

Lab 5: Draw Network Diagrams

Lab Scenario

Until now, you have gathered information about the open ports, services running on the ports, OS details, security mechanisms details, etc. of the target network using various port and network scanning techniques and tools.

As a professional ethical hacker or a pen tester, the last step in the penetration process is to draw a network diagram that assists in identifying the topology or architecture of a target network. The network diagram also helps to trace the path to the target host in the network and enables you to understand the position of firewalls, IDSs, routers, and other access control devices.

As a professional ethical hacker or pen tester, you should be able to create a pictorial representation of network topology used in the target network. The network diagrams can be used to launch further attacks on the target network.

Lab Objectives

- Draw network diagrams using Network Topology Mapper

Overview of Network Diagrams


Drawing a network diagram assists in the identification of the topology or architecture of a target network, and further assists you in finding the vulnerabilities or weak points of security mechanisms. These vulnerabilities can then be exploited to bypass the target's network. The network diagram also helps the network administrators to manage their networks.

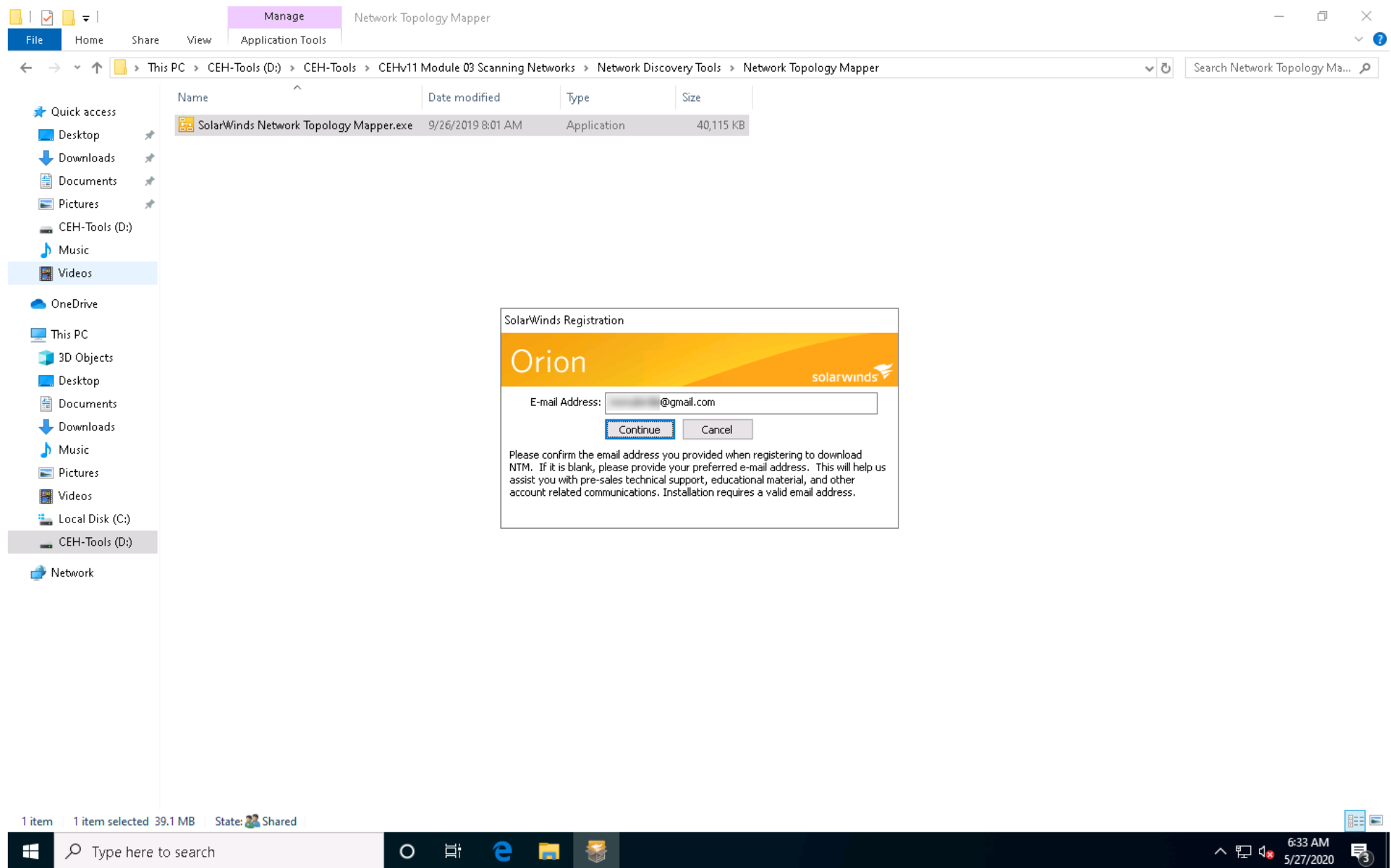
Task 1: Draw Network Diagrams using Network Topology Mapper

Network Topology Mapper discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data. It automatically detects new devices and changes to network topology, simplifies inventory management for hardware and software assets, and addresses reporting needs for PCI compliance and other regulatory requirements

Here, we will use Network Topology Mapper to draw network diagrams of the target network.

1. ☐ In the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**, and then double-click **SolarWinds Network Topology Mapper.exe**.

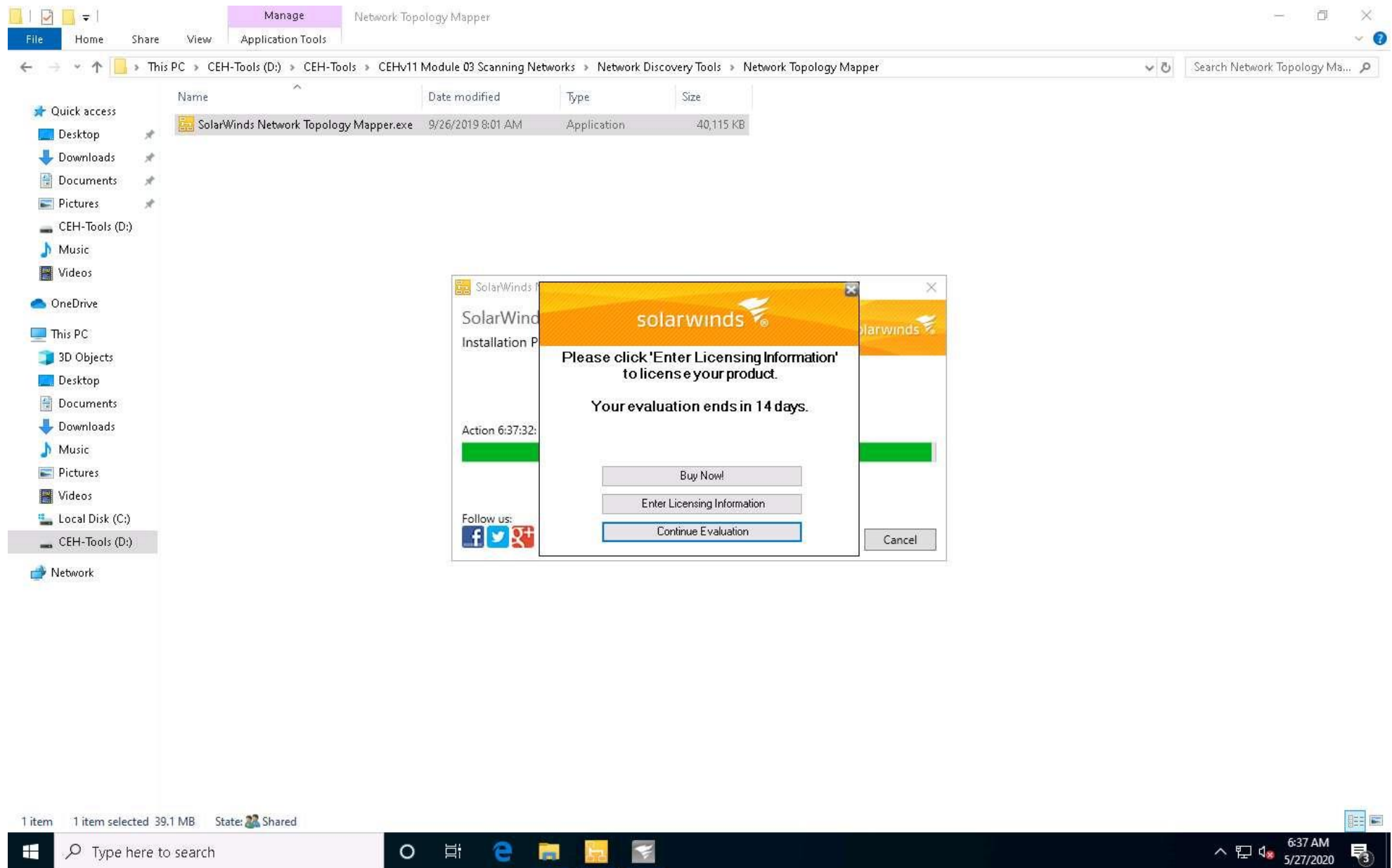
2.  The **SolarWinds Registration** dialog-box opens. Enter a working email address, and then click **Continue**.



