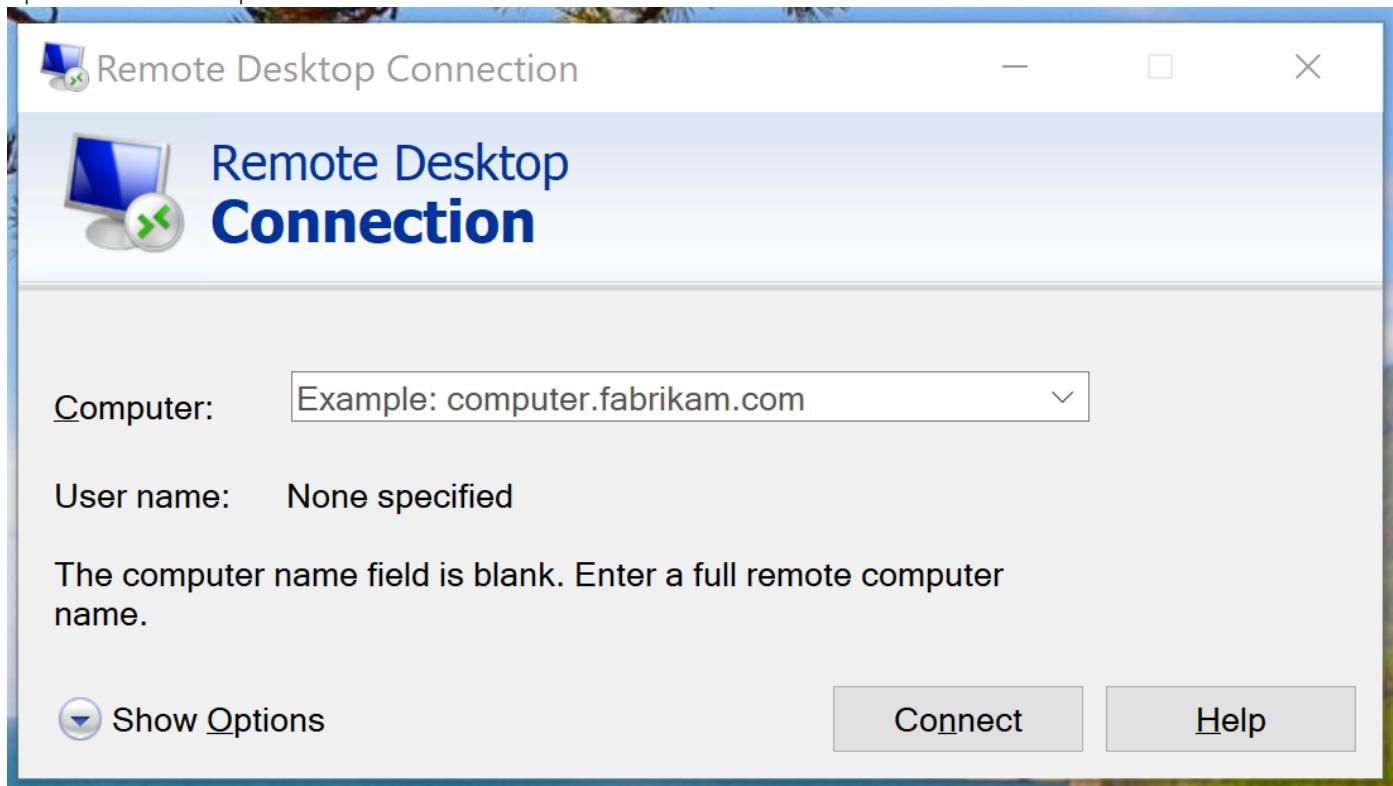


n4-super-installer

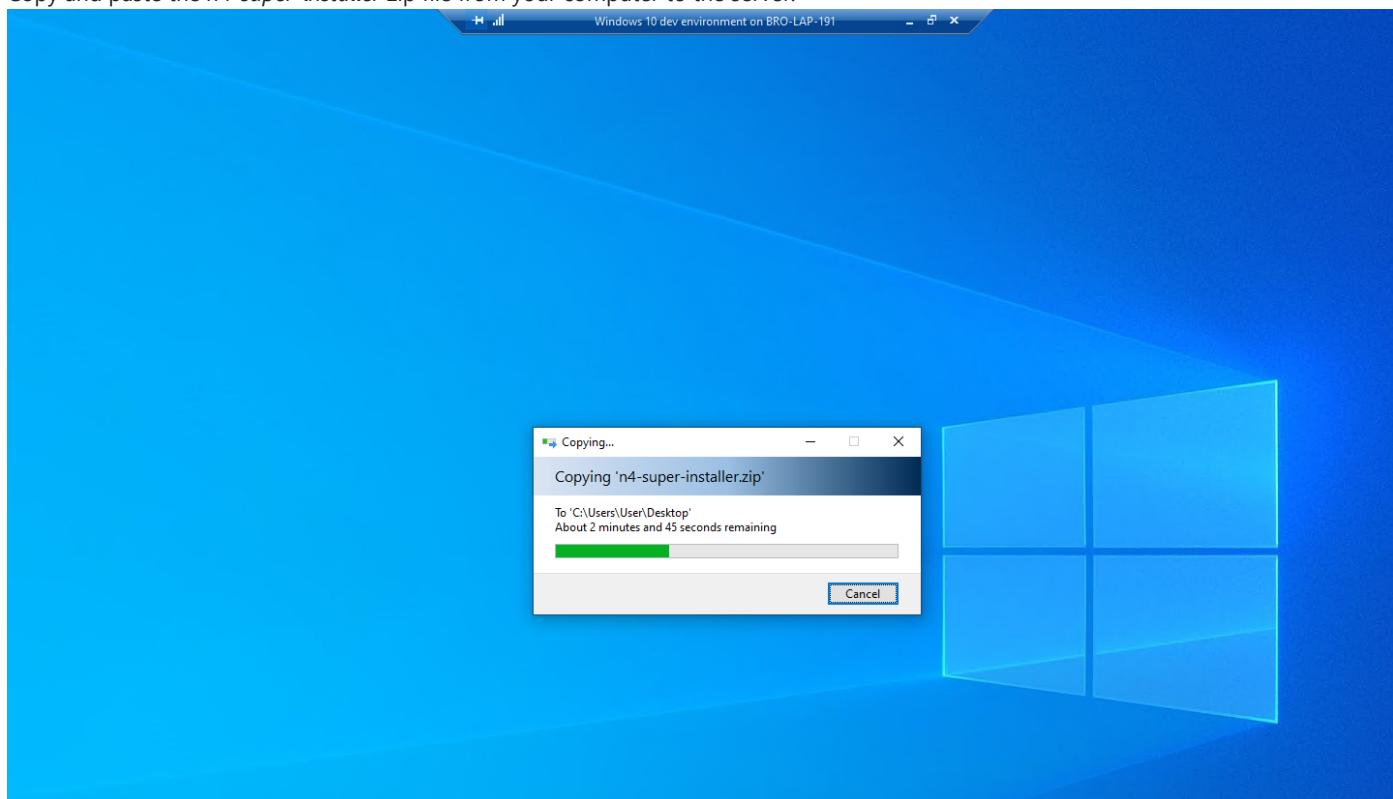
This powershell script automates portions of the