

# How to troubleshoot “Error registering with the Network Management Card” When running the PowerChute Virtual Machine or PowerChute on a Linux system.

First, review the error to determine the cause.

If the error reports “Security information is incorrect.”

The error is reported if the PowerChute Username or the Authentication Phrase is incorrectly set on the Network Management Card or the PowerChute web UI.

## PowerChute Setup: Network Management Card Registration

Please wait while PowerChute registers with the Network Management Card(s). This may take a few minutes.

Error registering with the Network Management Card(s).



192.168.0.128

Security information for <https://192.168.0.128:443> is incorrect. Please check that the PowerChute User Name and Authentication Phrase match the Network Management Card.

Show Log

The Username entered in the PowerChute Parameters and the Authentication Phrase must match the Username and Authentication Phrase entered in the PowerChute web UI setup. To view the PowerChute Parameters on the Network Management Card, log into the card and go to Configuration and Shutdown; at the bottom of the page, you will see the PowerChute Parameters.

Below is the PowerChute Setup Security page from the PowerChute web UI.

## PowerChute Setup: Security

These details will be used for logging into PowerChute and for authentication with the Network Management Card.

User Name

Password

Authentication Phrase

If HTTPS or HTTP is not enabled, you must enable the one you will use for communication in the PowerChute Parameters to allow a connection. If HTTP or HTTPS are not enabled, you will see the error Cannot connect to https://ip address:443 or HTTP://ip address:80.

### PowerChute Setup: Network Management Card Registration

---

Please wait while PowerChute registers with the Network Management Card(s). This may take a few minutes.

Error registering with the Network Management Card(s).



**192.168.0.128**

Cannot connect to <https://192.168.0.128:443>

Show Log

#### PowerChute Shutdown Parameters

##### Maximum Required Delay

Force negotiation

##### On-Battery Shutdown Behavior

Restart when power is restored

Turn off and stay off

Ignore PCNS shutdown commands

##### User Name

PCNSadmin

##### Authentication Phrase

#### PCNS Communication Protocols

##### HTTP

Enable

##### HTTPS

Enable

Apply

Cancel

If you see the error "PowerChute is not receiving data from the Network Management Card." That indicates UDP port 3052 is blocked, or the PowerChute client and network Management Cards have mismatched subnet masks. The NMC sends data to the PowerChute clients using UDP port 3052. PowerChute will not receive the data if the port is blocked anywhere along the network path.

### PowerChute Setup: Network Management Card Registration

---

Please wait while PowerChute registers with the Network Management Card(s). This may take a few minutes.

Error registering with the Network Management Card(s).



**192.168.0.128**

PowerChute is not receiving data from the Network Management Card. [More information](#)

Show Log

Note 1: If configuring PowerChute with Redundant or Advanced UPSs, refer to Schneider Electric FAQ000259214, along with the steps below.

Note 2: If configuring PowerChute with a Galaxy VL running firmware 10.11.0 & Galaxy VS with firmware 6.72.0, the Network Management Card must be reset after configuration, or PowerChute will report “not receiving data.”

By default, ports 3052 and 6547 are open on the PowerChute VM. When installing PowerChute on any other system, the user is asked to allow the installer to open the needed ports. If, when installing on another system, the user disallows the ports opening, they cannot access the web UI, and PowerChute will not receive data from the NMC/s.

To resolve the issue “PowerChute is not receiving data,” check that PowerChute has opened UDP port 3052 in the PowerChute web UI,

**PowerChute™**  
— NETWORK SHUTDOWN

Home Configuration UPS Configuration Help

Event Log

Delete Log File Export Log

Display 20 events

Events 1 to 5 of 5

Date	Time	Event
01/19/2024	13:45:08	PowerChute successfully accessed TCP port 6547.
01/19/2024	13:45:08	PowerChute is attempting to access TCP port 6547.
01/19/2024	13:44:54	PowerChute Network Shutdown version 5.0.0 monitoring started.
01/19/2024	13:44:54	PowerChute successfully accessed UDP port 3052.
01/19/2024	13:44:54	PowerChute is attempting to access UDP port 3052.

To test the PowerChute VM or a Linux system to verify the ports are 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 ~]#
```

Verify that the PowerChute system and Network Management card/s have compatible subnet masks.

To view the PowerChute network information, enter the command `ip a`.