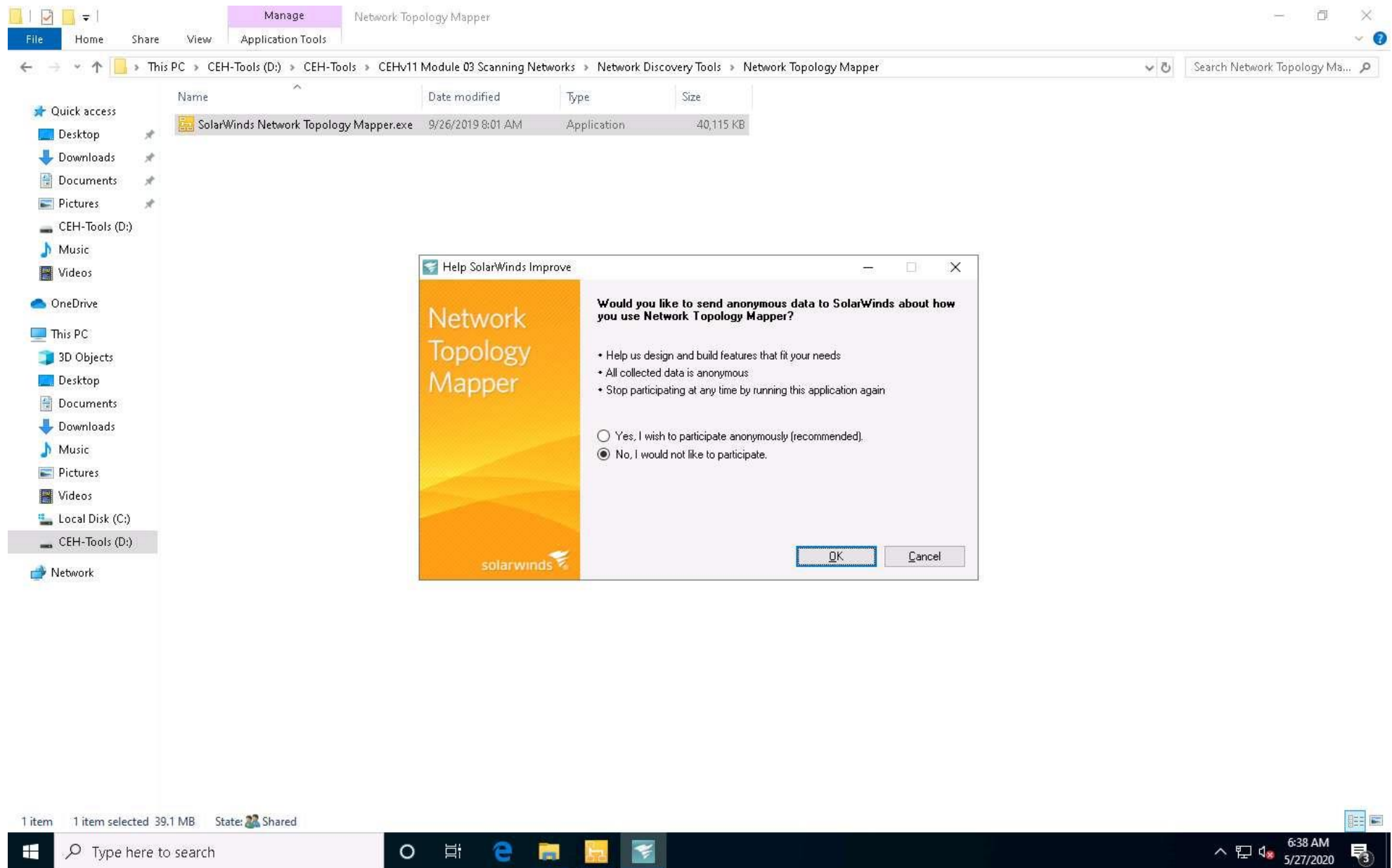
3. ☐ In the next window, accept the license agreement and click **Install**.

If a **User Account Control** window appears, click **Yes**.

4. ☐ The SolarWinds license pop-up appears; click **Continue Evaluation**.



5. ☐ The **Help SolarWinds Improve** window appears. Click the **No, I would not like to participate** radio button, and then click **OK**.



6. ☐ Once the installation is complete, and the **SolarWinds Network Topology Mapper** window opens, click **Close**.

Ensure that the **Run SolarWinds Network Topology Mapper now** option is selected.

The screenshot shows a Windows File Explorer window titled "Network: Topology Mapper" with the "Manage" tab selected. The address bar shows the path: This PC > CEH-Tools (D:) > CEH-Tools > CEHV11 Module 03 Scanning Networks > Network Discovery Tools > Network Topology Mapper. The file list contains one item: "SolarWinds Network Topology Mapper.exe" (Application, 40,115 KB, modified 9/26/2019 8:01 AM). A setup completion dialog box is overlaid on the file explorer. The dialog box has a title bar "SolarWinds Network Topology Mapper" and a close button. The main text reads "SolarWinds Network Topology Mapper Setup" and "Setup Completed". Below this, it says "SolarWinds Network Topology Mapper setup completed successfully". There is a checkbox labeled "Run SolarWinds Network Topology Mapper now" which is checked. At the bottom left, there are social media links for Facebook, Twitter, and Google+. At the bottom right is a "Close" button. The Windows taskbar at the bottom shows the search bar with "Type here to search", several application icons, and the system tray with the date and time "6:41 AM 5/27/2020".