installation process for an N4 Supervisor.

Directions of use

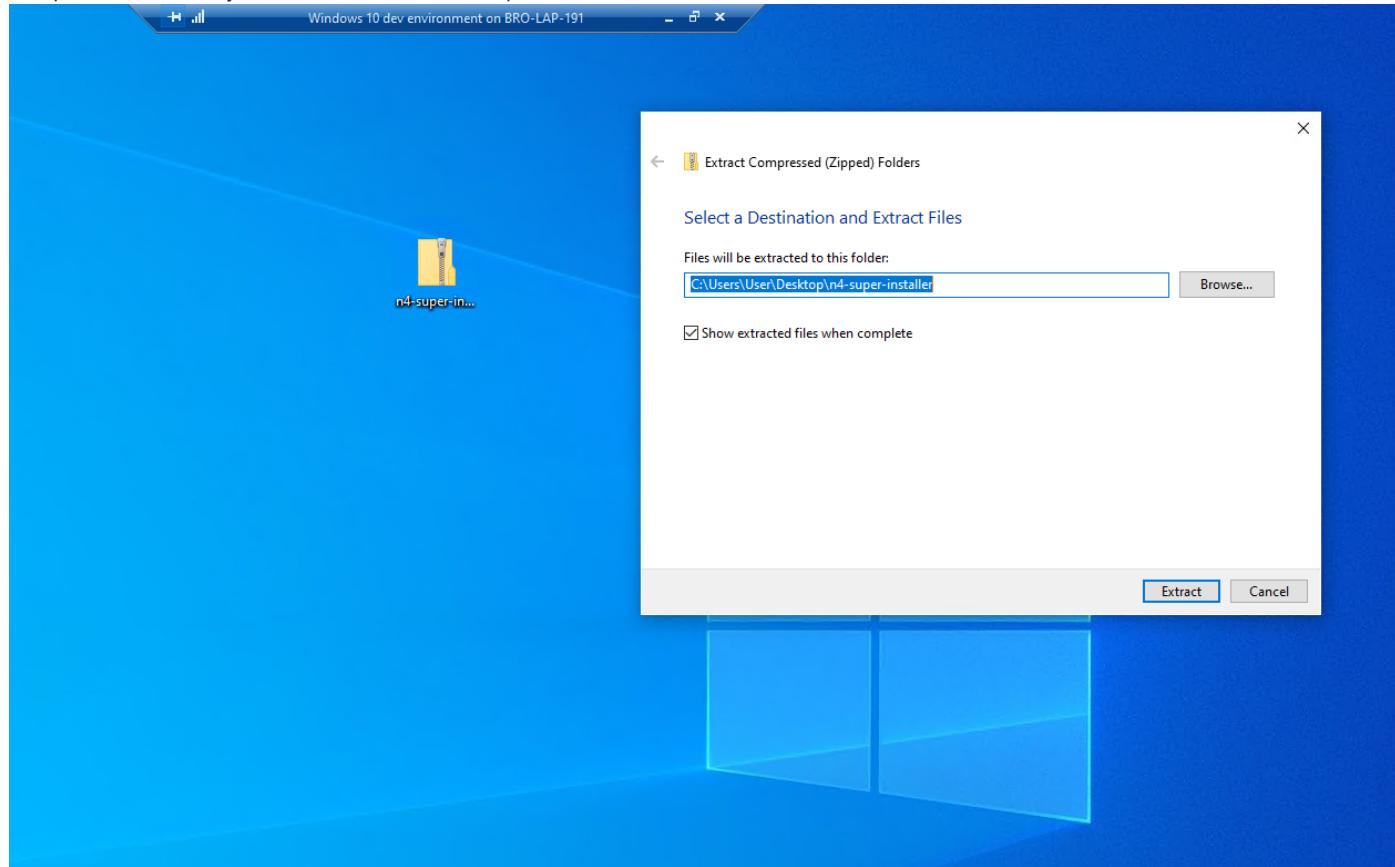
1. Open a Remote Desktop Connection with the server