```
Test-pcns
Welcome to PowerChute Network Shutdown 5.0.0 for VMware
Please complete the PowerChute Setup wizard to ensure that your VMware Hosts and Virtual Machines
are protected.
To configure PowerChute Network Shutdown using the Setup Wizard, browse to:
https://192.168.0.182:6547/
Test-pcns login: root
Password:
[root@Test-pcns ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:9b:dd:ba brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.0.182/24 brd 192.168.0.255 scope global dynamic noprefixroute ens192
        valid_lft 7063sec preferred_lft 7063sec
    inet6 fe80::250:56ff:fe9b:ddba/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@Test-pcns ~]#
```

To view the Network Management Card setting, log into the card and go to Configuration > Network > TCP/IP

The screenshot shows a web interface with a green navigation bar containing: Home, Status, Control, Configuration, Tests, Logs, About. Below the navigation bar is the "IPv4 Settings" section. It contains a table titled "Current IPv4 Settings" with the following data:

System IP	Subnet Mask	Default Gateway	MAC Address
192.168.0.128	255.255.255.0	192.168.0.1	28 29 86 1C 73 98
Mode	DHCP Server:	Lease Acquired	Lease Expires
DHCP	192.168.0.1	12/01/2023 11:09	01/20/2024 04:12

In the examples above, the PowerChute system shows the subnet to be /24, which equals 255.255.255.0, which matches the Network Card setting. Also, the broadcast address is 192.168.0.255, so PowerChute will listen for broadcast messages from that address. The Network Card sends the UDP packets to the broadcast address 192.168.0.255.

To verify that the PowerChute VM or Linux system receives packets from a Network Management Card, install and run the utility tcpdump. To install on the PowerChute VM, enter the command **dnf install tcpdump**.

**NOTE:** To install the tcpdump utility, the PowerChute VM must have internet access.

```
Test-pcns
[root@localhost ~]# dnf install tcpdump
AlmaLinux 8 - BaseOS
AlmaLinux 8 - AppStream
AlmaLinux 8 - Extras
Dependencies resolved.
=====
Package                                Architecture                            Version
=====
Installing:
tcpdump                                x86_64                                  14:4.9.3-3.e18
Transaction Summary
=====
Install 1 Package

Total download size: 452 k
Installed size: 1.1 M
Is this ok [y/N]: y
Downloading Packages:
tcpdump-4.9.3-3.e18.x86_64.rpm
=====
Total
AlmaLinux 8 - AppStream
Importing GPG key 0xC21AD6EA:
  Userid      : "AlmaLinux <packager@almalinux.org>"
  Fingerprint: E53C F5EF 91CE B0AD 1812 ECB8 51D6 647E C21A D6EA
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-AlmaLinux
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :
  Running scriptlet: tcpdump-14:4.9.3-3.e18.x86_64
  Installing     : tcpdump-14:4.9.3-3.e18.x86_64
  Running scriptlet: tcpdump-14:4.9.3-3.e18.x86_64
  Verifying      : tcpdump-14:4.9.3-3.e18.x86_64

Installed:
  tcpdump-14:4.9.3-3.e18.x86_64

Complete!
[root@localhost ~]#
```

Next, run the command **tcpdump -w traffic.pcap** to capture network traffic to and from the system. Wait 3 to 4 minutes and then enter Ctrl C. to stop the capture. A file with the name traffic.pcap will be created in the present working directory.

```

Test-pcns
[root@localhost ~]# tcpdump -w traffic.pcap
dropped privs to tcpdump
tcpdump: listening on ens192, link-type EN10MB (Ethernet), capture size 262144 bytes
^C149 packets captured
149 packets received by filter
0 packets dropped by kernel
[root@localhost ~]# _

```

```

Test-pcns
[root@localhost ~]# pwd
/root
[root@localhost ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg  kickstart-post.log  original-ks.cfg  traffic.pcap
[root@localhost ~]# _

```

To review the capture, run the command **tcpdump -r traffic.pcap** and search for UDP packets from the Network Management Card. In the example below, the capture shows UDP packets from IP address 192.168.0.128, 3052: UDP. The IP address shown is that of a test Network Management Card.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.128	192.168.0.255	UDP	775	45843 → 3052 Len=733
2	3.165674	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
3	10.581907	192.168.0.1	224.0.0.1	IGMPv2	60	Membership Query, general
4	13.265528	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
5	14.318372	192.168.0.166	192.168.0.255	UDP	854	36364 → 3052 Len=812
6	22.057749	Dell_cc:4c:ad	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.120 (Reply)
7	23.389452	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
8	25.500552	192.168.0.128	192.168.0.255	UDP	562	63747 → 3052 Len=520
9	33.481570	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
10	40.099940	192.168.0.166	192.168.0.255	UDP	854	45358 → 3052 Len=812
11	43.593574	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357
12	51.001986	192.168.0.128	192.168.0.255	UDP	775	42174 → 3052 Len=733
13	52.417178	Dell_cc:4c:ad	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.120 (Reply)
14	53.769494	192.168.0.1	255.255.255.255	UDP	399	48613 → 29810 Len=357

**NOTE:** The file traffic.pcap can be viewed on a Windows system with the Wireshark application if Wireshark is available, as shown above.