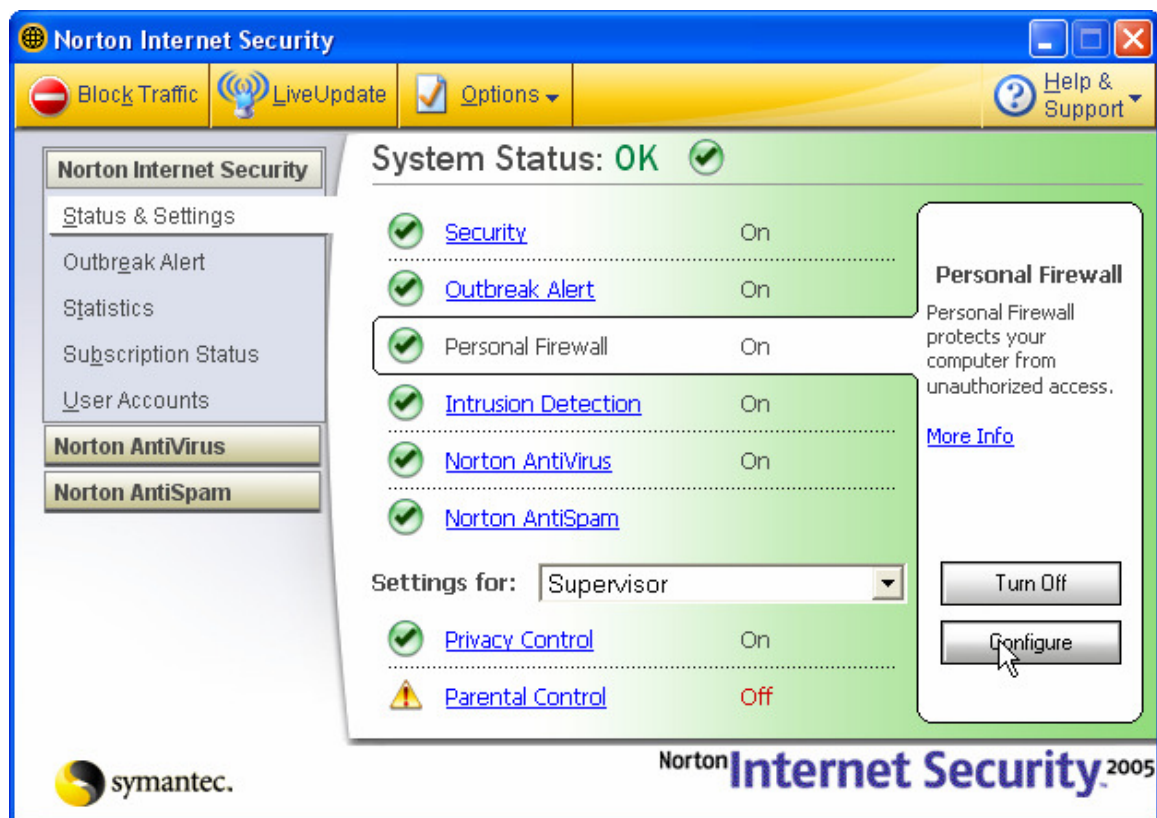