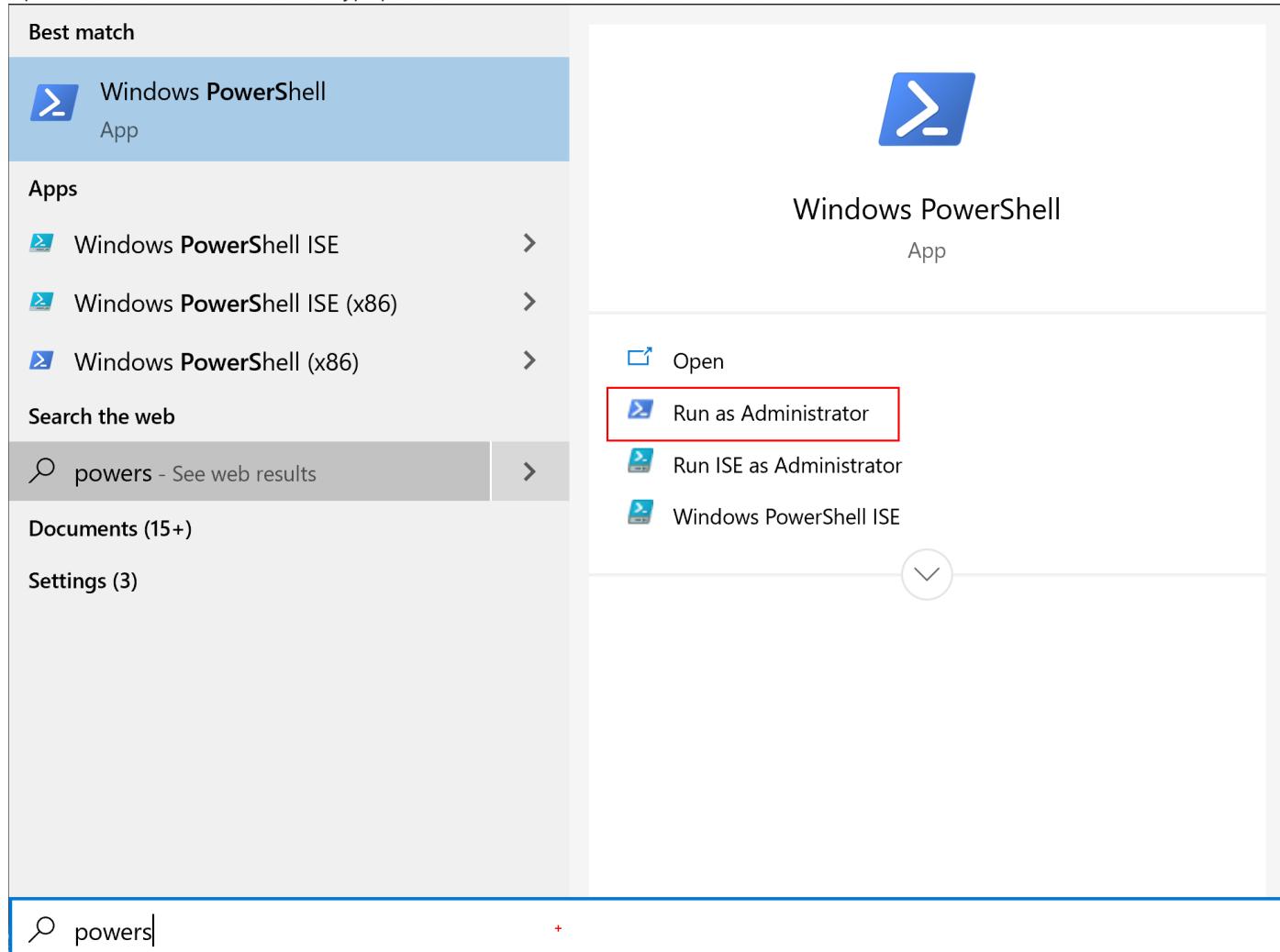
2. Copy and paste the *n4-super-installer* zip file from your computer to the server.



