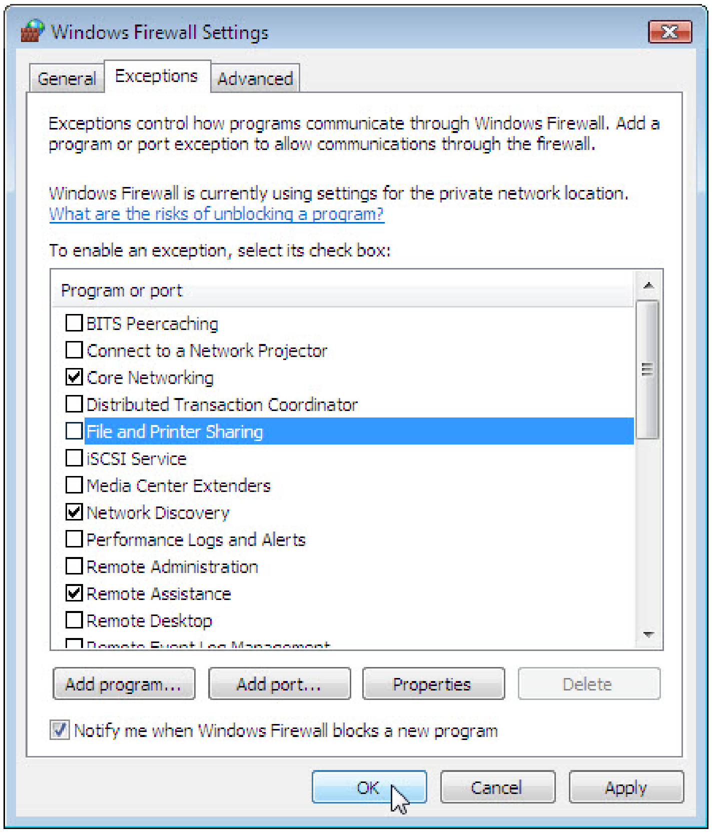
- Only create an exception or open a port when you really need to, and remove exceptions or close ports that you no longer need.
- Never create an exception or open a port for a program that you do not recognize.

Creating too many exceptions in your Programs and Services file can have negative consequences. Describe a negative consequence to having too many exceptions.

Close “Windows Help and Support” window.

Step 5

From computer 1:
To turn off an exception remove the check mark from **File and Printer Sharing > OK**.



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the private network location.
What are the risks of unblocking a program?

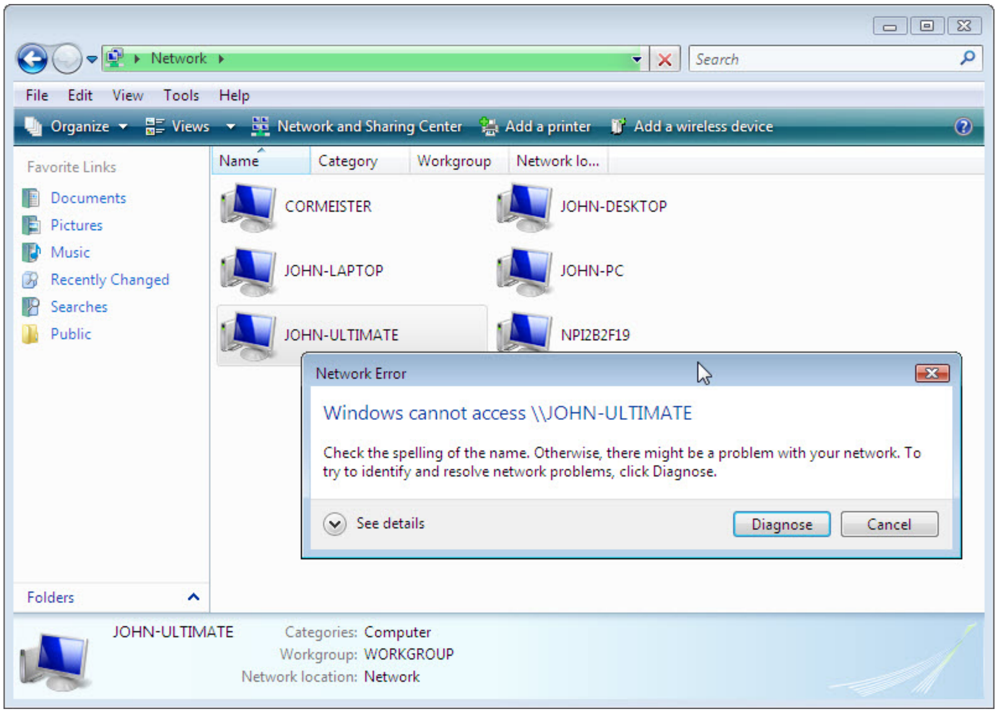
To enable an exception, select its check box:

Program or port

- □ BITS Peercaching
- □ Connect to a Network Projector
- ☑ Core Networking
- □ Distributed Transaction Coordinator
- □ File and Printer Sharing
- □ iSCSI Service
- □ Media Center Extenders
- ☑ Network Discovery
- □ Performance Logs and Alerts
- □ Remote Administration
- ☑ Remote Assistance
- □ Remote Desktop
- □ Remote Event Log Management

☑ Notify me when Windows Firewall blocks a new program

From computer 2:
Open **My Network Place >** select **View workgroup computers** and try connecting to computer 1.



Windows cannot access \\JOHN-ULTIMATE

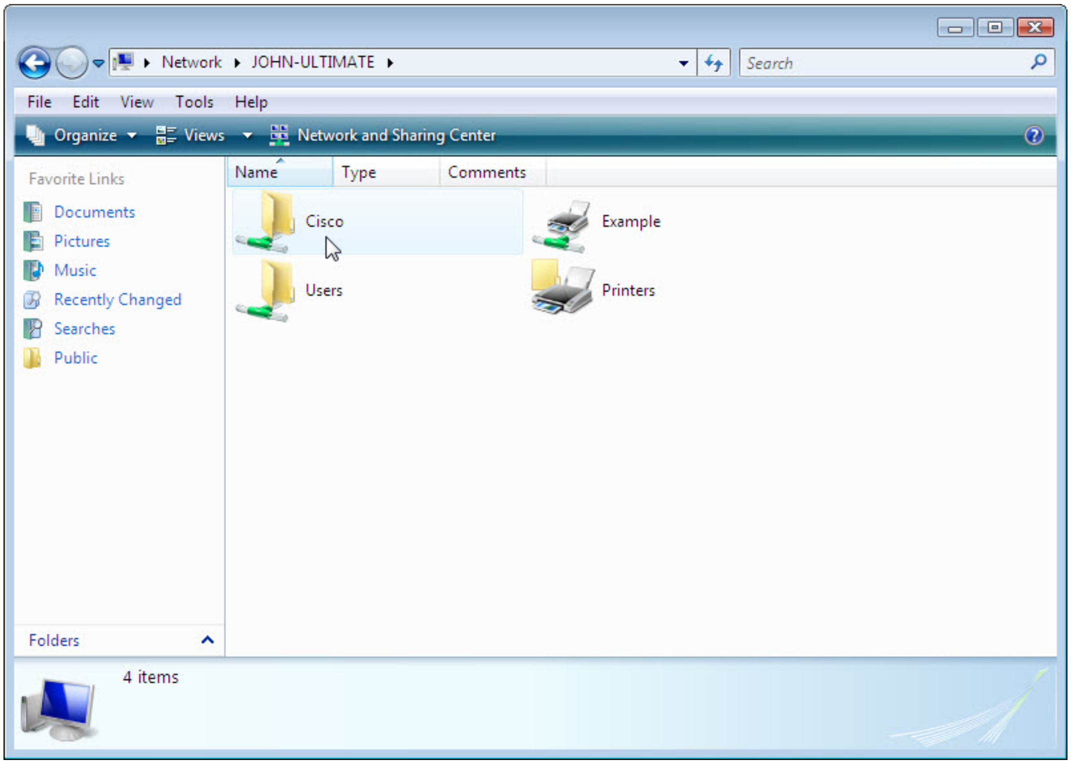
Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click Diagnose.