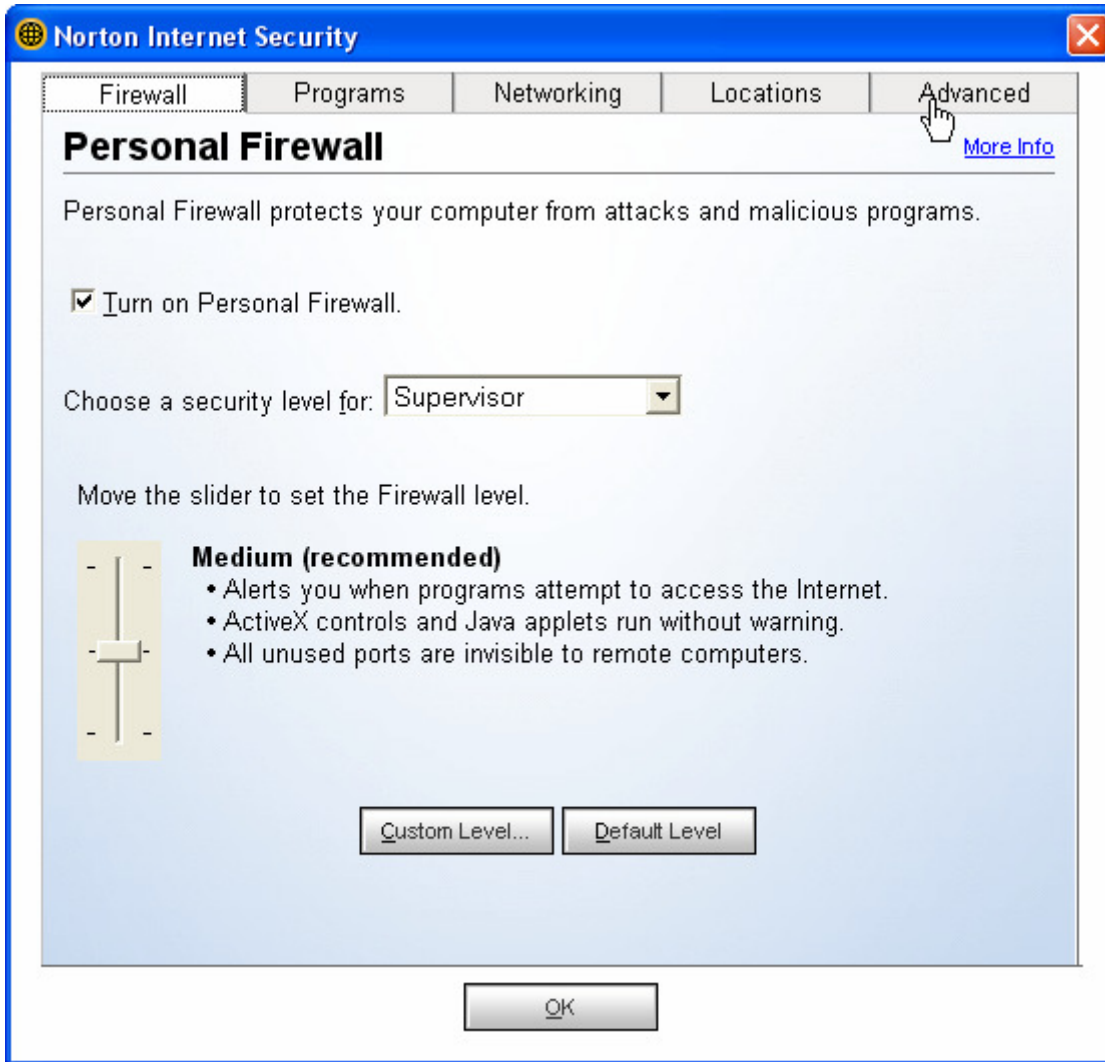