3. Unzip the installer on your Windows user's desktop.



4. Open the Windows Start Menu and type *powershell*, then select Run As Administrator

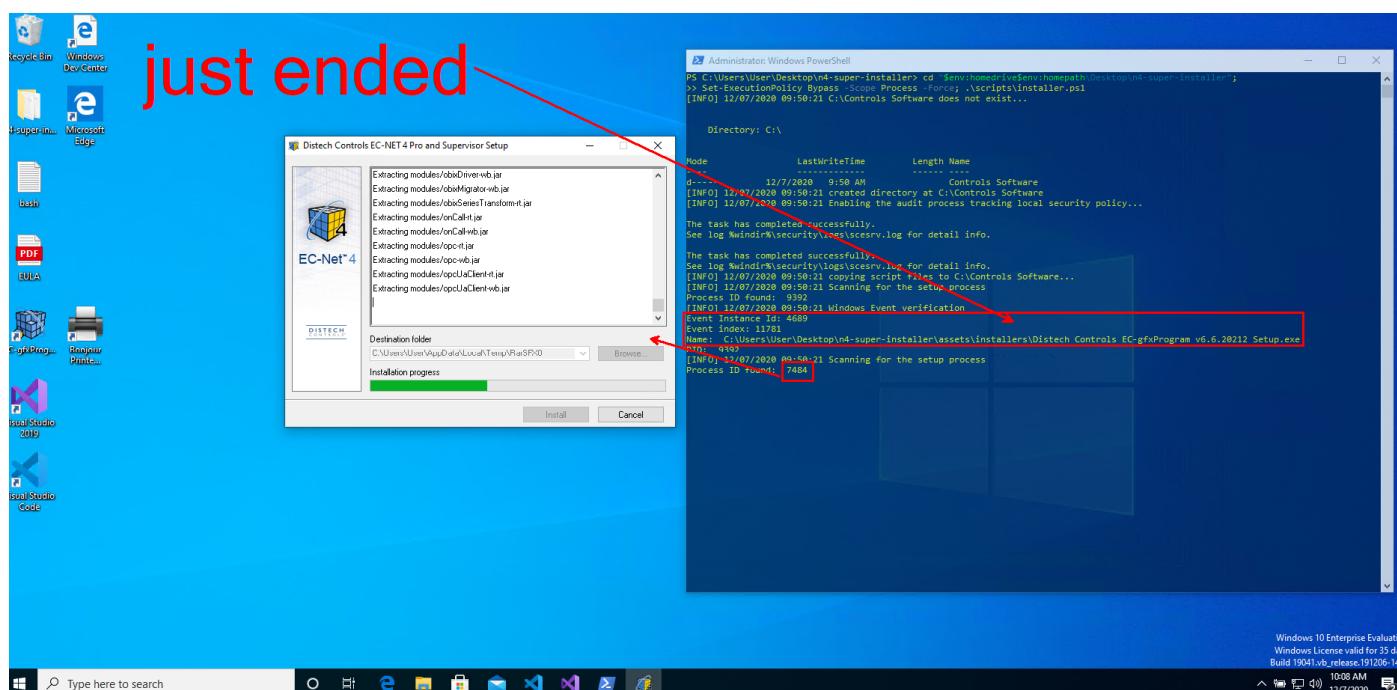
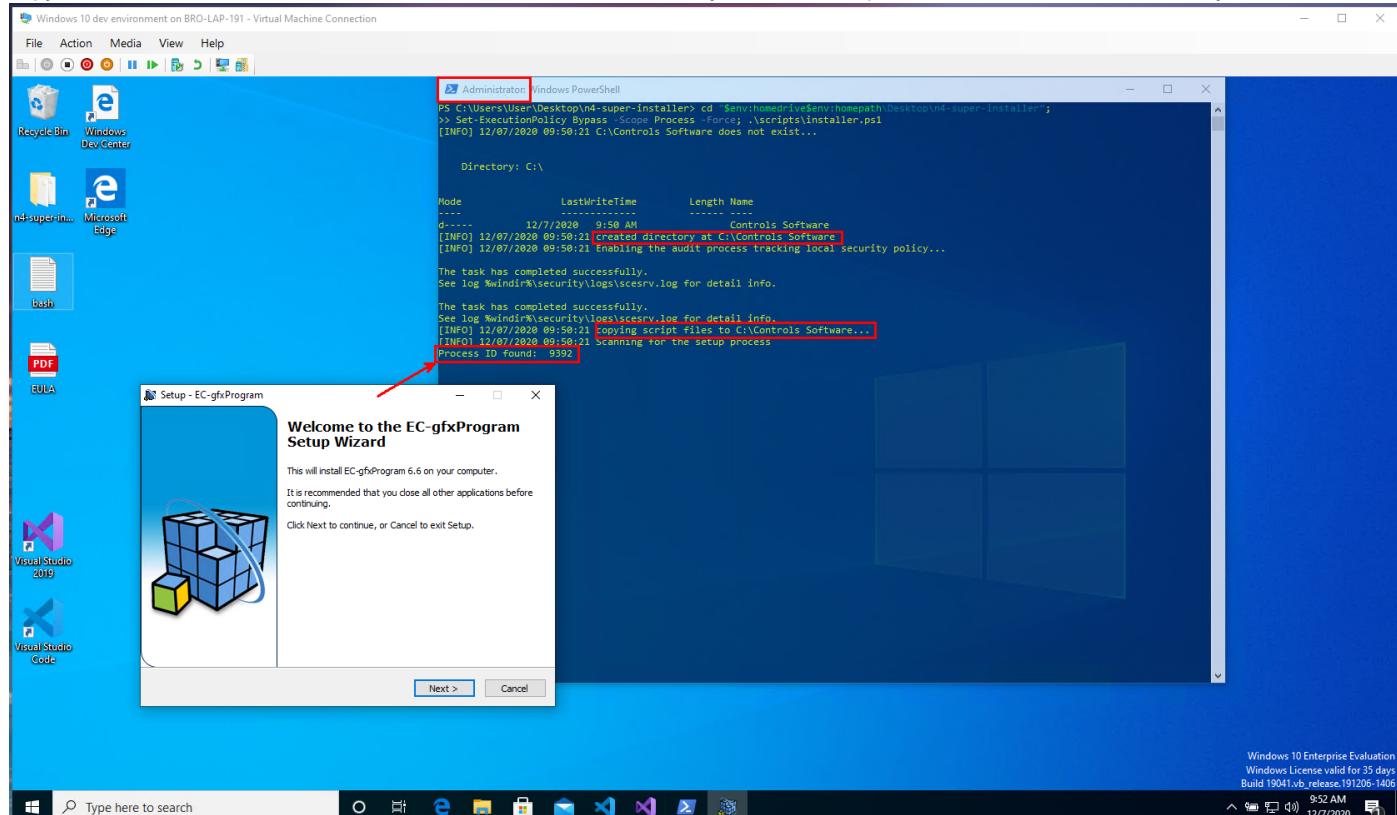