JOHN-ULTIMATE Categories: Computer
Workgroup: WORKGROUP
Network location: Network

Can you connect to computer 1?

From computer 1:
To turn on an exception add a check mark to **File and Printer Sharing > OK**.

From computer 2:
Refresh **My Network Place** and try connecting to computer 1.

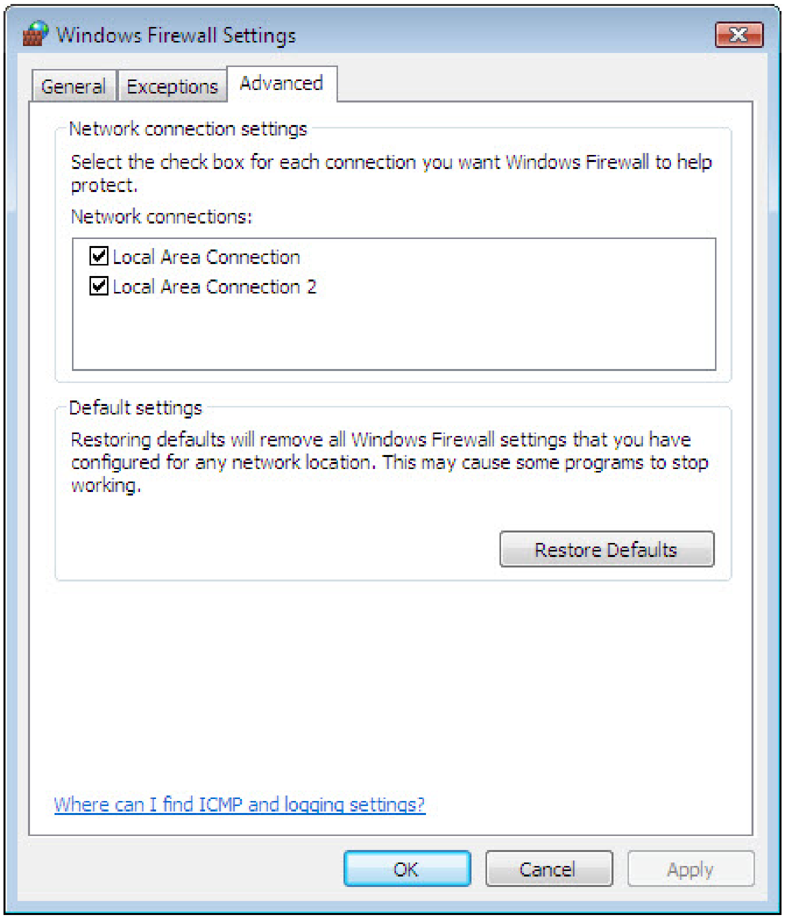


Can you connect to computer 1?

Log off computer 2. Use computer 1 for the rest of the lab.

Step 6

From the Windows Firewall Settings window select the **Advanced** tab to view the **Network Connection Settings**. Network Connection Settings displays the different connections configured for your computer.


Windows Firewall Settings
General
Exceptions
Advanced

Network connection settings

Select the check box for each connection you want Windows Firewall to help protect.

Network connections:

☑ Local Area Connection
☑ Local Area Connection 2

Default settings

Restoring defaults will remove all Windows Firewall settings that you have configured for any network location. This may cause some programs to stop working.

