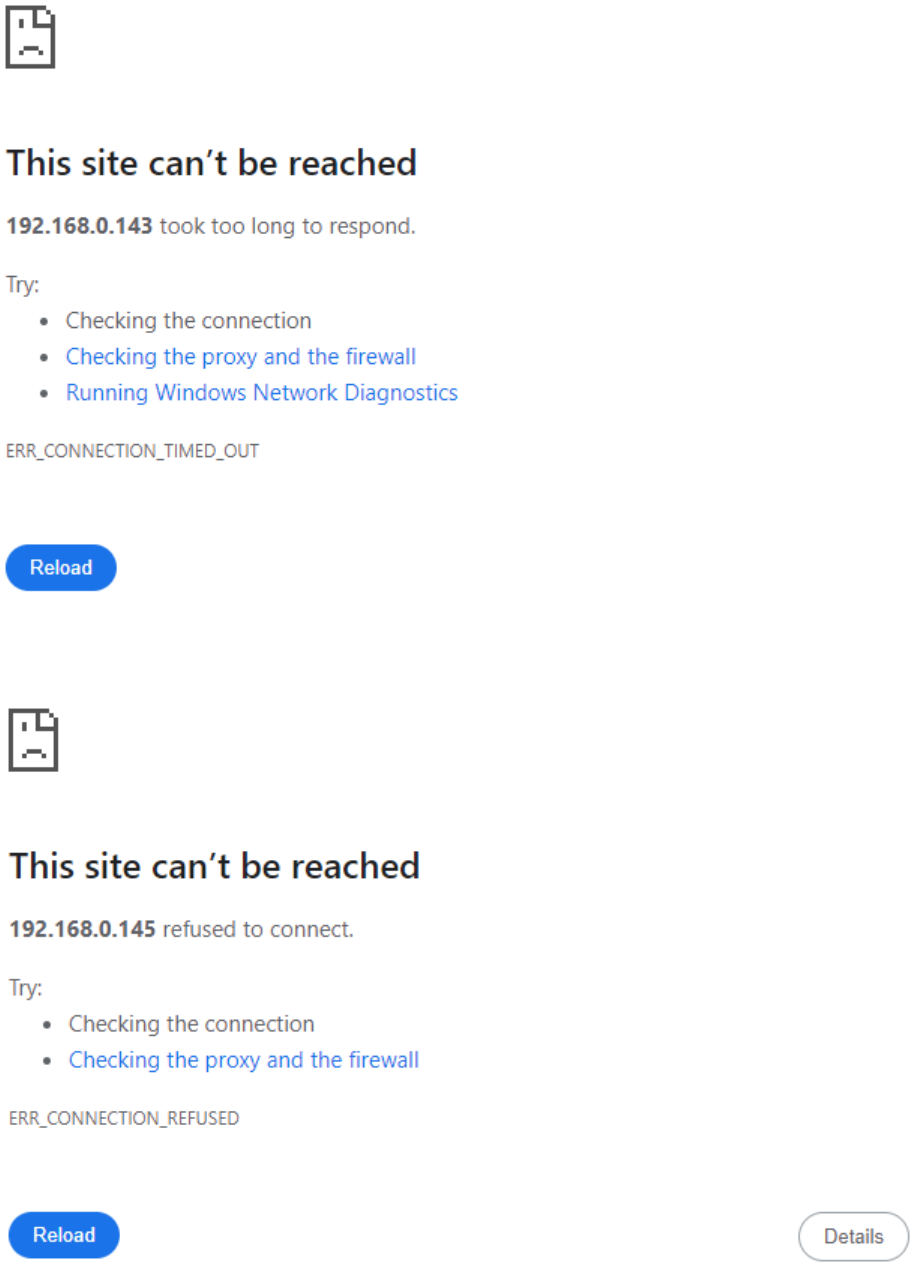
When connecting to a PowerChute Network Shutdown web UI, the connection fails with the error “this site can’t be reached.”