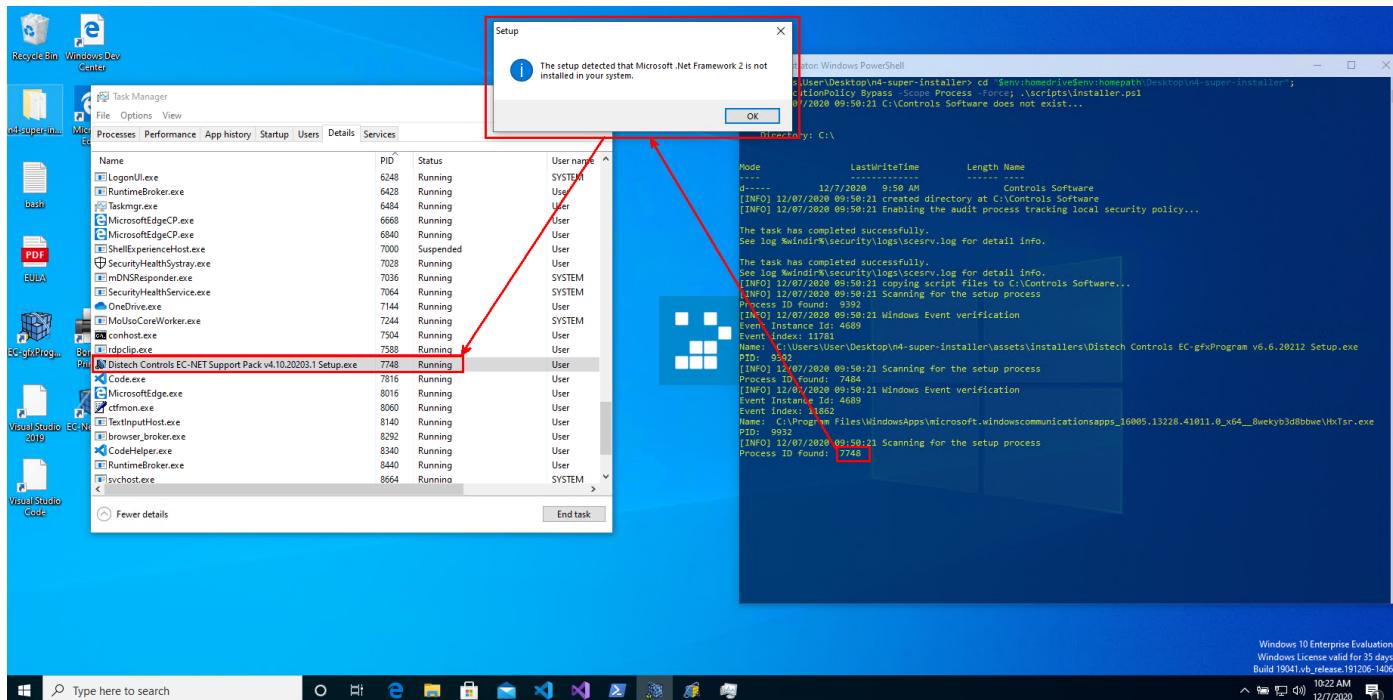
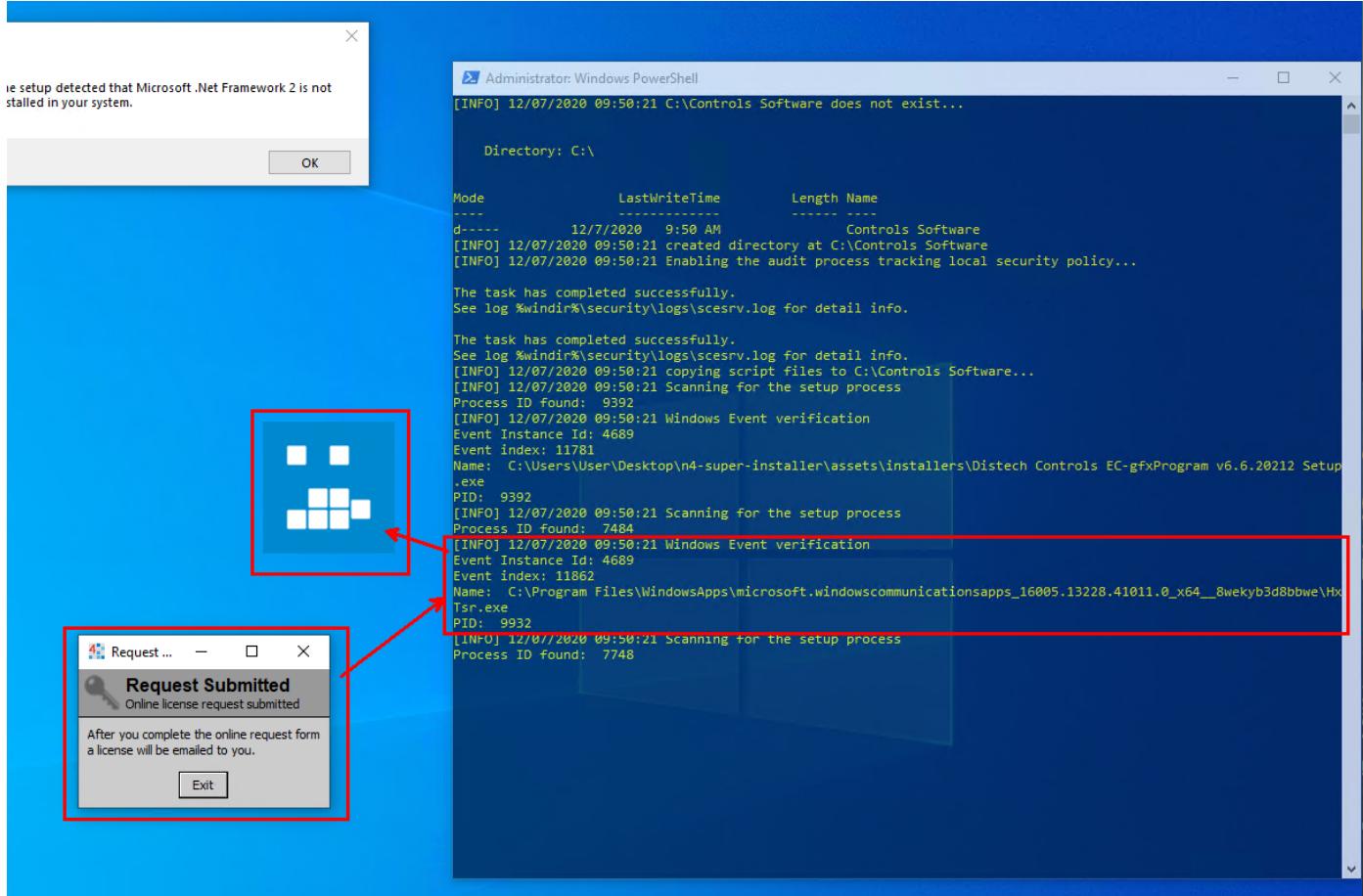
5. Copy the code below, and paste it on the Powershell blue command prompt:

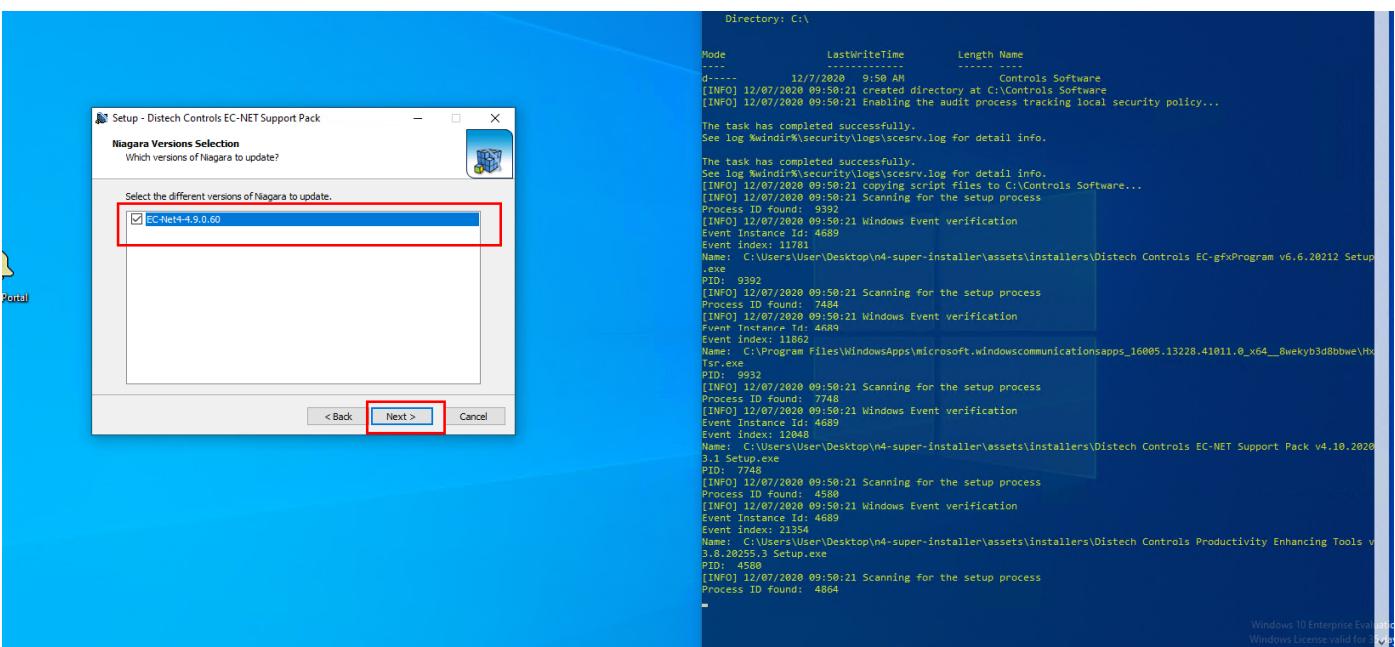
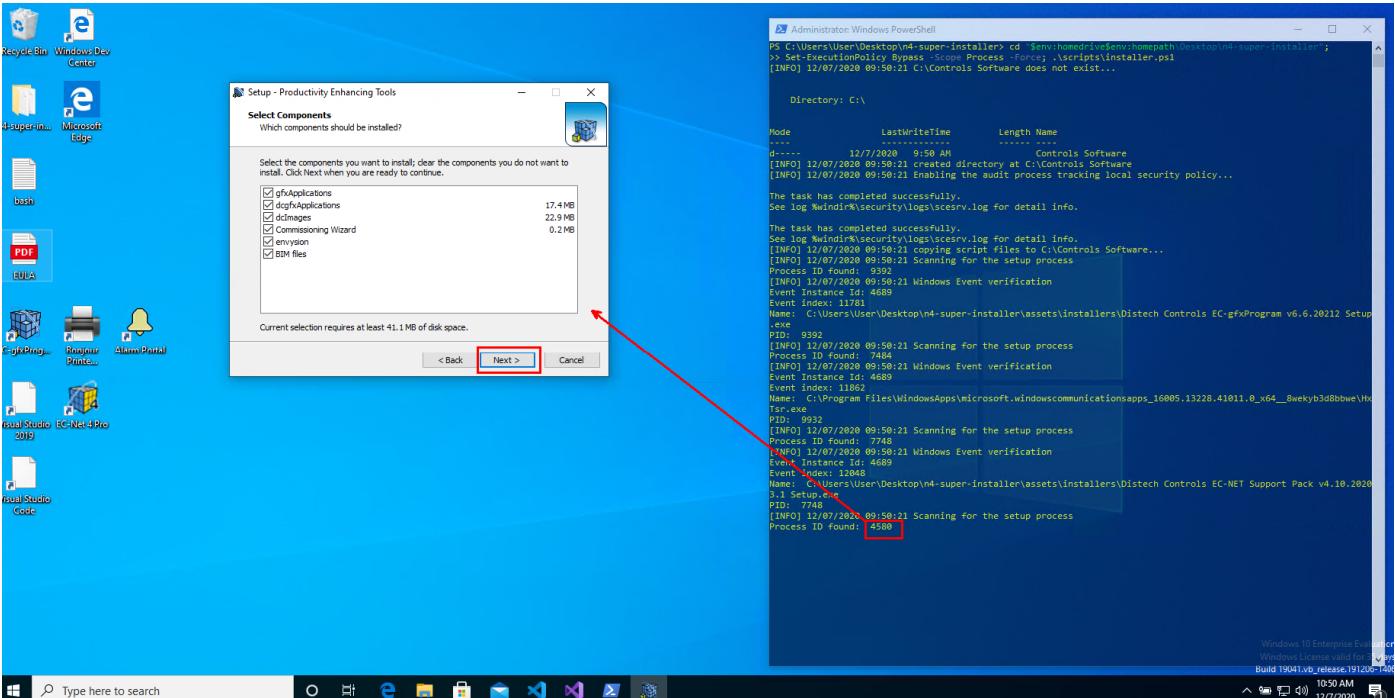
```
cd "$env:homedrive$env:homepath\Desktop\n4-super-installer";
Set-ExecutionPolicy Bypass -Scope Process -Force; .\scripts\installer.ps1
```

