

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



This site can't be reached

192.168.0.143 took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload



This site can't be reached

192.168.0.145 refused to connect.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_REFUSED

Reload

Details

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.

```
Command Prompt
C:\Users\sesa89312>ping 192.168.0.143

Pinging 192.168.0.143 with 32 bytes of data:
Reply from 192.168.0.143: bytes=32 time<1ms TTL=64
Reply from 192.168.0.143: bytes=32 time=1ms TTL=64
Reply from 192.168.0.143: bytes=32 time<1ms TTL=64
Reply from 192.168.0.143: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.143:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\sesa89312>
```

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`

```
Command Prompt
C:\Users\sesa89312>tracert 192.168.0.143

Tracing route to 192.168.0.143 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  192.168.0.143

Trace complete.

C:\Users\sesa89312>
```

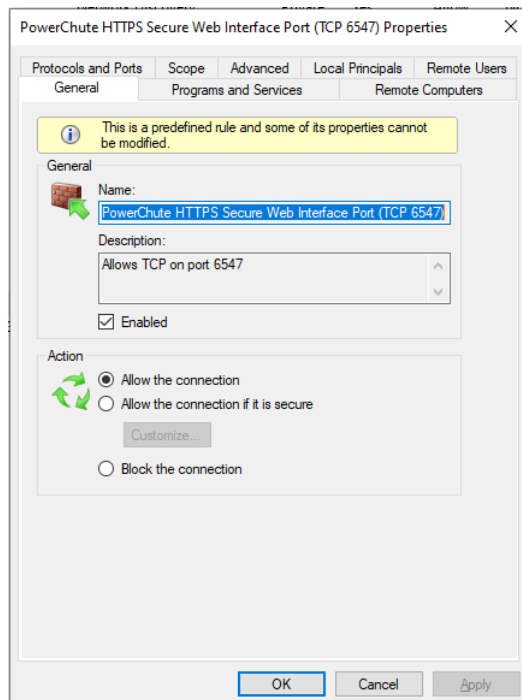
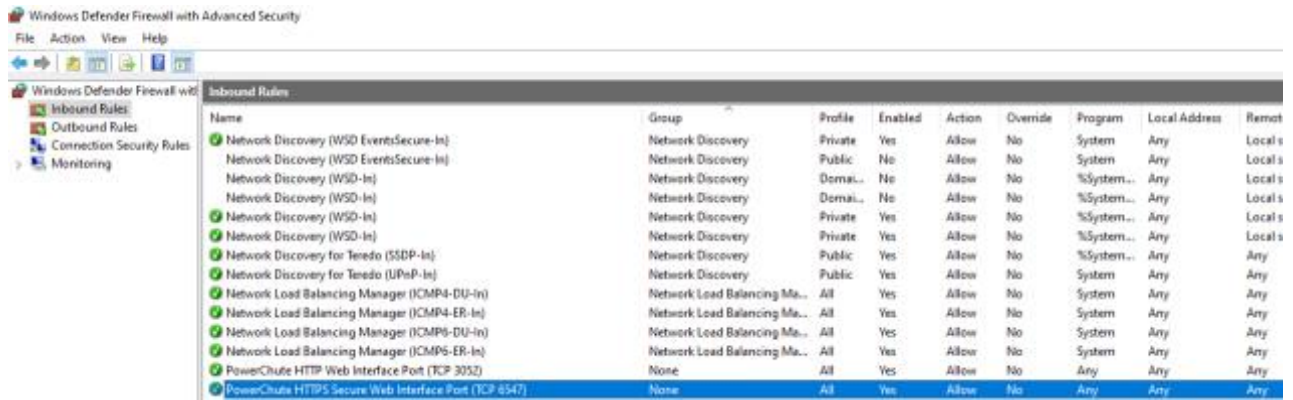
In the example above, there was only one switch between the Windows system and the PowerChute client.

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](#).

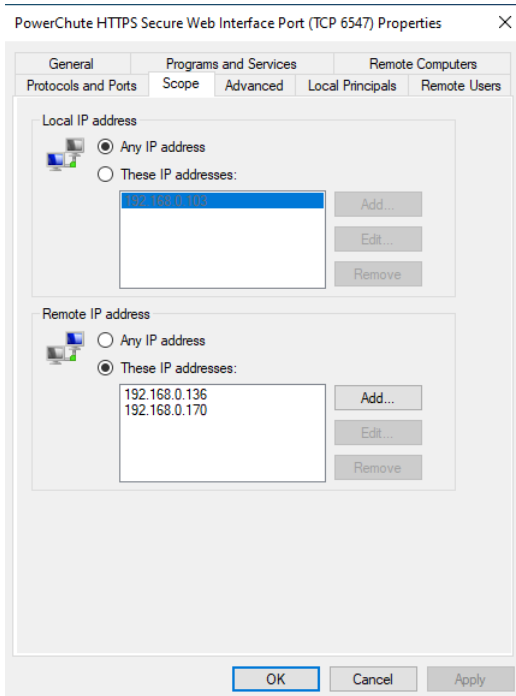
The Profile should be All, Enabled Yes, Action Allow, Program Any, Local Address Any, Remote Address Any, Protocol TCP, Local Port 6547.