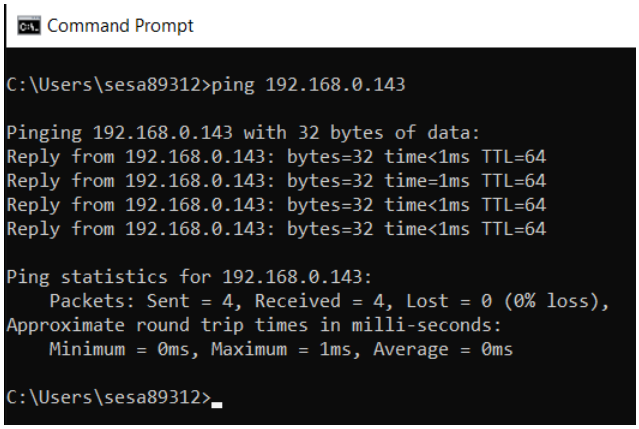


First, verify that the PowerChute service is running on the system. See Schneider Electric FAQ FA290624.

Next, verify that cookies are allowed by the browser. See Schneider Electric FAQ FA159729.

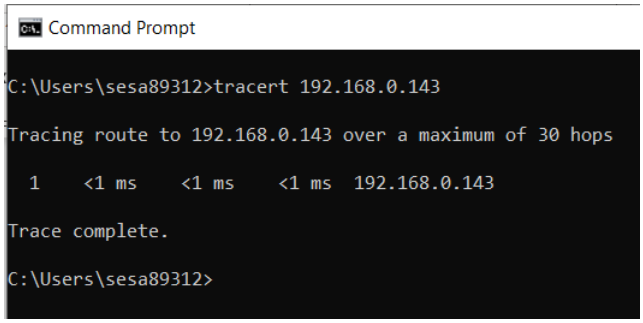
Next, verify that the proper IP address and port are being used. The correct port is TCP 6547.

Next, ping the PowerChute system.



If the system can be ping, run a traceroute to the PowerChute system.

From a Windows system, open a command prompt and enter the command tracert <IP address of the PowerChute system. Example: tracert 192.168.0.143



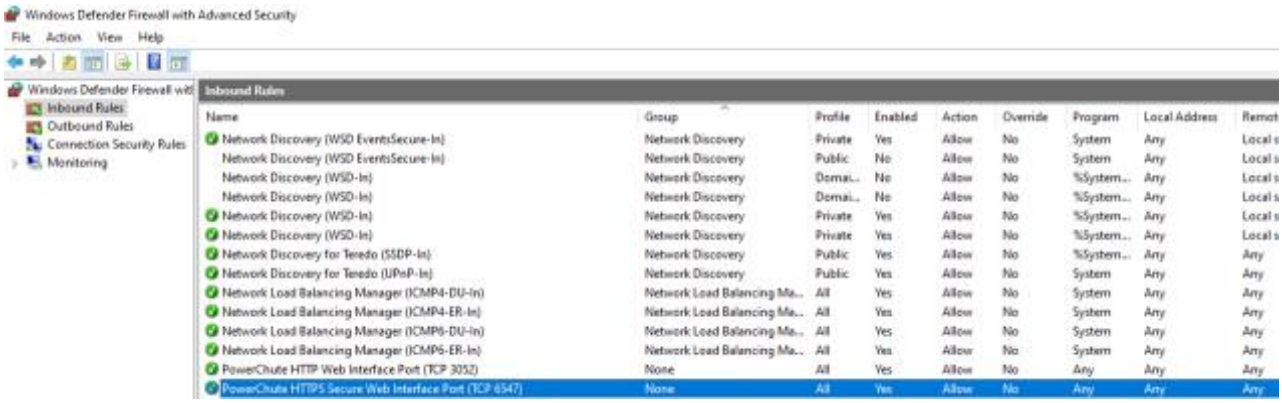
In the example above, there was only one switch between the Windows system and the PowerChute client.