Updating Norton Internet Security to work with FocalpointNet DNS addressing

1. Open Norton Internet Security and highlight “Personal Firewall”.
2. Click on “Configure”

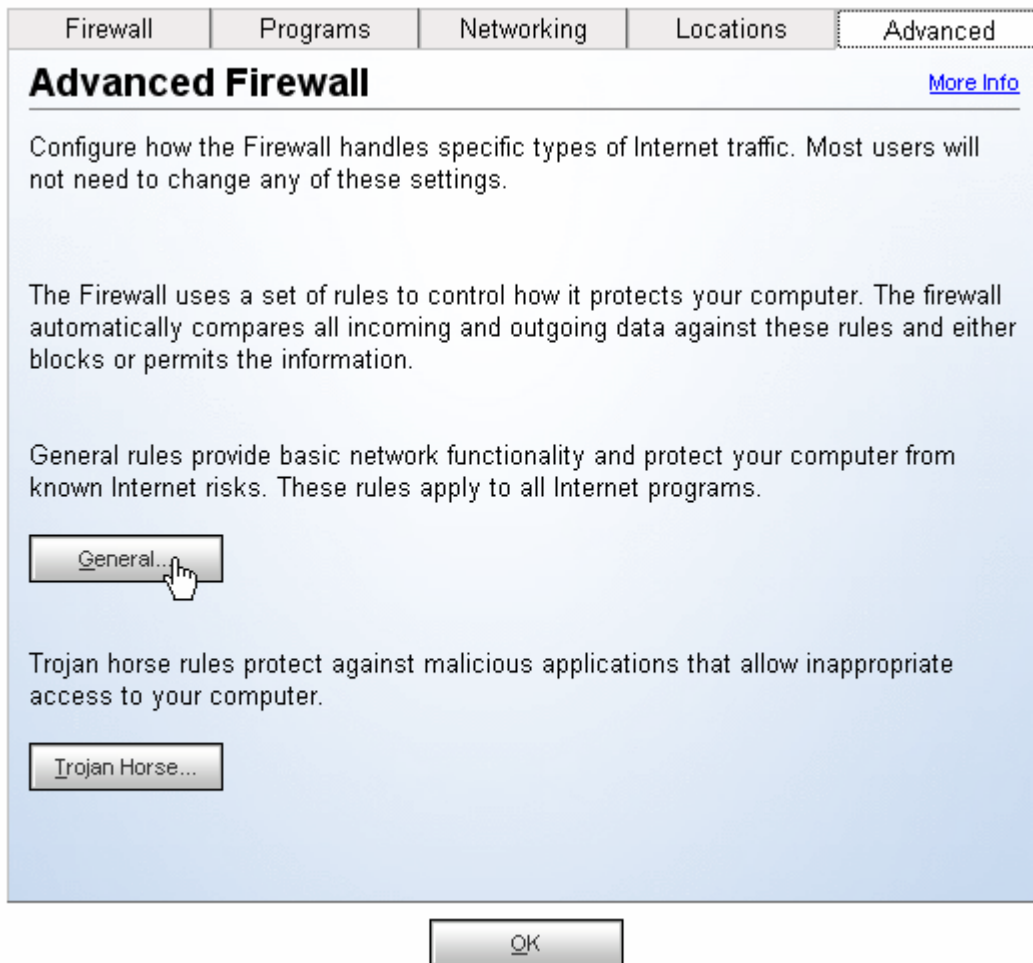


3. Click on “Advanced”





4. Click on “General”



5. Click on “Add”

General Rules [More Info](#)

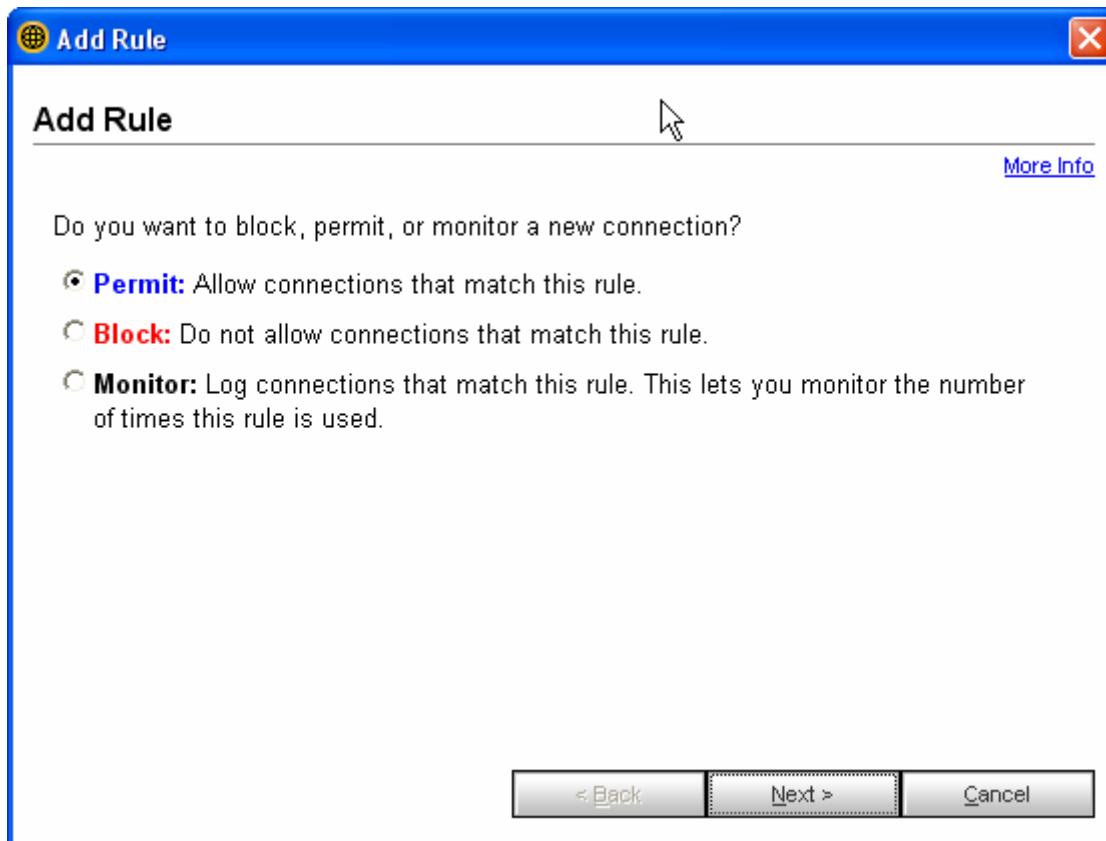
Settings for: Home (Active)


