

FAQ# MTN-9AJMA2

Question: What causes the Hardware Configuration to be unable to connect to the controller?

Answer:

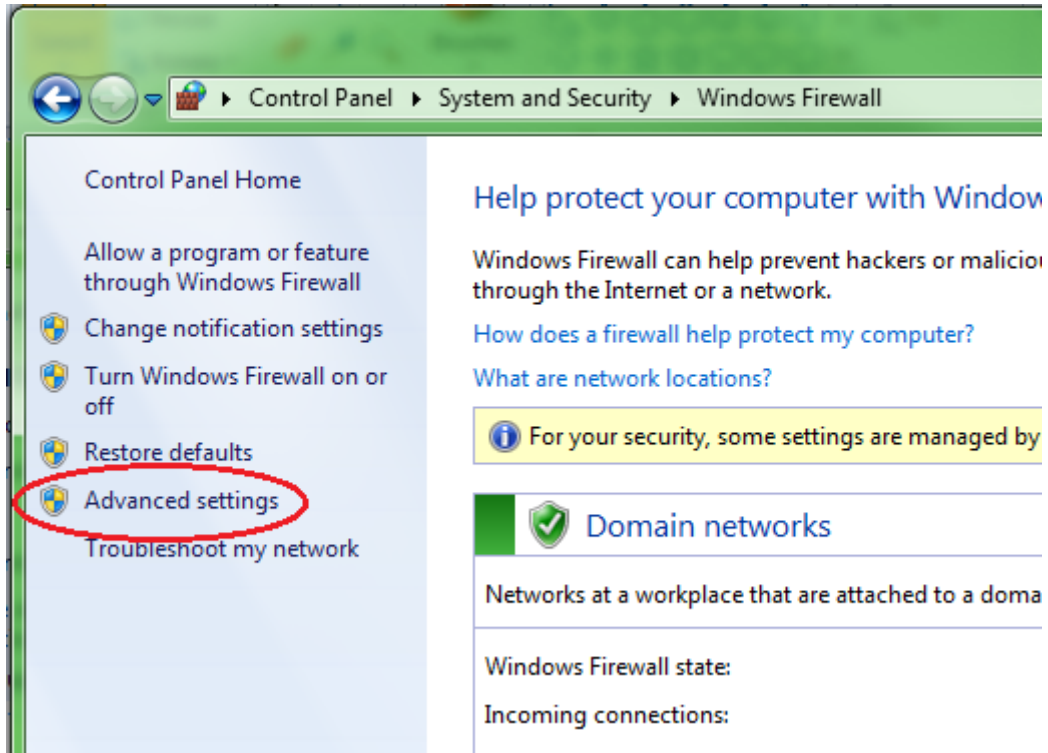
The first step to debugging this issue is verifying the MPiec controller is connected to the same network as your computer and has the desired IP address settings. This can be done by either sending a ping to the controller or connecting to the controller's web server.

If the Hardware Configuration is still unable to connect after verifying other communication with the controller, the next step is to check the Alarm Status page in the web server. Check the list for alarm 4403 0005 – RMI Connection Rejected. If this error is present, it means the port the Hardware Configuration is trying to communicate with is already being used by an open Machine Operations page in the web server. To solve this problem, close any open web pages connected to the controller's Machine Operations. After this try connecting to the controller with the Hardware Configuration.

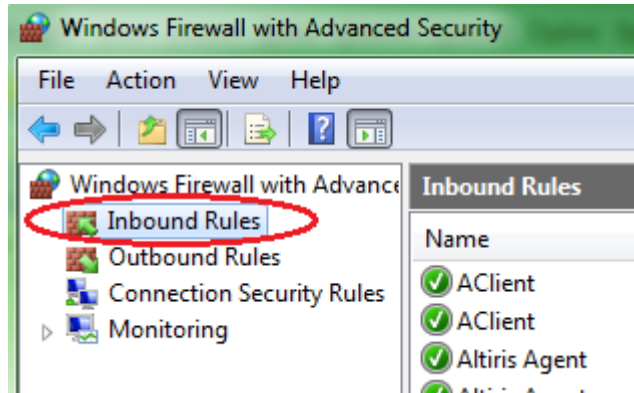
If connection is still being rejected without causing the error mentioned above, it is likely that a firewall on the computer is blocking the Hardware Configuration's connection to the controller through port 4040. (This is the port the Hardware Configuration uses to connect to the controller. A list of all ports used by the controller can be found in section 1.9.0 of the Hardware Configuration help manual). The following are steps to stop the firewall from blocking the connection for Windows 7 users