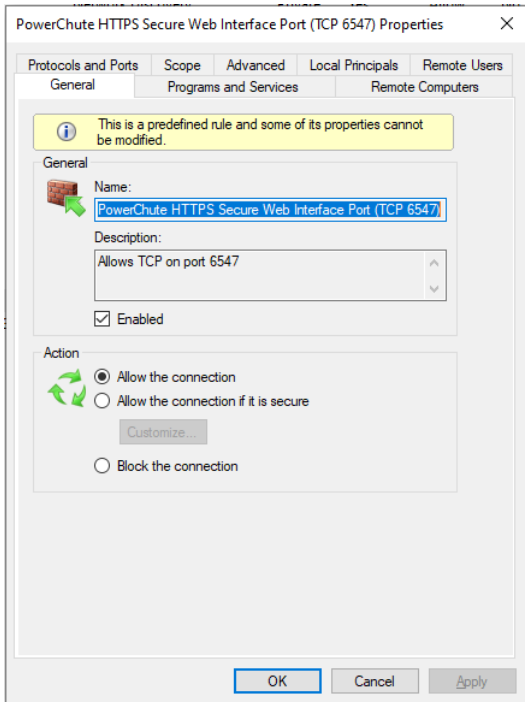
Windows OS

Next, verify that TCP port 6547 is open on the PowerChute system. The port is opened by default when the software is installed. On a Windows system, the user is asked if they would like to open the port. If the user selects no, the port is not opened, and a connection cannot be made to the PowerChute web UI. The port can be added manually if it is not available/opened. See Microsoft document Configure rules with a group policy.

The Profile should be All, Enabled Yes, Action Allow, Program Any, Local Address Any, Remote Address Any, Protocol TCP, Local Port 6547.

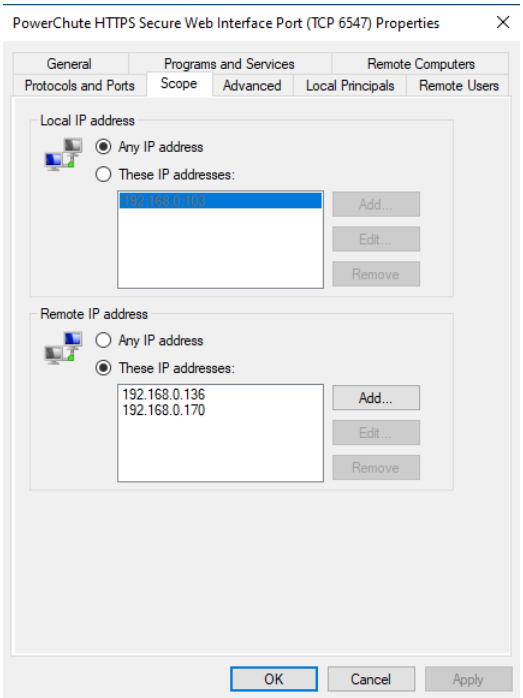
On a Windows system, open Control Panel, Windows Defender Firewall, Advanced setting, Inbound Rules.



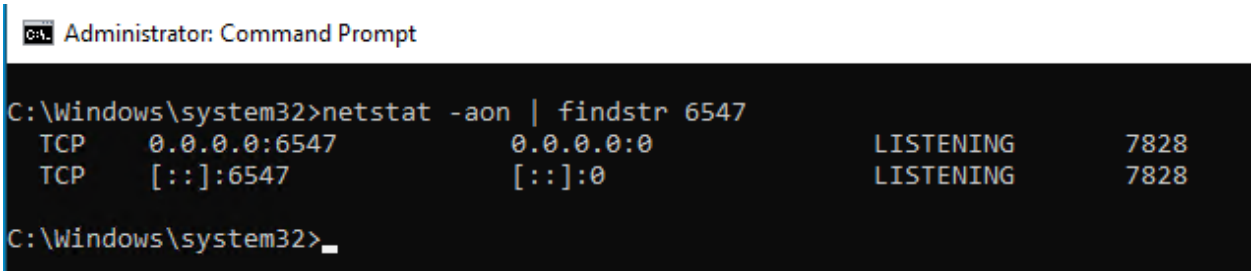


To improve security, change the Scope and add the specific IP address. Then, only those IP addresses will be

In the example below, we have restricted the connection to port 6547 to IP addresses 192.168.0.136 and remote system 192.168.0.170.



Check that port 6547 is open using the command prompt netstat -aon | findstr 6547.