File Explorer Path: This PC > CEH-Tools (D:) > CEH-Tools > CEHV11 Module 03 Scanning Networks > Network Discovery Tools > Network Topology Mapper

Name	Date modified	Type	Size
SolarWinds Network Topology Mapper.exe	9/26/2019 8:01 AM	Application	40,115 KB

SolarWinds Network Topology Mapper Setup
Setup Completed

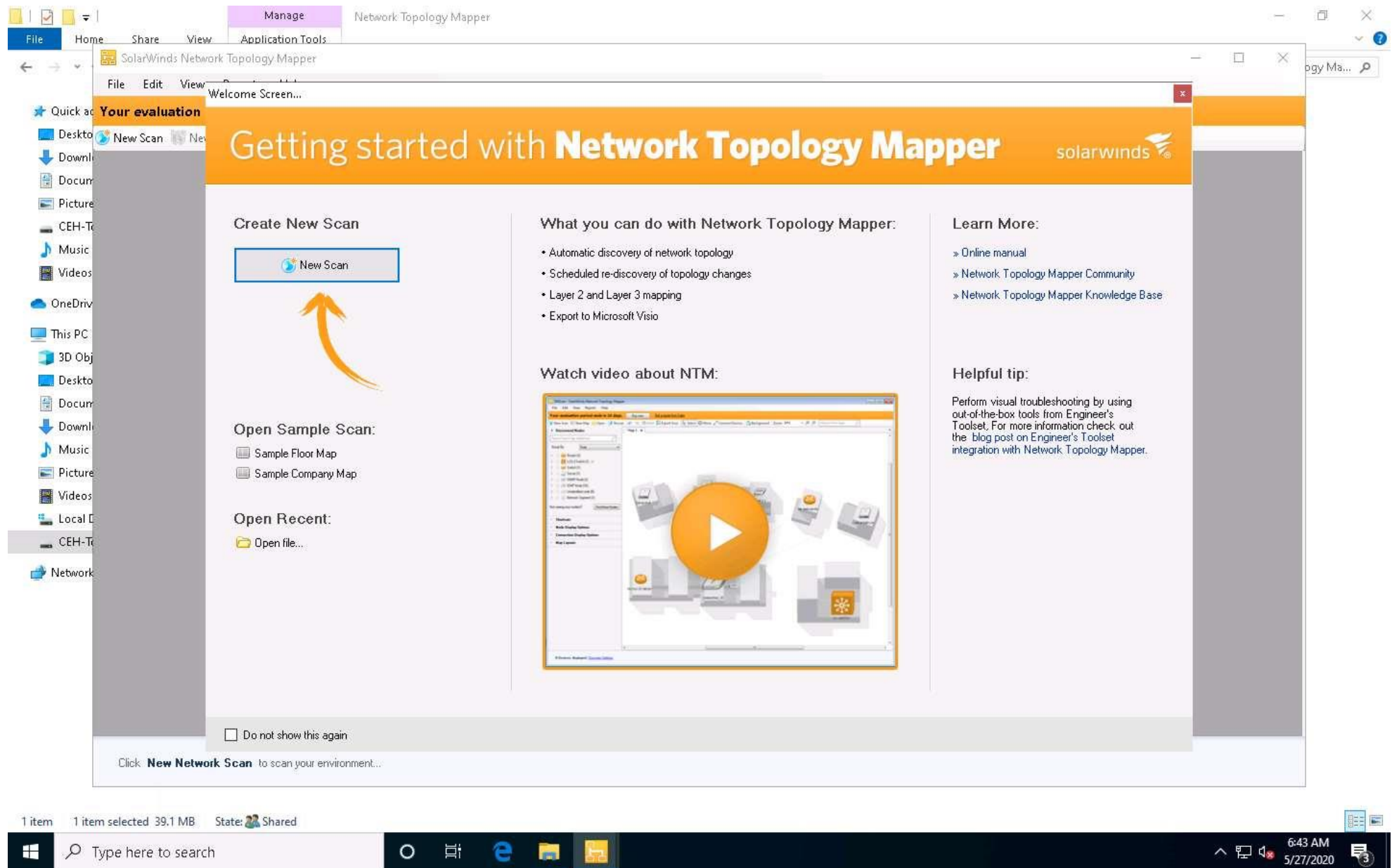
SolarWinds Network Topology Mapper setup completed successfully

☒ Run SolarWinds Network Topology Mapper now

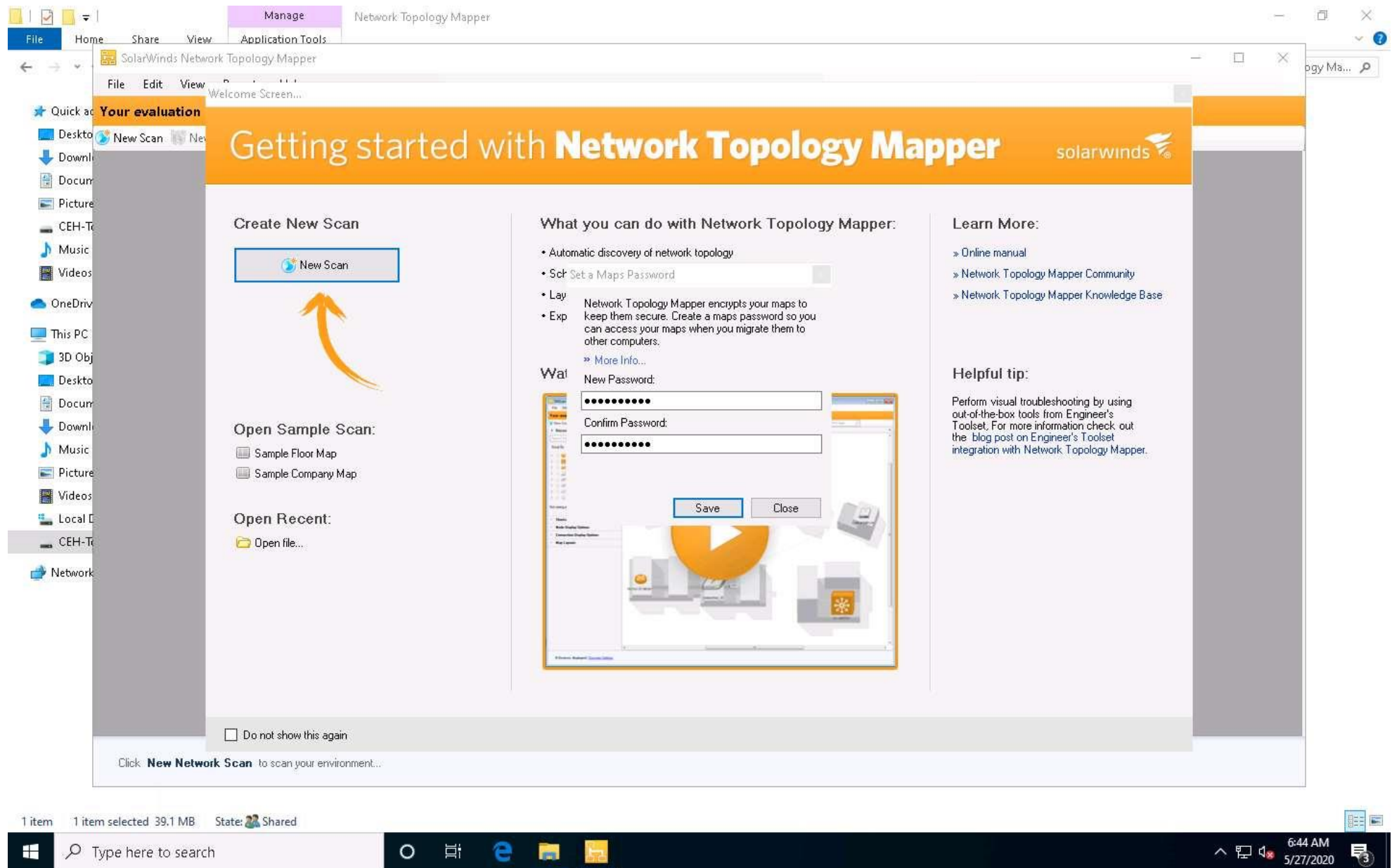
Follow us: [f](#) [t](#) [g+](#)

