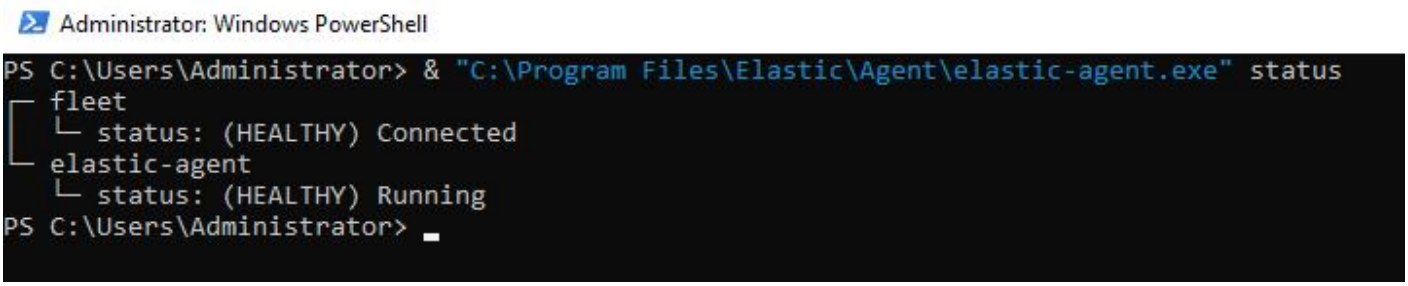
AQUILA EDR Connection Issues - Windows

When Elastic Agent installs Endpoint, they connect locally to share status and updates. If this connection fails, Elastic Agent shows as Unhealthy, and Endpoint won’t work properly.

How to Check if There's a Problem

1. **Check Agent Status**
   Open PowerShell as Administrator and run:

```
& "C:\Program Files\Elastic\Agent\elastic-agent.exe" status
```



Look for messages like:

- Endpoint has missed check-ins
- localhost:6788 cannot be bound to

2. **Check Endpoint Settings**
   Open this file:

```
C:\Program Files\Elastic\Endpoint\elastic-endpoint.yaml
```

Find the line that says fleet.agent.id.
If the value is 00000000-0000-0000-0000-000000000000, the connection failed.

Check the Logs

Look for these messages in the Endpoint logs:

- Failed to find connection to validate. Is Agent listening on 127.0.0.1:6788?

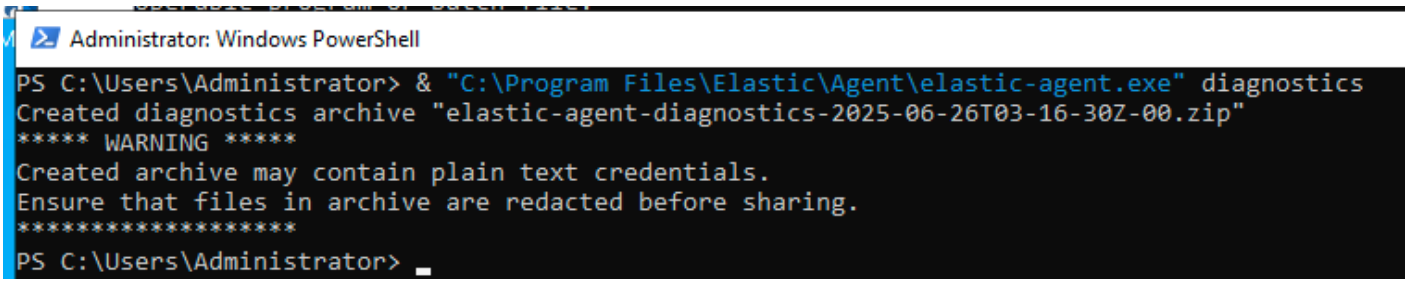
- Failed to validate connection. Is Agent running as root/admin?
- Unable to make GRPC connection in deadline(60s)

These show a connection problem between Agent and Endpoint.