These rules determine how the firewall handles incoming and outgoing connections. Rules that appear earlier in the list override later rules.

<input checked="" type="checkbox"/>	Description
<input checked="" type="checkbox"/>	Default Inbound ICMP Permit , Direction: Inbound, Computer: Any, Adapter: Any, Communications: Specific, Protocol: ICMP
<input checked="" type="checkbox"/>	Default Outbound ICMP Permit , Direction: Outbound, Computer: Any, Adapter: Any, Communications: Any, Protocol: ICMP
<input checked="" type="checkbox"/>	Default Inbound DNS Permit , Direction: Inbound, Computer: Any, Adapter: Any, Communications: Specific, Protocol: UDP
<input type="checkbox"/>	Default Inbound NetBIOS Name



6. Select Permit and then click on “Next





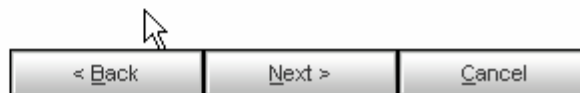
7. Click on “Connection to and from other computers”. Then Click on “Next”.

Add Rule

[More Info](#)

What type of connection do you want to **permit**?

- Connections **to** other computers
Type of connection made by most Internet-enabled applications. Also called outbound connections.
- Connections **from** other computers
Type of connection typical of a server application such as a Web server or FTP server. Also called inbound connections.
- Connections **to and from** other computers
Some applications utilize both types of connections (inbound and outbound).





8. Click on “Only the computers and sites listed below”. Then Click on “Add”.

Add Rule



[More Info](#)

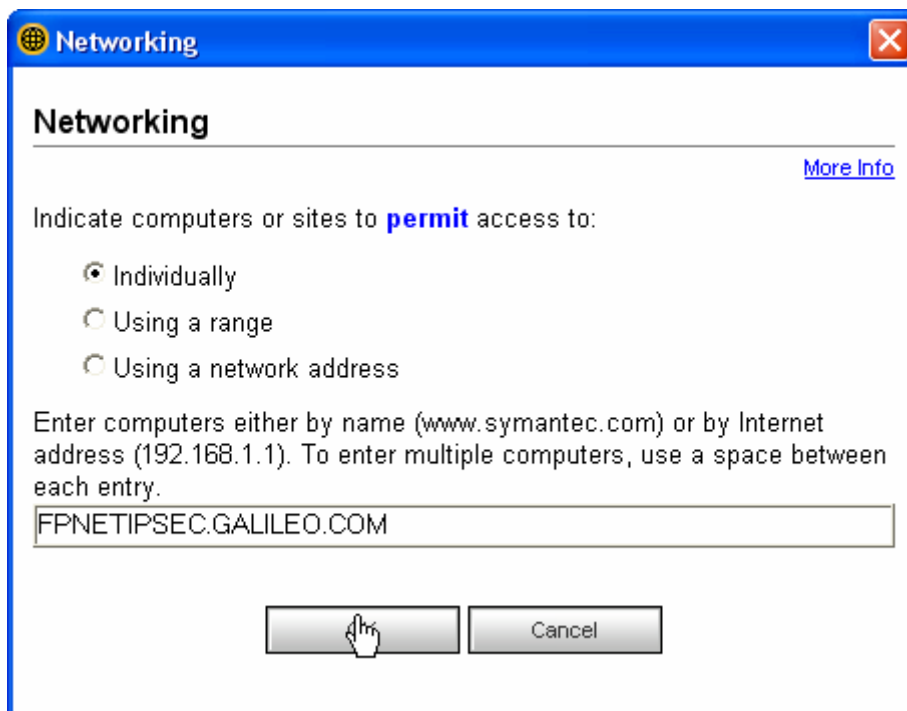
What computers or sites do you want to **permit**?