Close

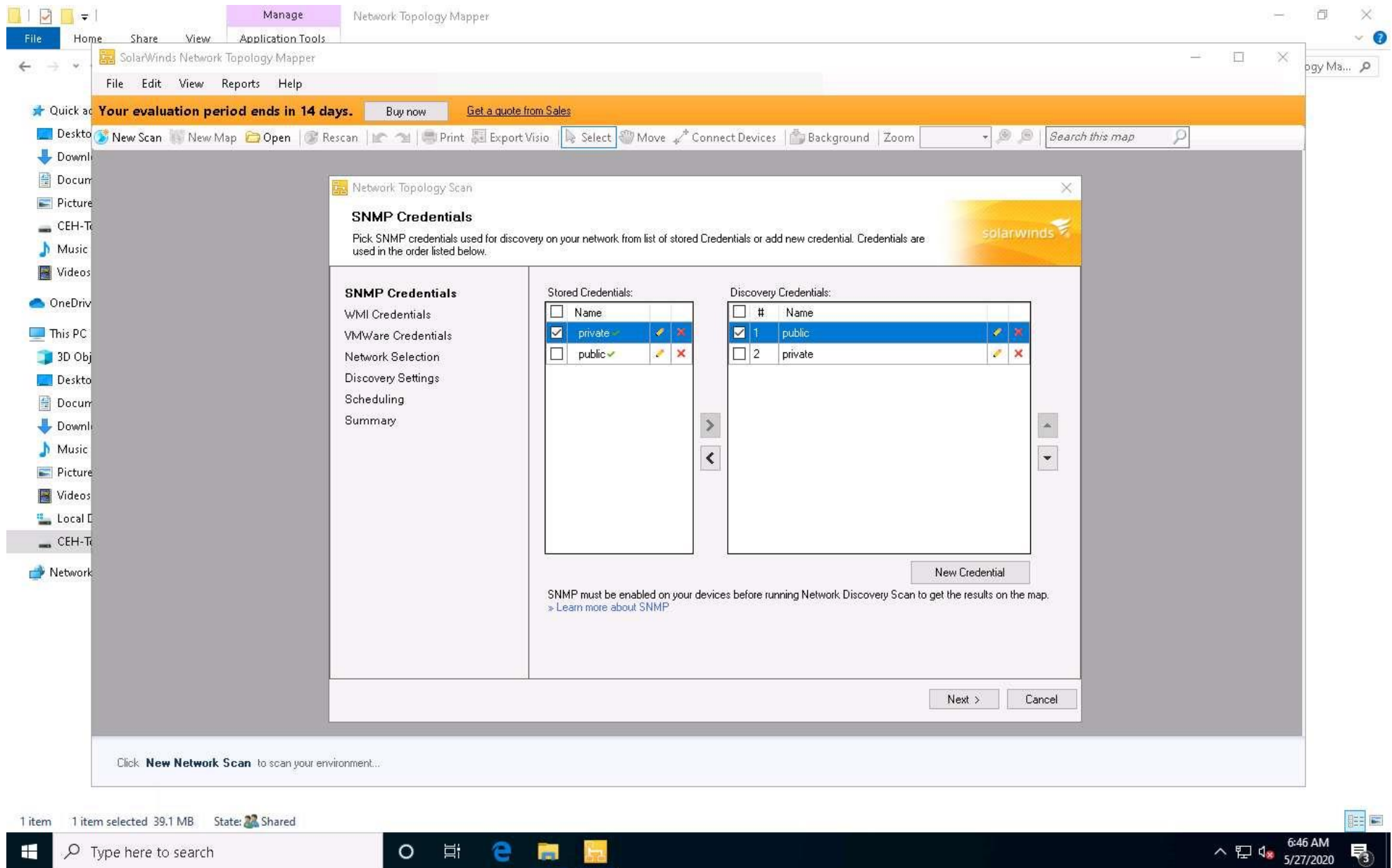
7. ☐ The **Solarwinds** pop-up opens; click **Continue Evaluation**.
8. ☐ The **SolarWinds Network Topology Mapper** main window appears, along with the **Welcome Screen....** Click **New Scan** in the left pane of the **Welcome Screen**.



9. ☐ The **Set a Maps Password** pop-up appears. Enter a password (here, **qwerty@123**) of your choice in the **New Password** field, re-enter the same password in the **Confirm Password** field, and click **Save**.

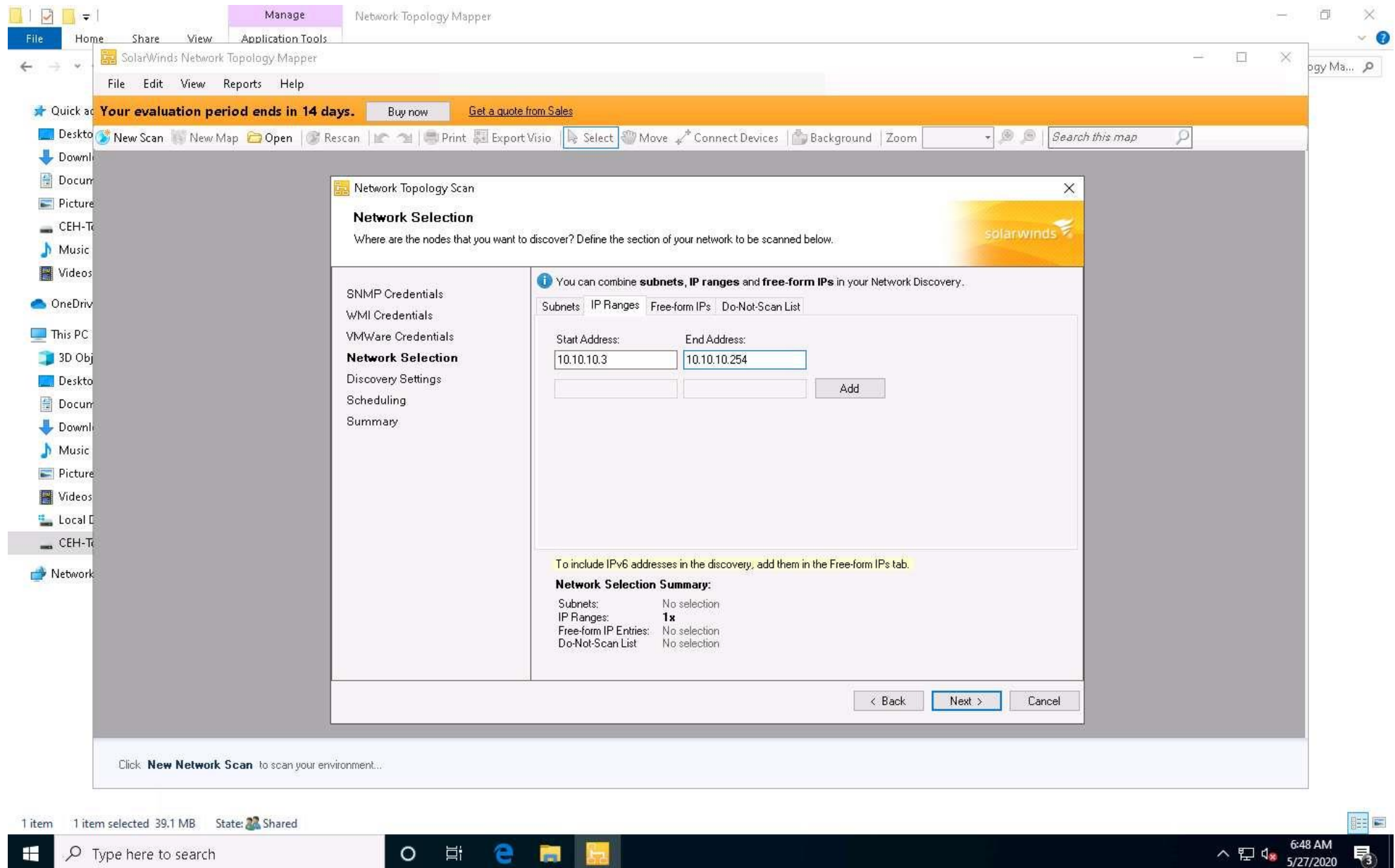


10. ☐ The **Network Topology Scan** window appears. In the **SNMP Credentials** section, select the **private** credential under the **Stored Credentials** section and **public** credential under the **Discovery Credentials** section, and then click **Next**.