<ul style="list-style-type: none">- Open the Control Panel- Open System and Security- Click on Windows Firewall	 <p>The screenshot shows the Windows 7 Control Panel window with the address bar displaying 'Control Panel > System and Security'. The left-hand navigation pane lists various system settings, with 'System and Security' selected. The main content area displays several system status tiles: 'Action Center', 'Windows Firewall' (which is circled in red), 'System', and 'Windows Update'. The 'Windows Firewall' tile includes the text 'Check firewall status' and 'Allow a program through Windows Firewall'.</p>
---	---

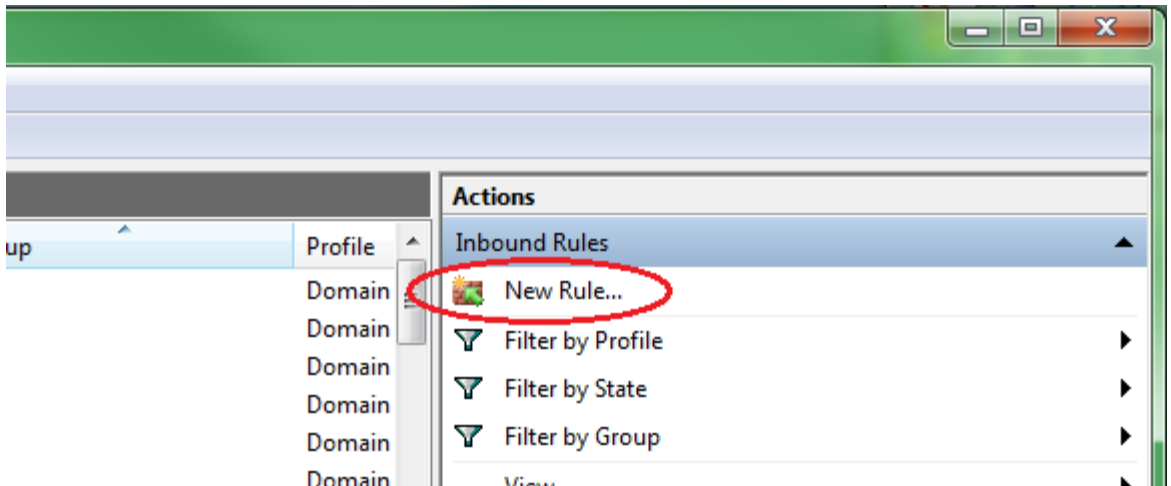
Click on Advanced Settings



Click on Inbound Rules



Click on New Rule...



Rule Type
Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

- Program**
Rule that controls connections for a program.
- Port**
Rule that controls connections for a TCP or UDP port.
- Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.
- Custom**
Custom rule.

[Learn more about rule types](#)

< Back **Next >** Cancel

New Inbound Rule window opens...
- Choose "Port"
- Click on Next

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.
Customize...
- Block the connection**

[Learn more about actions](#)

< Back **Next >** Cancel

- Choose "Allow the connection"
- Click Next

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.
- Public**
Applies when a computer is connected to a public network location.

[Learn more about profiles](#)

< Back **Next >** Cancel

- Leave all the boxes checked
- Click Next

Name
Specify the name and description of this rule.

Steps:

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

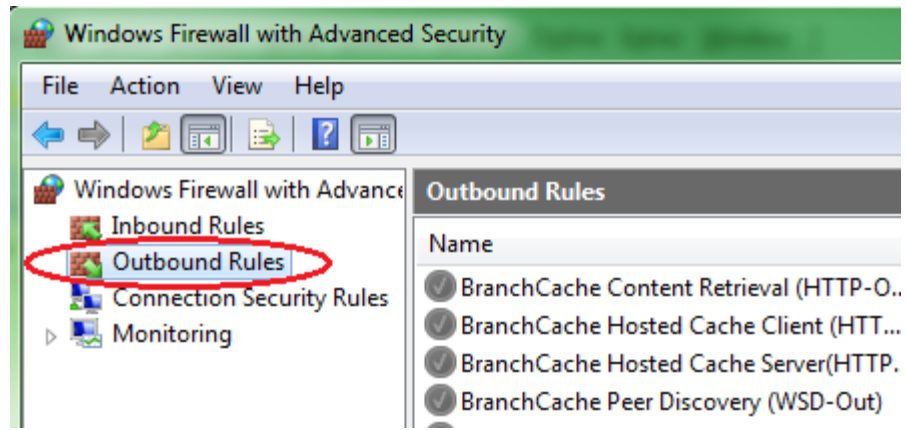
Name:
Allow 4040 Inbound

Description (optional):

< Back **Finish** Cancel

- Name your new Inbound rule
Click Finish

- Repeat Steps 4 to 9 to create a new Outbound Rule



Exit Firewall settings.
Exit Control Panel.
Restart your computer.