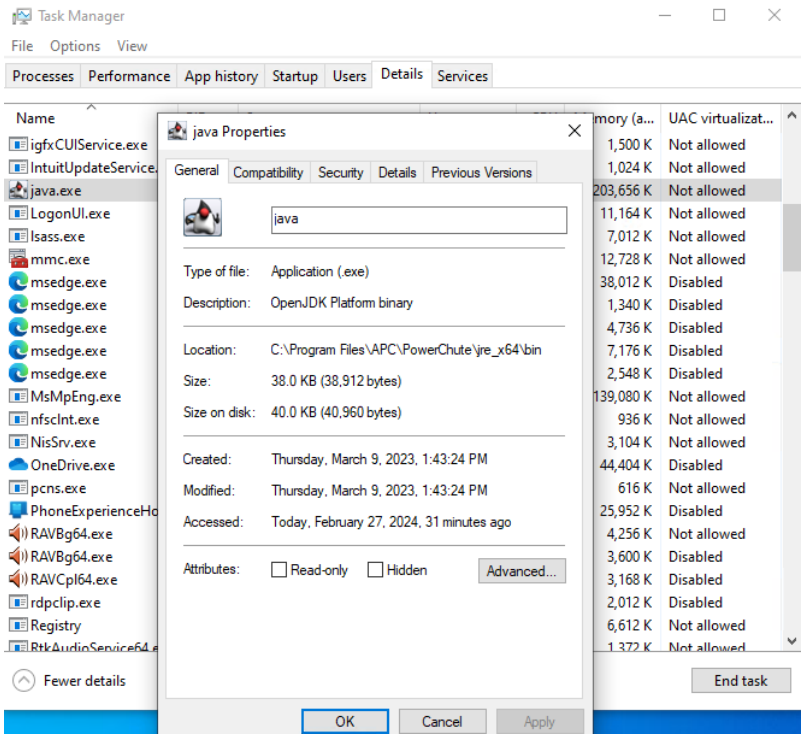


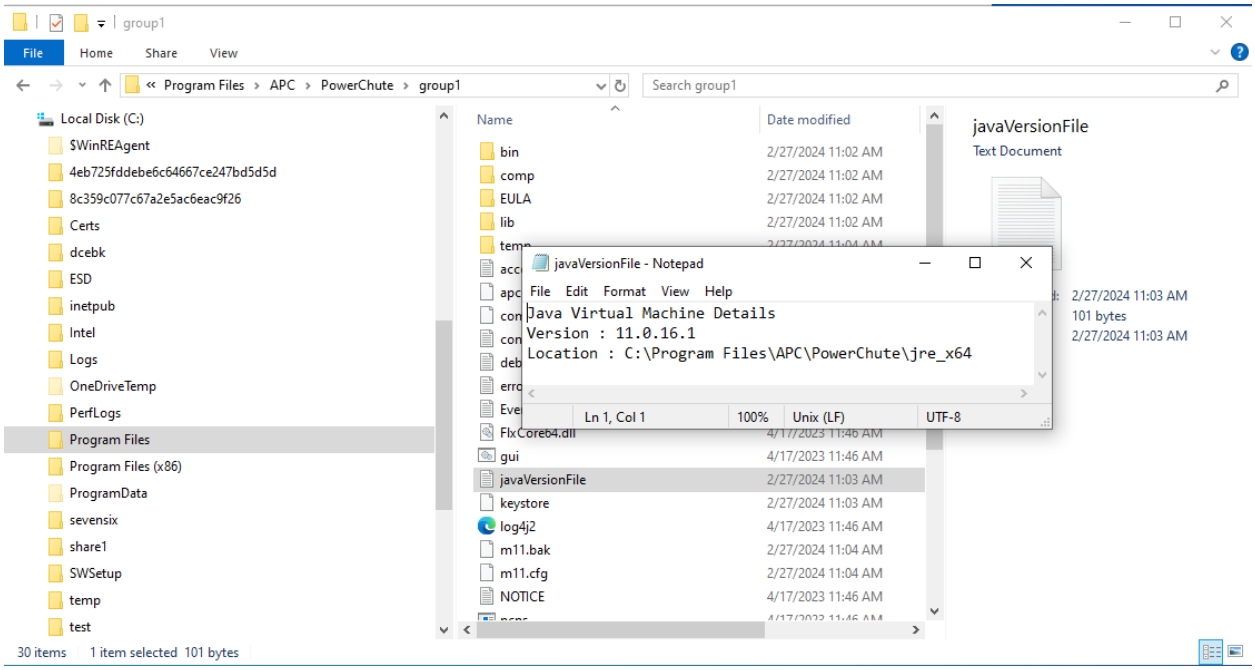
Verify PowerChute uses port 6547 via the command prompt; enter the command **tasklist | findstr [PID]**, replacing the [PID] with the process ID from the first command.