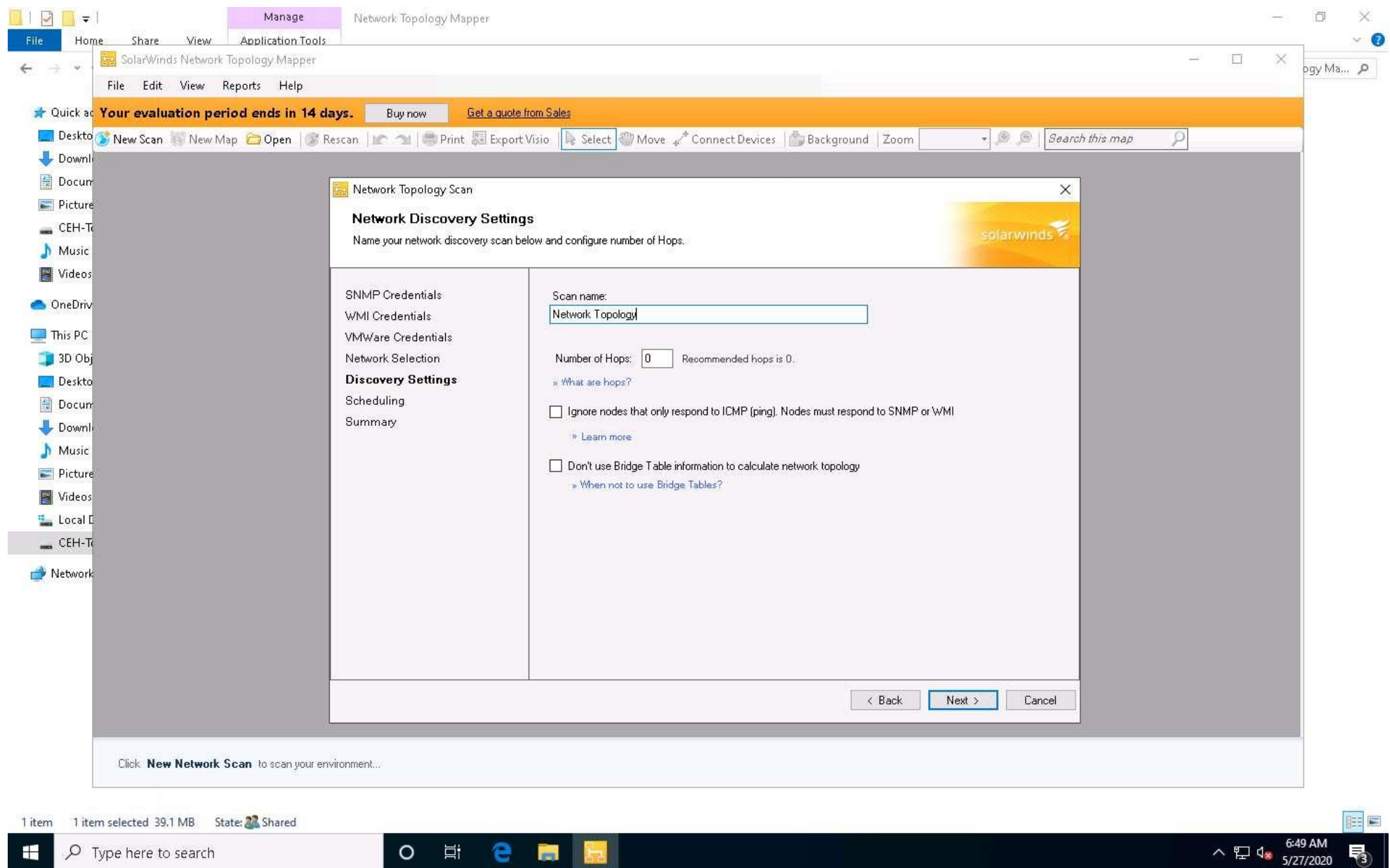


11. ☐ Leave the **WMI Credentials** and **VMWare Credentials** section to default and click **Next**.

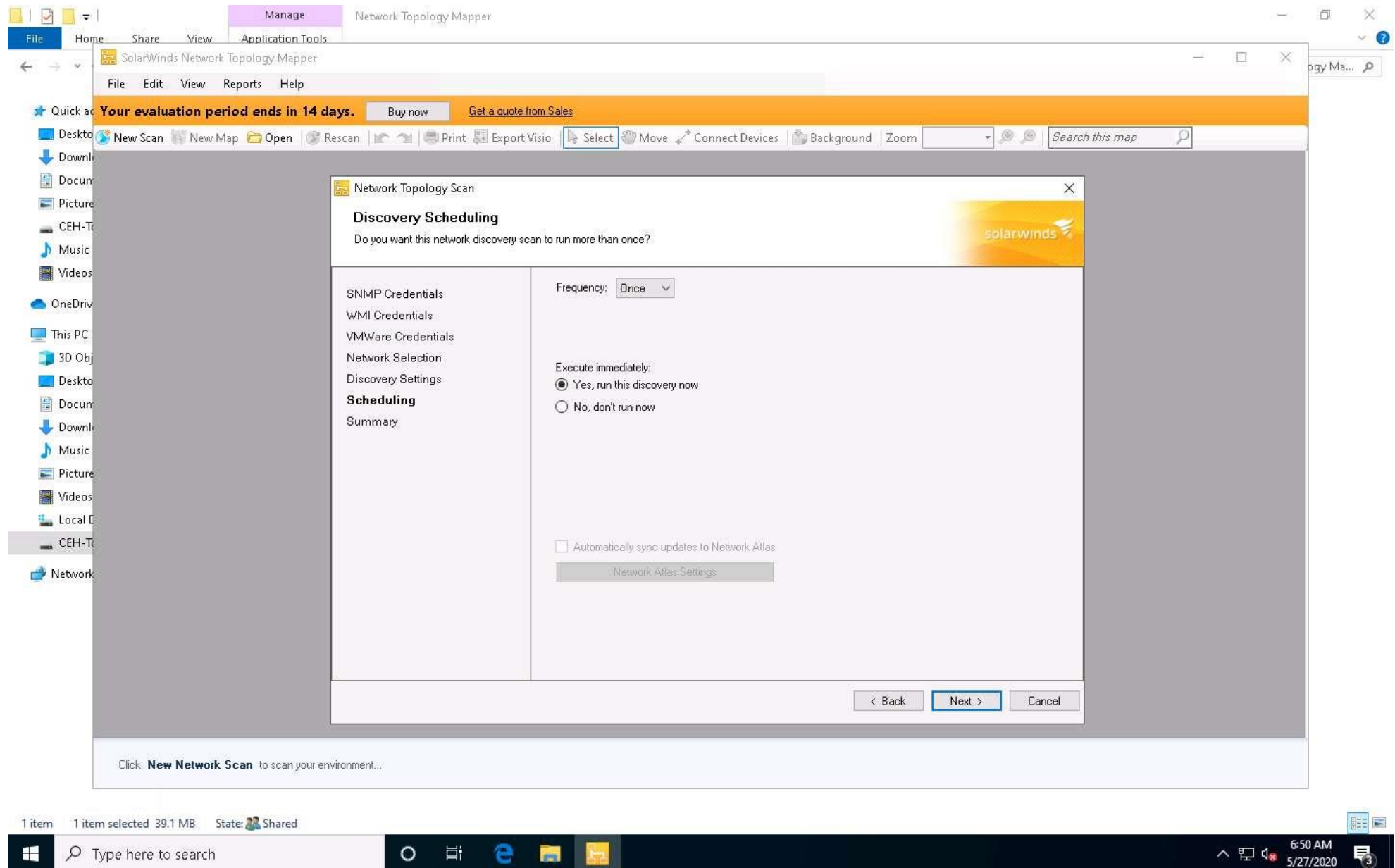
12. ☐ The **Network Selection** section appears. Click the **IP Ranges** tab in the right-pane, enter the IP address range (**10.10.10.3 - 10.10.10.254**) in the **Start Address** and **End Address** fields, and click **Next**.