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`.

```
Administrator: Command Prompt
C:\Windows\system32>netstat -aon | findstr 6547
TCP    0.0.0.0:6547      0.0.0.0:0        LISTENING      7828
TCP    [::]:6547       [::]:0           LISTENING      7828
C:\Windows\system32>
```

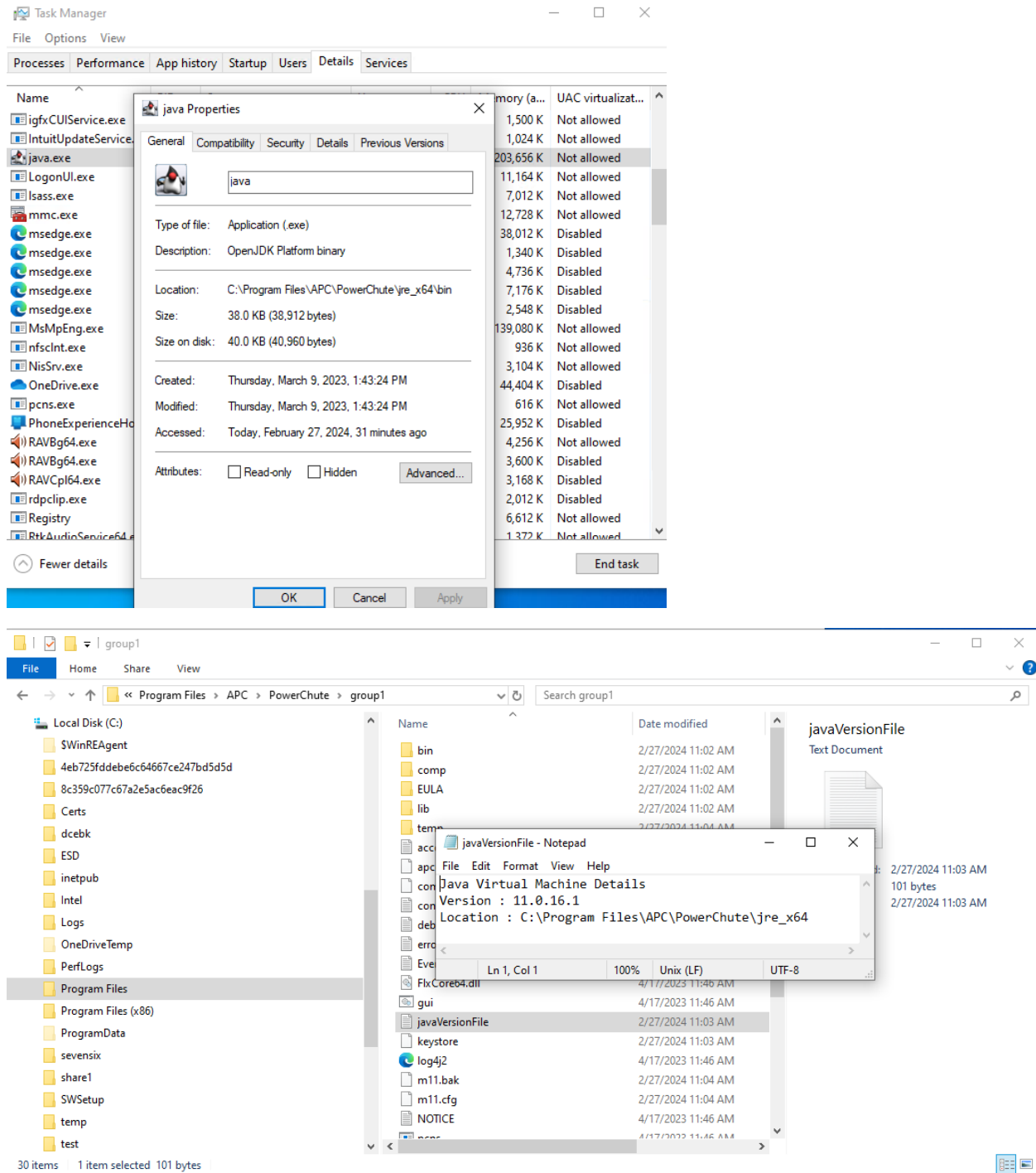
Verify PowerChute uses port 6547 via the command prompt; enter the command `tasklist | findstr [PID]`, replacing the [PID] with the process ID from the first command.

```
Administrator: Command Prompt
C:\Windows\system32>netstat -aon | findstr 6547
TCP    0.0.0.0:6547      0.0.0.0:0        LISTENING      7828
TCP    [::]:6547       [::]:0           LISTENING      7828
C:\Windows\system32>tasklist | findstr 7828
java.exe           7828 Services           0      237,536 K
C:\Windows\system32>
```

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`

```
Test-pcns
[root@localhost ~]# lsof -i
COMMAND  PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
NetworkMa 946 root  28u IPv4  26329      0t0  UDP localhost.localdomain:bootpc->_gateway:bootps
java      6024 root  84u IPv6  40182      0t0  UDP *:43108
java      6024 root  85u IPv6  40196      0t0  UDP *:apc-3052
java      6024 root  86u IPv6  40381      0t0  TCP *:apc-6547 (LISTEN)
[root@localhost ~]#
```

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).

```
PCNS443
[root@PCNS443-0n141 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-02-29 09:03:20 EST; 29min ago
     Docs: man:firewalld(1)
  Main PID: 1038 (firewalld)
    Tasks: 2 (limit: 4896)
   Memory: 39.1M
    CGroup: /system.slice/firewalld.service
            └─1038 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid
```

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

```
[root@PCNS443-0n141 ~]# firewall-cmd --list-ports
80/tcp 443/tcp 3052/tcp 6547/tcp 80/udp 161/udp 162/udp 3052/udp
[root@PCNS443-0n141 ~]#
```

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`.

```
[root@localhost ~]# firewall-cmd --zone=public --add-port 6547/tcp
success
[root@localhost ~]# firewall-cmd --runtime-to-permanent
success
[root@localhost ~]# firewall-cmd --list-ports
6547/tcp
[root@localhost ~]#
```