Restore Defaults
Where can I find ICMP and logging settings?
OK
Cancel
Apply

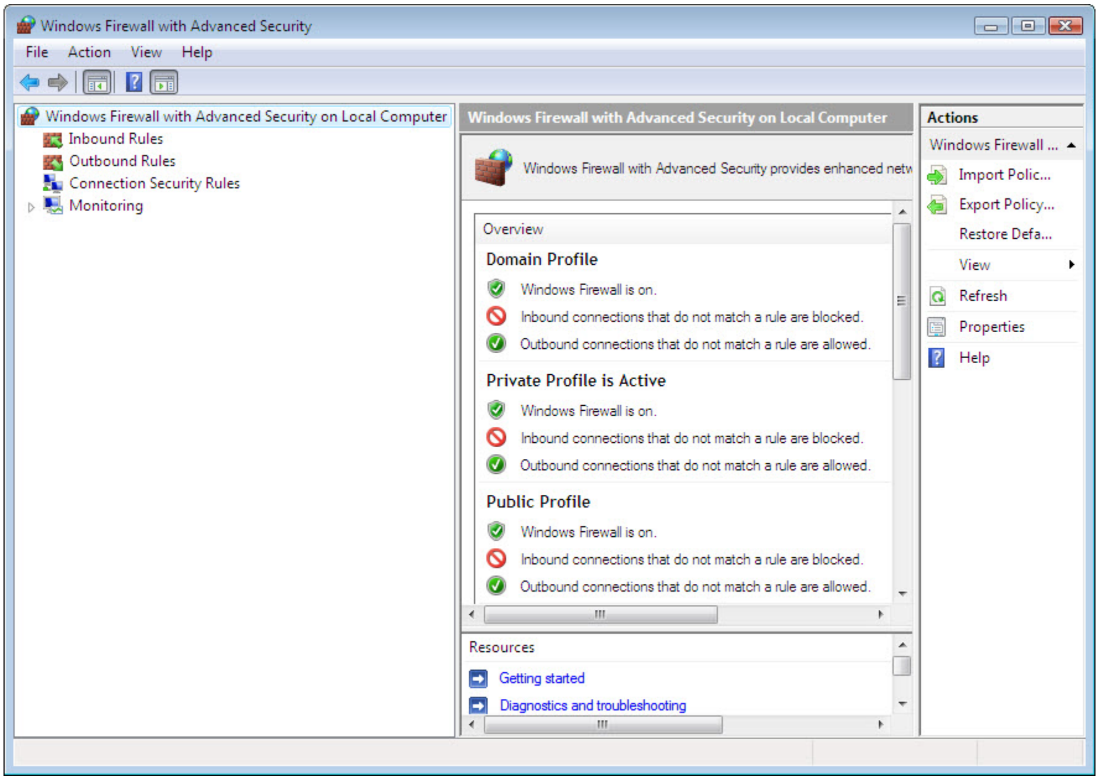
In the space below, list the connections protected by Windows Firewall.

Close all open Windows Firewall windows.

Step 7

There are many applications that users do not normally see that also need to get through the Windows Firewall to access your computer. These can be accessed in Windows Firewall with Advanced Security.

Click **Start > Control Panel > Administrative Tools > Windows Firewall with Advanced Security > Continue**.



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides enhanced netw

Overview

Domain Profile

✓ Windows Firewall is on.

🛇 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile is Active

✓ Windows Firewall is on.

🛇 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile

✓ Windows Firewall is on.