13. ☐ The **Discovery Settings** section appears. Enter a name under the **Scan name** field (here, "**Network Topology**") and click **Next**.



14. ☐ The **Scheduling** section appears. Ensure that **Once** is selected in the **Frequency** drop-down menu; under the **Execute immediately** radio button **Yes, run this discovery now** is selected; then, click **Next**.



15. ☐ The **Summary** section appears; click **Discover**.

The screenshot shows the SolarWinds Network Topology Mapper application window. The 'Manage' tab is active, and the 'Network Topology Mapper' window is open. A 'Network Topology Scan' dialog box is displayed, showing the 'Network Discovery Summary' section. The summary includes the following configuration details:

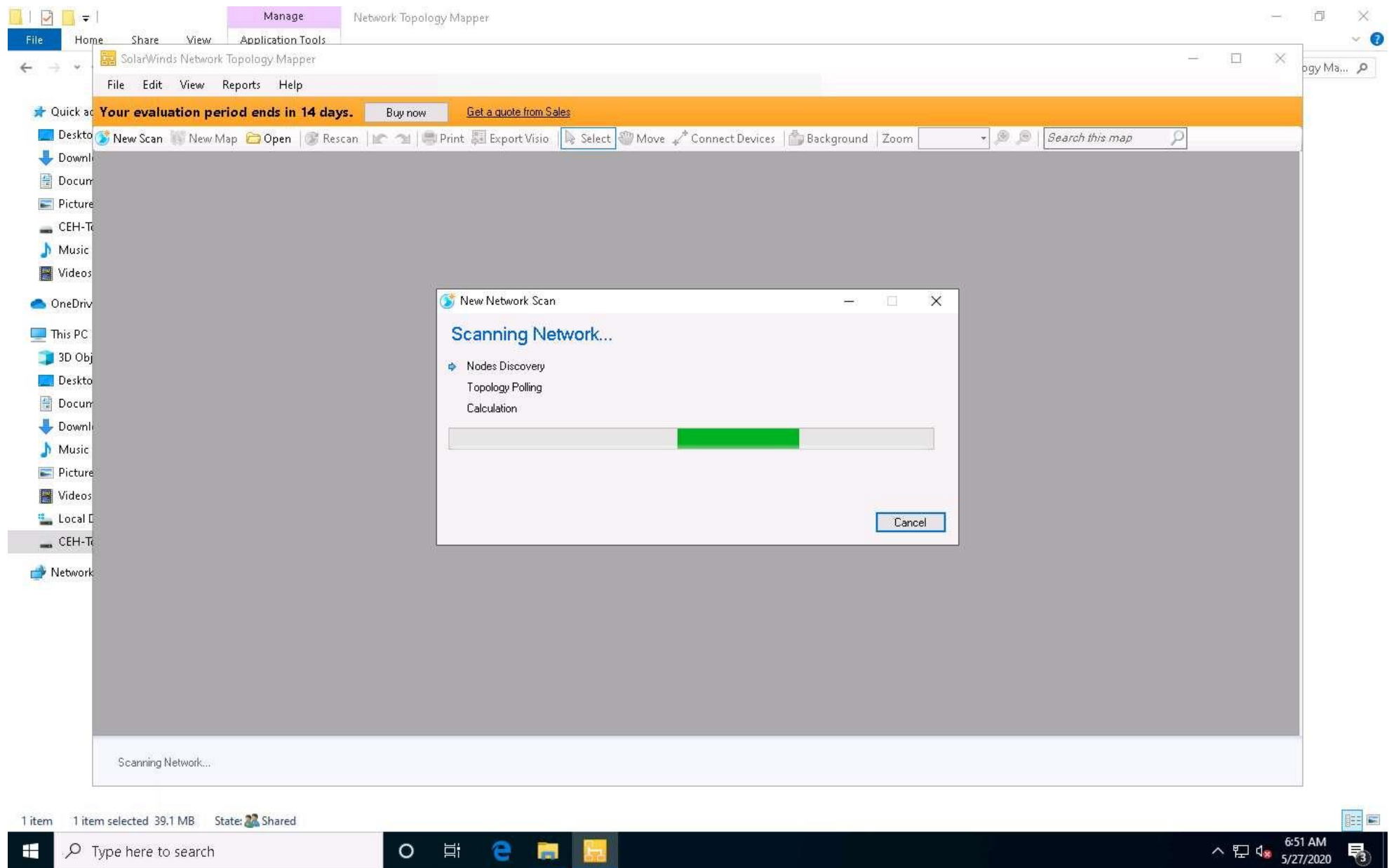
Category	Value
SNMP Credentials:	public private
WMI Credentials:	<no credentials added>
VMWare Credentials:	<no credentials added>
Network Selection:	IP ranges: 10.10.10.3 - 10.10.10.254 Subnets: <no selection> Free-form IPs: <no selection> Do-Not-Scan List: <no selection>
Discovery Settings:	Map name: Network Topology Number of Hops: 0
Scheduling:	Frequency: Once Execution: Immediately

Below the configuration details, there are 'TIPS' for network discovery:

- Network discovery can only draw connections between devices that have SNMP enabled. Non-SNMP devices cannot be mapped.
- Provide Windows and VMWare credentials for devices on your network.

At the bottom of the dialog box, there are three buttons: '< Back', 'Discover', and 'Cancel'. The 'Discover' button is highlighted. The background application window shows a sidebar with various icons and a top menu bar with options like 'File', 'Edit', 'View', 'Reports', and 'Help'. A banner at the top of the application window states 'Your evaluation period ends in 14 days.' with links to 'Buy now' and 'Get a quote from Sales'.

16. ☐ The **New Network Scan** window appears; the Network Topology Mapper starts scanning the network for live hosts.



17. ☐ The **Network Topology - SolarWinds Network Topology Mapper** window appears. The **Network Topology Mapper** displays a network topology diagram for the provided IP address range, as shown in the following screenshot.
18. ☐ Close the **Map Navigator** window.

Network Topology - SolarWinds Network Topology Mapper

File Edit View Reports Help

Your evaluation period ends in 14 days. Buy now Get a quote from Sales

New Scan New Map Open Rescan Print Export Visio Select Move Connect Devices Background Zoom 90% Search this map

Discovered Nodes

Search topology database

Group By: Role

- Server (2) ✓
- ICMP Node (4) ✓
- Network Segment (1) ✓

Not seeing your node(s)? Find More Nodes

Shortcuts

- Node Display Options
- Connection Display Options
- Map Layouts

Map Navigator

Map 1 x

10.10.10.13

10.10.10.14

IP Range
10.10.10.3 - 10.10.10.254

Server2016.CEH.com

Server2019

7 Devices displayed [Discovery Settings](#) Last completed network scan: 5/27/2020 6:53:34 AM Known devices found: 0 New devices found: 7 Removed devices found: 0

6:54 AM 5/27/2020

19. ☐ Expand **Node Display Options** in the right-hand pane and select the **IP address** checkbox. This displays IP addresses for all nodes in the layout.

Network Topology - SolarWinds Network Topology Mapper

File Edit View Reports Help

Your evaluation period ends in 14 days. Buy now Get a quote from Sales

New Scan New Map Open Rescan Print Export Visio Select Move Connect Devices Background Zoom 90% Search this map

Discovered Nodes

Shortcuts

Node Display Options

- ☒ Node name
- ☒ IP address
- ☐ Hostname
- ☐ System name
- ☐ Machine type
- ☐ Vendor
- ☐ System description
- ☐ System location
- ☐ Contact
- ☐ Polling method

Connection Display Options

Map Layouts

Map 1 x

7 Devices displayed [Discovery Settings](#) Last completed network scan: 5/27/2020 6:53:34 AM Known devices found: 0 New devices found: 7 Removed devices found: 0

Windows taskbar: Type here to search, 6:56 AM 5/27/2020

20. ☐ Now, expand the **Map Layouts** node, and select **Symmetrical** under the **Auto Arrange** section to change the topology layout of the mapped network. Each time you click **Symmetrical**, all nodes are rearranged randomly.