You should see the PID belongs to Java.

If you see multiple PIDs using port 6547, there will be an issue connecting to the PowerChute web UI. The other process must be stopped.

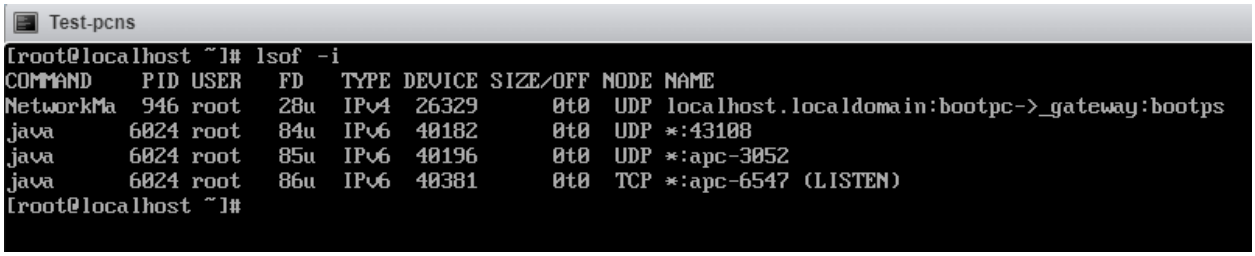
Check that the Java PID is for the version of Java PowerChute is using by running Task Manager. Open Task Manager, go to java.exe with the corresponding PID and Details and verify the location. Next, open the PowerChute folder, the default path of C:\Program Files\APC\PowerChute\group1, and open the Java versions file to check that the Java used by PowerChute is the same listed by Task Manager.





Linux OS

To test the PowerChute VM or a Linux system to verify that port 6547 is open, run the command **lsof -i**

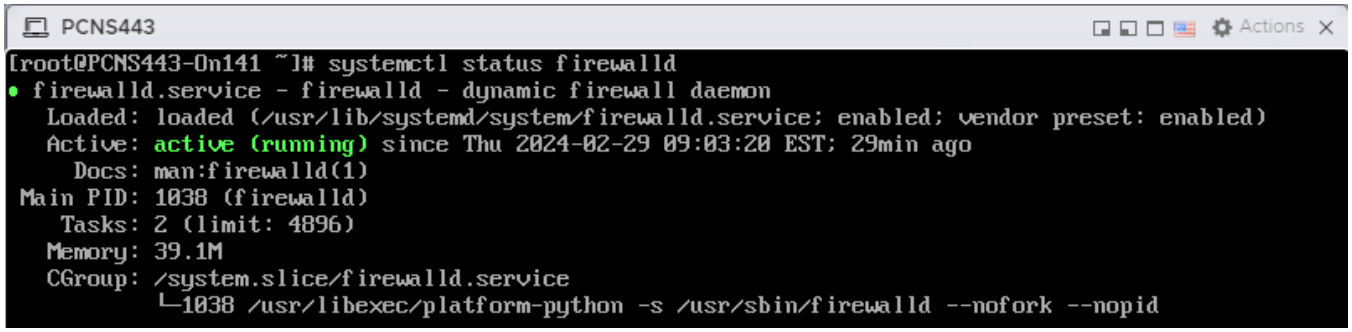


Note: the commands below are for the PowerChute AlmaLinux and CentOS VMs.

The command may be different for other Linux versions. For example, in Ubuntu 22, the command to check the firewall status is **sudo ufw status.**

If port 6547 is not open or if it is not available on the PowerChute VM, run the command.

systemctl status firewalld (to check the status of the firewall).



If the service is running, enter the command **firewall-cmd –list-port** (to view the ports in use)

If you do not see 6547/tcp, run the command **firewall-cmd –zone=public –add-port 6547/tcp**

The run the command **firewall-cmd –runtime-to-permanent.**

Finally, check the port status by running the **command firewall-cmd –list-ports.**