🛇 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Resources

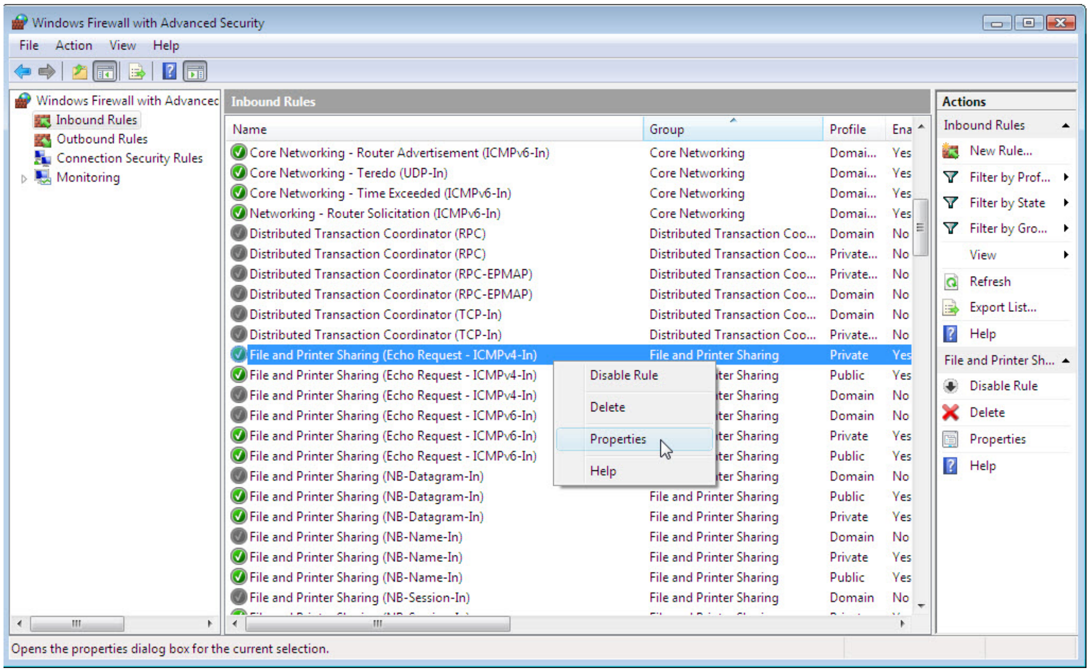
Getting started

Diagnostics and troubleshooting

What three firewall profiles are shown?

Which firewall profile is active?

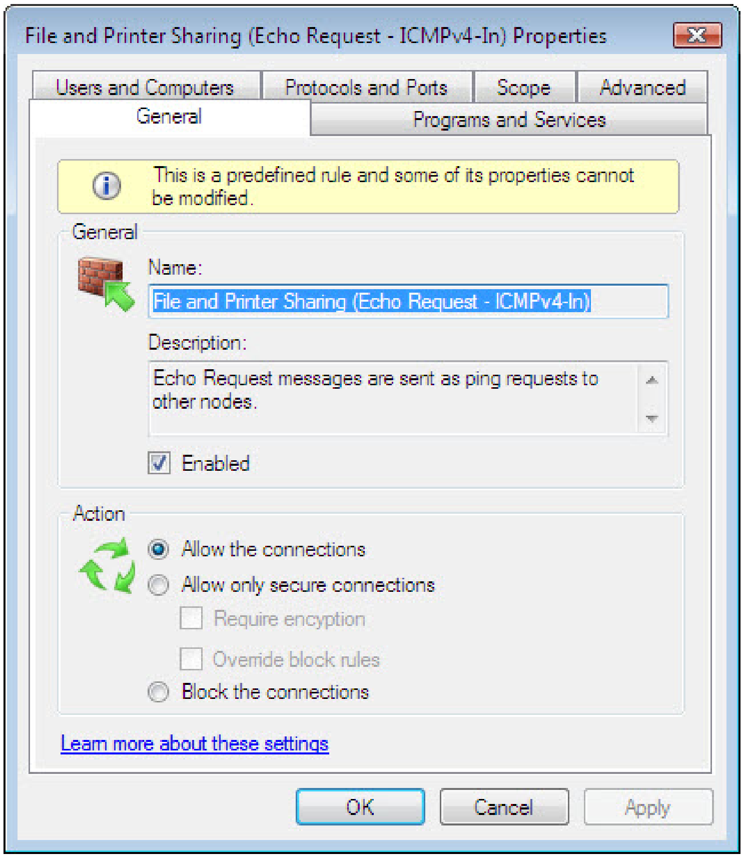
Click **Inbound Rules**. Expand the window so you can see the full name of the Inbound rules. Locate Files and Printer Sharing (Echo Request – ICMPv4-In). Right-click on the rule and select **Properties**.



Name	Group	Profile	Ena
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	Domai...	Yes
Core Networking - Teredo (UDP-In)	Core Networking	Domai...	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	Domai...	Yes
Networking - Router Solicitation (ICMPv6-In)	Core Networking	Domai...	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Private...	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	ter Sharing	Public	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	ter Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	ter Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	ter Sharing	Private	Yes
File and Printer Sharing (Echo Request - ICMPv6-In)	ter Sharing	Public	Yes
File and Printer Sharing (NB-Datagram-In)	ter Sharing	Domain	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Public	Yes
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private	Yes
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private	Yes
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Public	Yes
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No

Opens the properties dialog box for the current selection.

The “Files and Printer Sharing (Echo Request – ICMPv4-In) Propertise” window appears.



This is a predefined rule and some of its properties cannot be modified.