You may select the node display options of your choice: whichever options you choose, they are added to the topology map. These topology maps are saved automatically to **C:\ProgramData\Solarwinds\Network Topology Mapper\UserMaps**.

Network Topology - SolarWinds Network Topology Mapper

File Edit View Reports Help

Your evaluation period ends in 14 days. Buy now Get a quote from Sales

New Scan New Map Open Rescan Print Export Visio Select Move Connect Devices Background Zoom 90% Search this map

Discovered Nodes

Shortcuts

Node Display Options

Connection Display Options

Map Layouts

Auto Arrange:

Align: Symmetrical

Distribute:

Endpoint Summarization

Map 1 x

ICMP
Evaluation mode
Right click for node details

10.10.10.13
10.10.10.13

Server2016.CEH.com
10.10.10.16

Server2019
10.10.10.19

ICMP
Evaluation mode
Right click for node details

10.10.10.14
10.10.10.14

IP Range
10.10.10.3 - 10.10.10.254
Unknown

7 Devices displayed [Discovery Settings](#) Last completed network scan: 5/27/2020 6:53:34 AM Known devices found: 0 New devices found: 7 Removed devices found: 0

Type here to search

6:58 AM
5/27/2020

21. ☐ Right-click on a node (here **Server2016** with IP address **10.10.10.16**) and select **Node Properties** to view information about the selected node.

The screenshot displays the SolarWinds Network Topology Mapper interface. The main window shows a network map titled "Map 1" with a central node labeled "IP Range 10.10.10.3 - 10.10.10.254 Unknown". This central node is connected to five other nodes: three ICMP nodes (labeled "10.10.10.13 10.10.10.13", "10.10.10.14 10.10.10.14", and "Evaluation mode Right click for node details") and two server nodes (labeled "Server2016.CEH.com 10.10.10.16" and "Server2019 10.10.10.19"). The left sidebar contains various configuration options under "Map Layouts", including "Auto Arrange", "Align", "Distribute", and "Endpoint Summarization". The bottom status bar indicates "7 Devices displayed" and provides details about the last completed network scan on 5/27/2020 at 6:53:34 AM.

Network Topology - SolarWinds Network Topology Mapper

File Edit View Reports Help

Your evaluation period ends in 14 days. Buy now Get a quote from Sales

New Scan New Map Open Rescan Print Export Visio Select Move Connect Devices Background Zoom 90% Search this map

Discovered Nodes

Shortcuts

Node Display Options

Connection Display Options

Map Layouts

Auto Arrange:

Align:

Distribute:

Endpoint Summarization

Map 1

ICMP

Evaluation mode
Right click for node details

10.10.10.13
10.10.10.13

10.10.10.14
10.10.10.14

IP Range
10.10.10.3 - 10.10.10.254
Unknown

Server2016.CEH.com
10.10.10.16

Server2019
10.10.10.19

Evaluation mode
Right click for node details

7 Devices displayed [Discovery Settings](#)

Last completed network scan: 5/27/2020 6:53:34 AM Known devices found: 0 New devices found: 7 Removed devices found: 0

Type here to search

6:59 AM
5/27/2020

22. ☐ The **Node Details** window appears, displaying information about the selected node. Click **Close** to close the window.

The screenshot displays the SolarWinds Network Topology Mapper interface. The main window shows a network map with a central hub labeled "IP Range 10.10.10.3 - 10.10.10.254 Unknown" connected to several nodes. On the left, a sidebar contains navigation options: Discovered Nodes, Shortcuts, Node Display Options, Connection Display Options, and Map Layouts. The Map Layouts section includes Auto Arrange, Align, Distribute, and Endpoint Summarization tools. The right sidebar shows the Node Details window for the selected node, "Server2016.CEH.com".

Node Details - Basic Information

Node Name	Server2016.CEH.com
Primary Node Role	Server
Node Roles	
Polling IP Address	10.10.10.16
Physical Address	
IP Addresses	10.10.10.16 (discovered)
Hostname	Server2016
System Name	Server2016.CEH.com
System Description	Hardware: Intel64 Family 6 Mode
Machine Type	Windows 2012 R2 Domain Contro
Vendor	Windows
System Location	
Contact	
Polling Method	SNMPv2

Node Name
Server2016.CEH.com

Custom Properties

Property Name	Format	Value
---------------	--------	-------

7 Devices displayed [Discovery Settings](#) Last completed network scan: 5/27/2020 6:53:34 AM Known devices found: 0 New devices found: 7 Removed devices found: 0

6:59 AM 5/27/2020

23. ☐ Right-click on a node (**Server2016** with IP address **10.10.10.16**) and select **Integration with Windows Tools** and click **Remote Desktop**.

The screenshot displays the SolarWinds Network Topology Mapper interface. The main window shows a network map with a central hub labeled "IP Range 10.10.10.3 - 10.10.10.254 Unknown" connected to several nodes. A right-click context menu is open over the "Server2016 10.10.10.16" node. The menu options include "Node Properties", "Add Neighbors", "Copy", "Place Text", "Custom Icon", "Icon Size", "Integration with Engineer's Toolset", "Integration with Windows Tools" (highlighted), "Integration with Custom Tools", and "Delete Node(s)". A sub-menu is also visible, showing "Remote Desktop", "TraceRoute", "Ping", and "Telnet". The left sidebar contains navigation options like "Discovered Nodes", "Shortcuts", "Node Display Options", "Connection Display Options", and "Map Layouts". The bottom status bar indicates "7 Devices displayed" and provides details about the last network scan.

Network Topology - SolarWinds Network Topology Mapper

File Edit View Reports Help

Your evaluation period ends in 14 days. Buy now Get a quote from Sales

New Scan New Map Open Rescan Print Export Visio Select Move Connect Devices Background Zoom 90% Search this map

Map 1 x

Discovered Nodes

Shortcuts

Node Display Options

Connection Display Options

Map Layouts

Auto Arrange:

Align:

Distribute:

Endpoint Summarization

ICMP 10.10.10.13 10.10.10.13

ICMP 10.10.10.14 10.10.10.14

ICMP 10.10.10.19

Server2016 10.10.10.16

Server2019 10.10.10.19

IP Range 10.10.10.3 - 10.10.10.254 Unknown

Integration with Windows Tools

Remote Desktop

TraceRoute

Ping

Telnet

Node Properties

Add Neighbors

Copy

Place Text

Custom Icon

Icon Size

Integration with Engineer's Toolset

Integration with Custom Tools

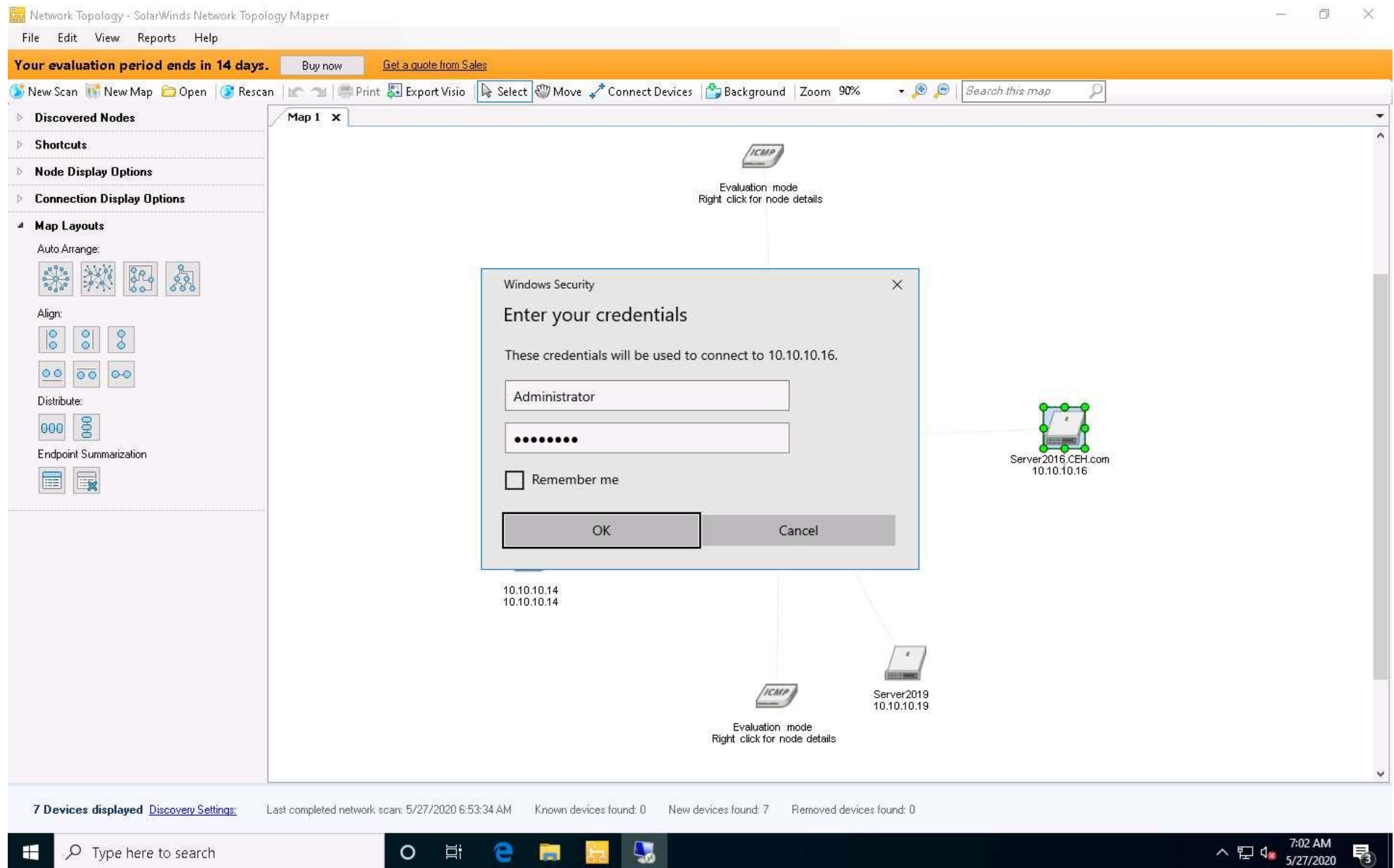
Delete Node(s)

7 Devices displayed Discovery Settings: Last completed network scan: 5/27/2020 6:53:34 AM Known devices found: 0 New devices found: 7 Removed devices found: 0

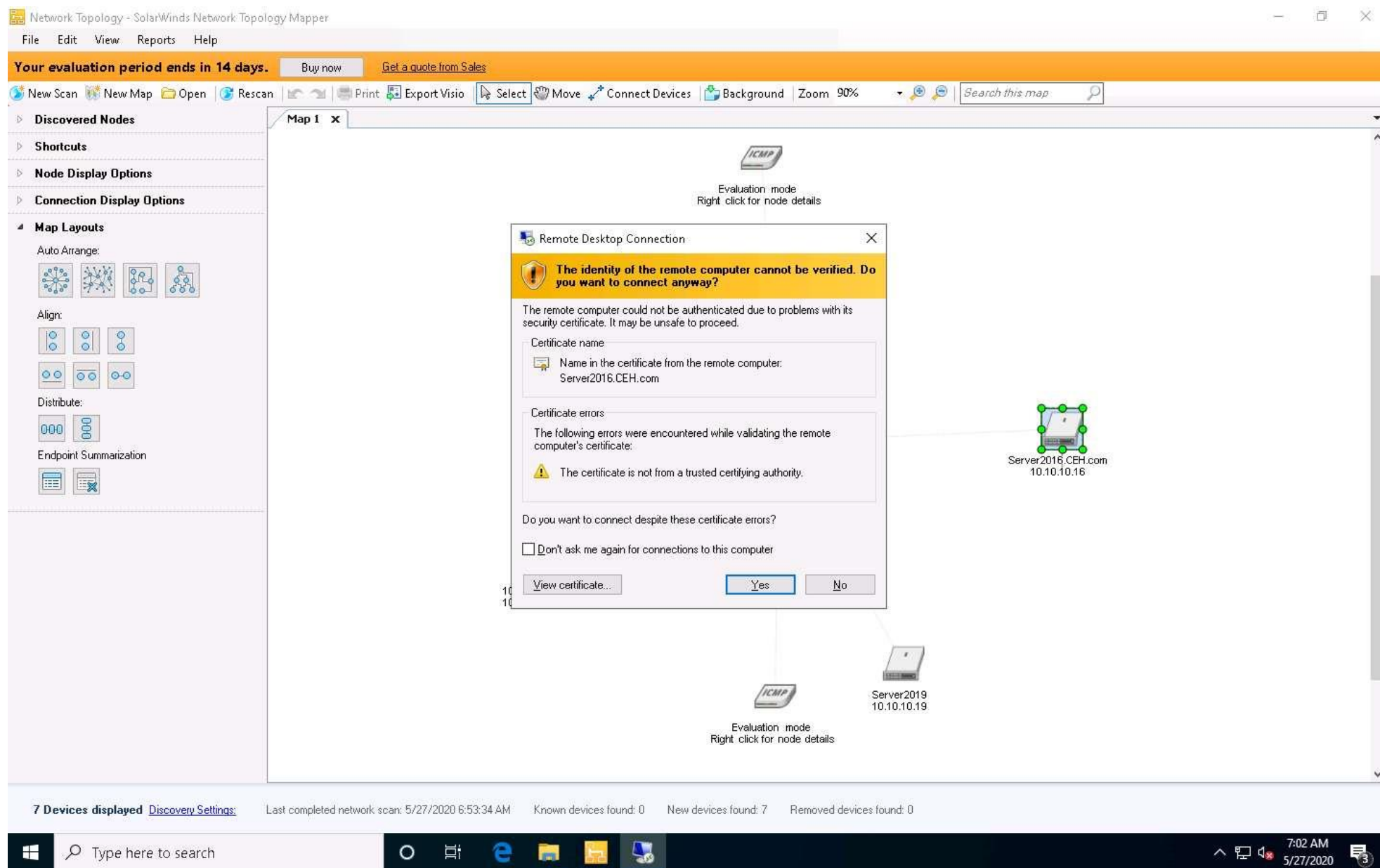
Type here to search

7:01 AM 5/27/2020

24. ☐ The **Windows Security** dialog box appears. Enter **Username** as **Administrator** and **Password** as **Pa\$\$w0rd** for **Windows Server 2016**, and click **OK**.



25. ☐ The **Remote Desktop Connection** pop-up appears; click **Yes**.



26. ☐ The **Remote Desktop Connection** is successfully set to the target machine (here, **Windows Server 2016**), as shown in the following screenshot.



27. ☐ You can use other options such as **Ping**, **Telnet**, and **Traceroute**. Similarly, an attacker can use this application to draw network diagrams, find the active hosts on the network, perform Ping, Telnet, etc.
28. ☐ This concludes the demonstration of drawing network diagram of the target network using Network Topology Mapper.
29. ☐ You can also use other network discovery tools such as **OpManager** (<https://www.manageengine.com>), **The Dude** (<https://mikrotik.com>), **NetSurveyor** (<http://nutsaboutnets.com>), **NetBrain** (<https://www.netbraintech.com>), and **Spiceworks Network Mapping Tool** (<https://www.spiceworks.com>) to draw network diagram of the target network.
30. ☐ Close all open windows and document all the acquired information.