

Troubleshooting



Richard Hicks

Richard M. Hicks Consulting, Inc.

@richardhicks www.richardhicks.com



Overview



Troubleshooting

Overview

- Error codes
- Common causes
- Tools and techniques



Troubleshooting



Finding Error Messages

Client event log

Server event log

rasphone.exe

rasdial.exe



NPS Auditing

```
# // View NPS event auditing settings
```

```
auditpol.exe /get /subcategory:"Network Policy Server"
```

```
# // Enable NPS event auditing
```

```
auditpol.exe /set /subcategory:"Network Policy Server" /success:enable /failure:enable
```



Common Error Codes

809

Can't connect

812

Can't authenticate

13801

**IKE authentication
failure**

13806

IKE certificate issue

13868

IPsec policy mismatch



Demo



Troubleshooting

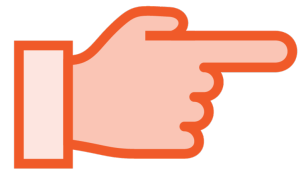


Validate SSTP with PowerShell

```
Invoke-WebRequest -Method Head -Uri 'https://vpn.example.net/sra_{BA195980-CD49-458b-9E23-C84EE0ADC75}/' -UseBasicParsing
```



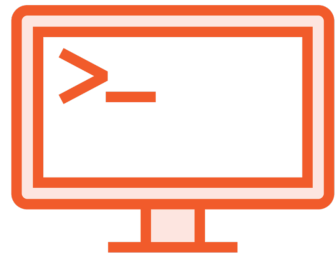
Error 809 and IKEv2



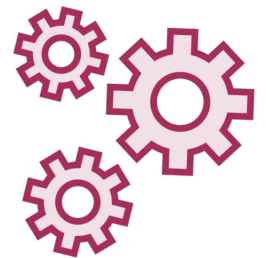
IKEv2 uses UDP



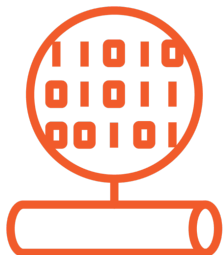
Can't use Test-NetConnection



Command line network trace



Pktmon.exe (Windows client and Server 2019 and later)



Netsh.exe (Windows Server 2016 and earlier)



Command Line Network Trace

```
# // best option
```

```
pktmon.exe start -c -f c:\$env:computername.etl --pkt-size 0 --comp nics --flags 0x10  
pktmon.exe stop
```

```
pktmon.exe etl2pcap capturefile.etl
```

```
# // legacy systems
```

```
netsh.exe trace start capture=yes tracefile=c:\$env:computername.etl  
netsh.exe trace stop
```



NPS communication failure can
result in error 812.



Expired CRLs can result in
error 13801.



Error 13868 Registry Entry

HKLM\SYSTEM\CurrentControlSet\Services\RasMan\Parameters\NegotiateDH2048_AES256 = 1



Summary



Troubleshooting

Summary

- Common errors
- Native tools
- Non-standard configuration