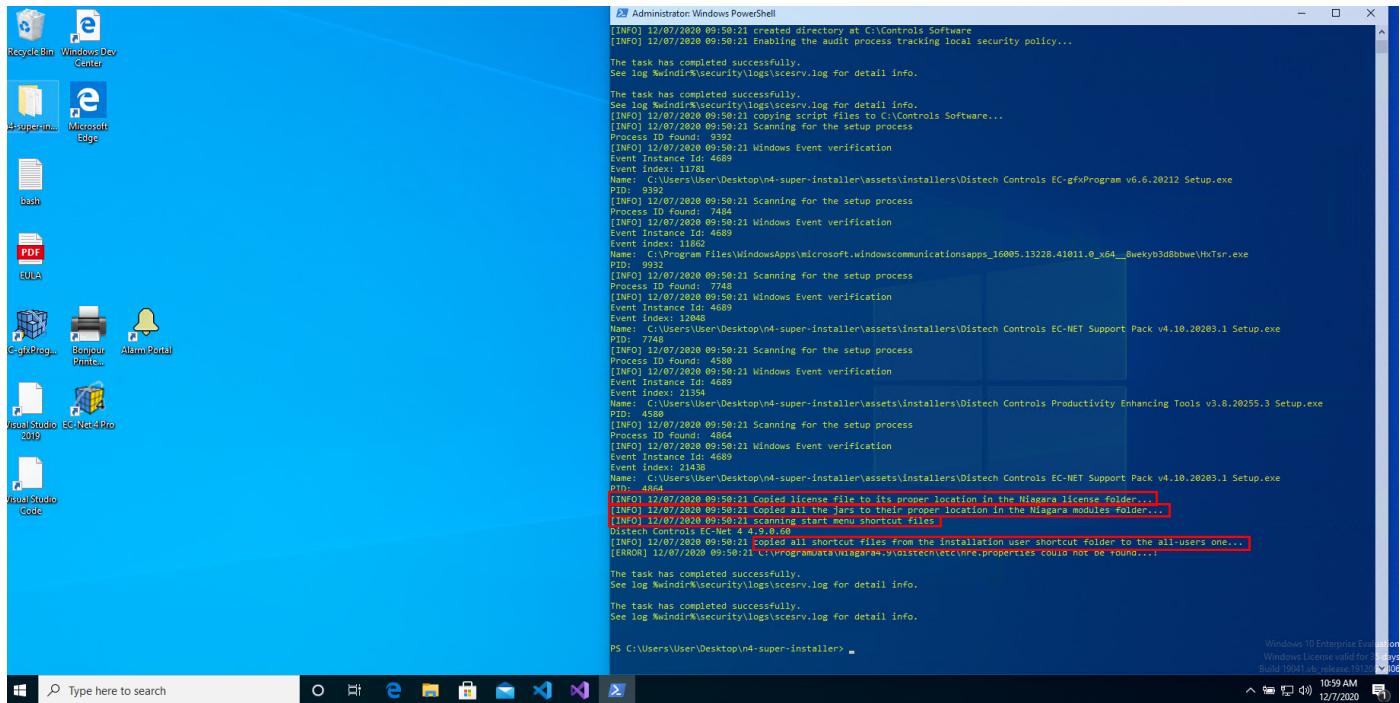
7. Press **Enter** and wait to follow the prompts for the software installation setups, which will be installed in sequential order. At this point the installer has created the *D:\Controls Software* folder and copied all the contents from the current download folder to the folder where application installers will be kept.