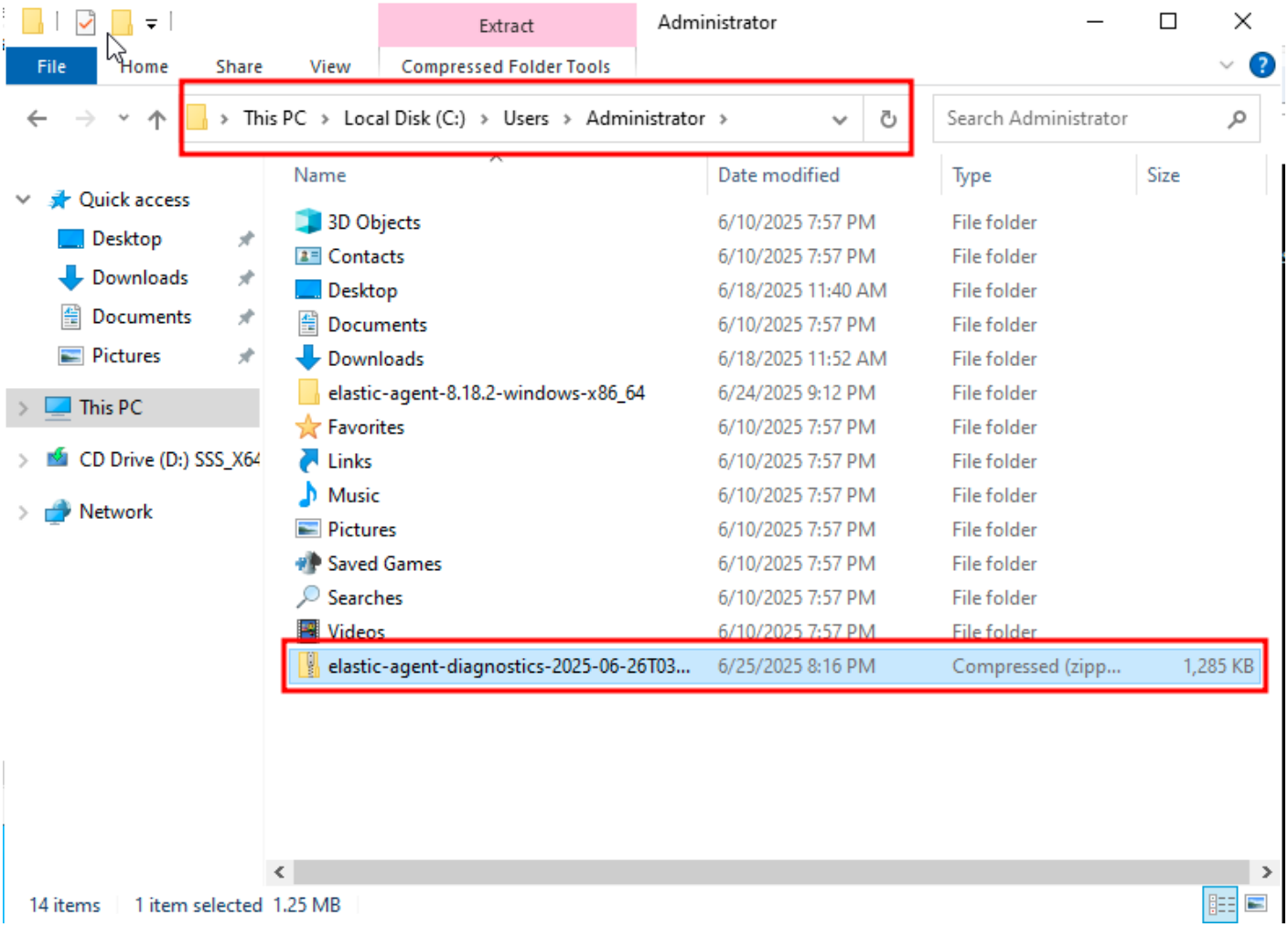
How to Fix It

1. **Run Diagnostics**
   Run this command on PowerShell as Administrator:

```
& "C:\Program Files\Elastic\Agent\elastic-endpoint.exe" diagnostics
```



Follow this file path to retrieve the Diagnostics Zip file created.



This will generate a report with possible causes.

2. **Check if Ports Are Used by Something Else**
   Run these:

```
netstat -an | findstr :6788
```

```
netstat -an | findstr :6789
```

If another program is using these ports, it could block the connection.

3. **Test if Localhost Works**
   Run this:

```
ping -4 localhost
```

It should respond with 127.0.0.1

Reference Link: https://www.elastic.co/guide/en/security/8.18/ts-management.html

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #2
Created 25 June 2025 09:45:09 by Richmond Abella
Updated 25 June 2025 12:20:35 by Kent Lauron