- Any computer
- Only the computers and sites listed below

Click Adapters to limit communications to specific network adapters. This is necessary only if you have more than one network adapter in your computer.



- 
- 
9. Check for “Individually”. Then add in the DNS name for your connection to Galileo.
FPNETIPSEC.GALILEO.COM or
FPNETNATT.GALILEO.COM or
FPNETPPTP.GALILEO.COM or
FPNETGIDS.GALILEO.COM
Then click “OK”



10. Click on “Next”

Add Rule

[More Info](#)

What computers or sites do you want to **permit**?

- Any computer
- Only the computers and sites listed below

Single Address	Name: FPNETIPSEC.GALILEO.COM	↑ ↓
-------------------	------------------------------	--------

Click Adapters to limit communications to specific network adapters. This is necessary only if you have more than one network adapter in your computer.



11. Check “TCP and UDP”. Then check “All types of communication (all ports, local and remote)”

Add Rule

[More Info](#)

What protocols do you want to **permit**?

- TCP
- UDP
- TCP and UDP
- ICMP

What types of communication, or ports, do you want to **permit**?

- All types of communication (all ports, local and remote)
- Only the types of communication or ports listed below

Add


Remove

< Back

Next >

Cancel





12. Click on “Next”

Add Rule

[More Info](#)

You can choose to be notified when a connection matches this rule.

When a connection matches a rule:

Only Log event after it occurs times

Create an event log entry



Notify me with a Security Alert

< Back

Next >

Cancel





13. Give the Rule a name such as “Nortel Rule” then click “Next”.

Add Rule

[More Info](#)

What do you want to call this rule?

This description appears in the Rule Summary list to help you identify this rule.

In which category does this rule belong?

Select the category that best describes the rule for which you've configured Internet access. Parental Control uses these categories to determine which applications and types of communication your children can use online.

General	▲
Instant Messaging	
Internet Advertising	☰
Networked Games	
Newsreaders	▼

< Back

Next >

Cancel



14. Make sure the (Active) profile is Checked. Then click “Next”.

Add Rule

[More Info](#)

Which locations should this rule be applied to?
This rule can be applied to multiple locations.

<input type="checkbox"/>	Default
<input checked="" type="checkbox"/>	Home (Active)
<input type="checkbox"/>	Office
<input type="checkbox"/>	Away

Check All



Uncheck All

< Back

Next >

Cancel





15. Click on “Finish” to Complete the addition of the Rule.

Add Rule

You have created the following rule to **permit** Internet communications for your computer:

Description: Nortel Rule

Action: **Permit**

Direction: In/Out

Computer: Specific

Adapter: Any

Communications: Any

Protocol: TCP and UDP

Locations: Home



16. Click “Ok” to complete the changes to the rules.

General Rules [More Info](#)

Settings for: Home (Active)