8. After all the setups are done the installer will copy the jars into the modules directory, it will copy the license file into its proper folder, and copy the start menu shortcut folders from the installation user directory to the allusersprofile start menu shortcut directory.









9. The Support Pack needs the .NET Framework version 2.0 to be installed, the installer runs local, but it still requires internet access to Microsoft Services.
10. The nre.properties gets edited to allocate more memory in the JVM, then the file gets copied from the Niagara default installation folders over to [C:\ProgramData\Niagara4.9\distech\etc](#) and [C:\Users\User\Niagara4.9\distech\etc](#); a copy of the original unedited version of the nre.properties file gets archived in case it is needed.

Engineering Notes

In eventvwr.msc, we are looking for the process-creation (4688) and process-terminations (4689) events in the Windows event viewer to track the overall install process

The expected output in the event viewer for each setup.exe program this installer runs should look like this:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	12/1/2020 12:44:21 PM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	12/1/2020 12:44:21 PM	Microsoft Windows security auditing.	4688	Process Creation

followed by:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	12/1/2020 12:48:37 PM	Microsoft Windows security auditing.	4688	Process Termination
Audit Success	12/1/2020 12:49:12 PM	Microsoft Windows security auditing.	4688	Process Termination

full event log details

```
Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Date:         12/1/2020 12:44:21 PM
Event ID:      4688
Task Category: Process Creation
Level:        Information
Keywords:     Audit Success
User:          N/A
Computer:    WinDev2010Eval
Description:
A new process has been created.

Creator Subject:
Security ID:      S-1-5-21-3858184157-4174427647-2357676267-1001
Account Name:    User
Account Domain:  WINDEV2010EVAL
Logon ID:       0x31F70

Target Subject:
Security ID:      S-1-0-0
Account Name:    -
Account Domain:  -
Logon ID:       0x0

Process Information:
New Process ID:   0x249c
New Process Name: C:\Users\User\AppData\Local\Temp\is-NVBLR.tmp\Distech Controls EC-gfxProgram v6.6.20212 Setup.tmp
Token Elevation Type:  %%1937
Mandatory Label:   S-1-16-12288
Creator Process ID: 0x26c0
Creator Process Name:  C:\Users\User\projects\n4-super-installer\assets\installers\Distech Controls EC-gfxProgram
v6.6.20212 Setup.exe
```

```
Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Date:         12/1/2020 12:44:21 PM
Event ID:      4688
Task Category: Process Creation
Level:        Information
Keywords:     Audit Success
User:          N/A
Computer:    WinDev2010Eval
Description:
A new process has been created.

Creator Subject:
Security ID:      S-1-5-21-3858184157-4174427647-2357676267-1001
Account Name:    User
Account Domain:  WINDEV2010EVAL
Logon ID:       0x31F70

Target Subject:
Security ID:      S-1-0-0
Account Name:    -
Account Domain:  -
Logon ID:       0x0

Process Information:
New Process ID:   0x26c0
New Process Name: C:\Users\User\projects\n4-super-installer\assets\installers\Distech Controls EC-gfxProgram v6.6.20212
Setup.exe
Token Elevation Type:  %%1937
Mandatory Label:   S-1-16-12288
Creator Process ID: 0x6fc
Creator Process Name:  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Command References
secpol.msc
eventvwr.msc

```
clear-eventlog -logname Security -computername ($env:COMPUTERNAME)
```