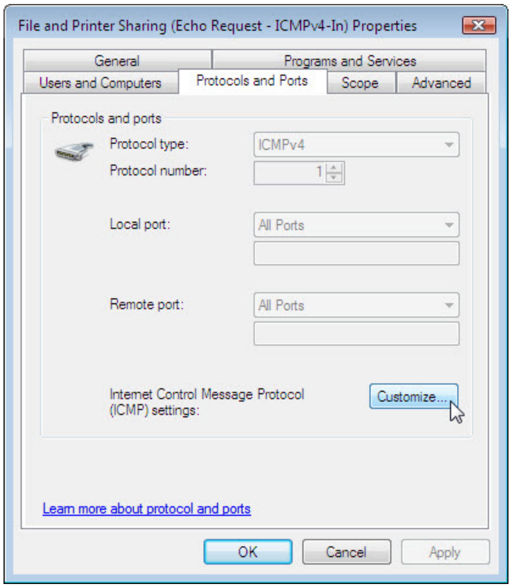
Name:
File and Printer Sharing (Echo Request - ICMPv4-In)

Description:
Echo Request messages are sent as ping requests to other nodes.

☑ Enabled

● Allow the connections
○ Allow only secure connections
□ Require encryption
□ Override block rules
○ Block the connections

Click **Protocols and Ports** tab **> Customize**.



File and Printer Sharing (Echo Request - ICMPv4-In) Properties

Protocols and ports

Protocol type: ICMPv4

Protocol number: 1

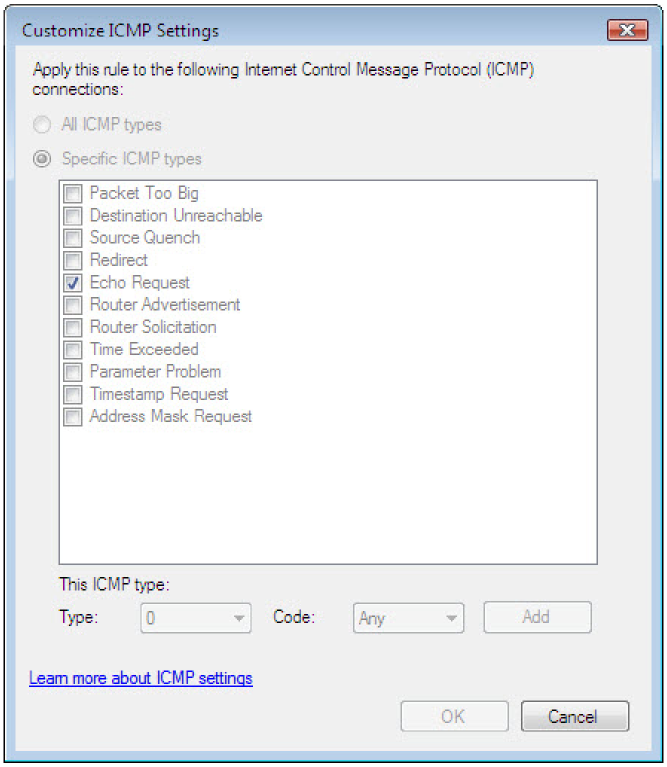
Local port: All Ports

Remote port: All Ports

Internet Control Message Protocol (ICMP) settings: Customize...

Learn more about protocol and ports

The “Customize ICMP” Settings window appears.



Customize ICMP Settings

Apply this rule to the following Internet Control Message Protocol (ICMP) connections:

○ All ICMP types

● Specific ICMP types

- ☐ Packet Too Big
- ☐ Destination Unreachable
- ☐ Source Quench
- ☐ Redirect
- ☑ Echo Request
- ☐ Router Advertisement
- ☐ Router Solicitation
- ☐ Time Exceeded
- ☐ Parameter Problem
- ☐ Timestamp Request
- ☐ Address Mask Request

This ICMP type:

Type: 0 Code: Any

Learn more about ICMP settings

In the example here, allowing incoming echo requests is what allows network users to “ping” your computer to determine if it is present on the network and how fast information travels to and from it.

In the space below, list the requests for information that your computer will not respond to.

Close all open windows.