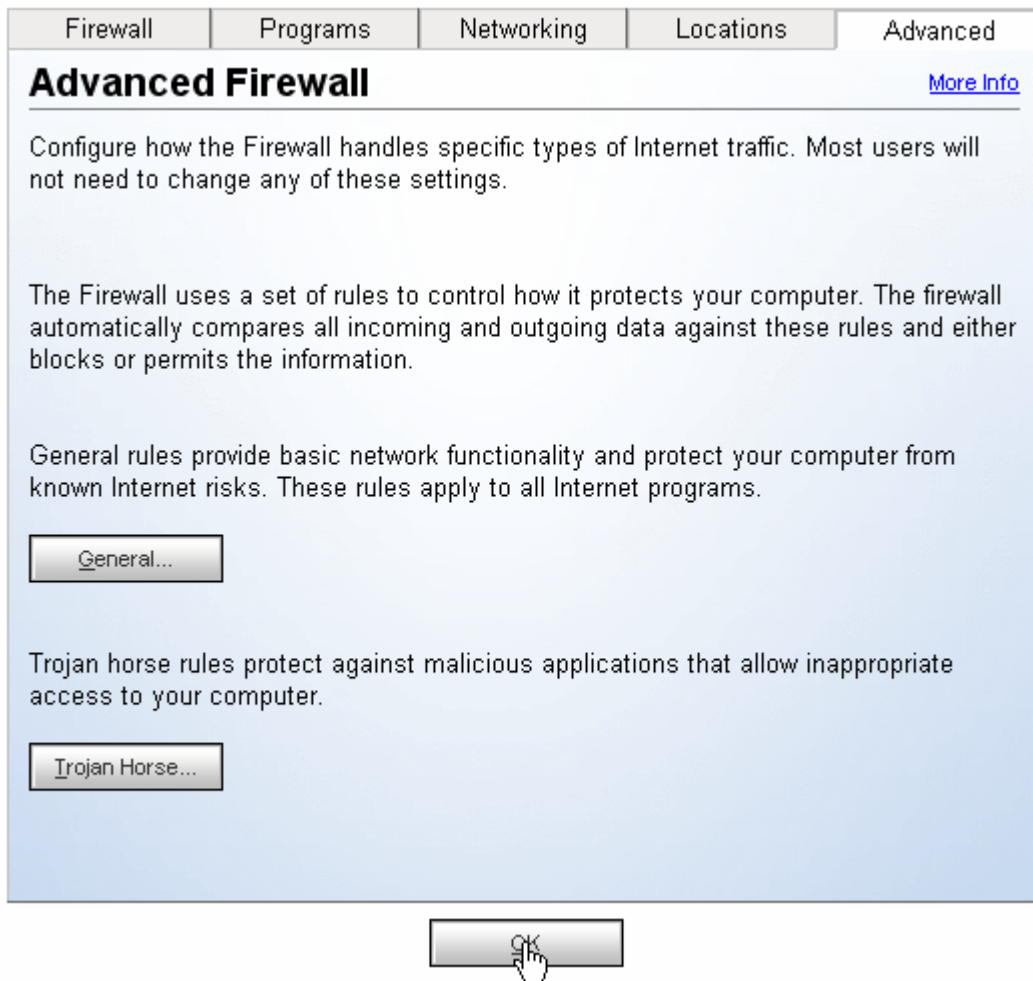
These rules determine how the firewall handles incoming and outgoing connections. Rules that appear earlier in the list override later rules.

<input checked="" type="checkbox"/>	Description
<input checked="" type="checkbox"/>	Default Inbound ICMP Permit , Direction: Inbound, Computer: Any, Adapter: Any, Communications: Specific, Protocol: ICMP
<input checked="" type="checkbox"/>	Default Outbound ICMP Permit , Direction: Outbound, Computer: Any, Adapter: Any, Communications: Any, Protocol: ICMP
<input checked="" type="checkbox"/>	Default Inbound DNS Permit , Direction: Inbound, Computer: Any, Adapter: Any, Communications: Specific, Protocol: UDP
<input type="checkbox"/>	Default Inbound NetBIOS Name





17. Click “Ok” to complete the Advanced Firewall settings.



18. Click on the Red “X” in the upper right hand corner to close out Norton Internet Security.



Note: At this point re-try the Nortel Client Connection.

You should now be able to connect to the Galileo system.

