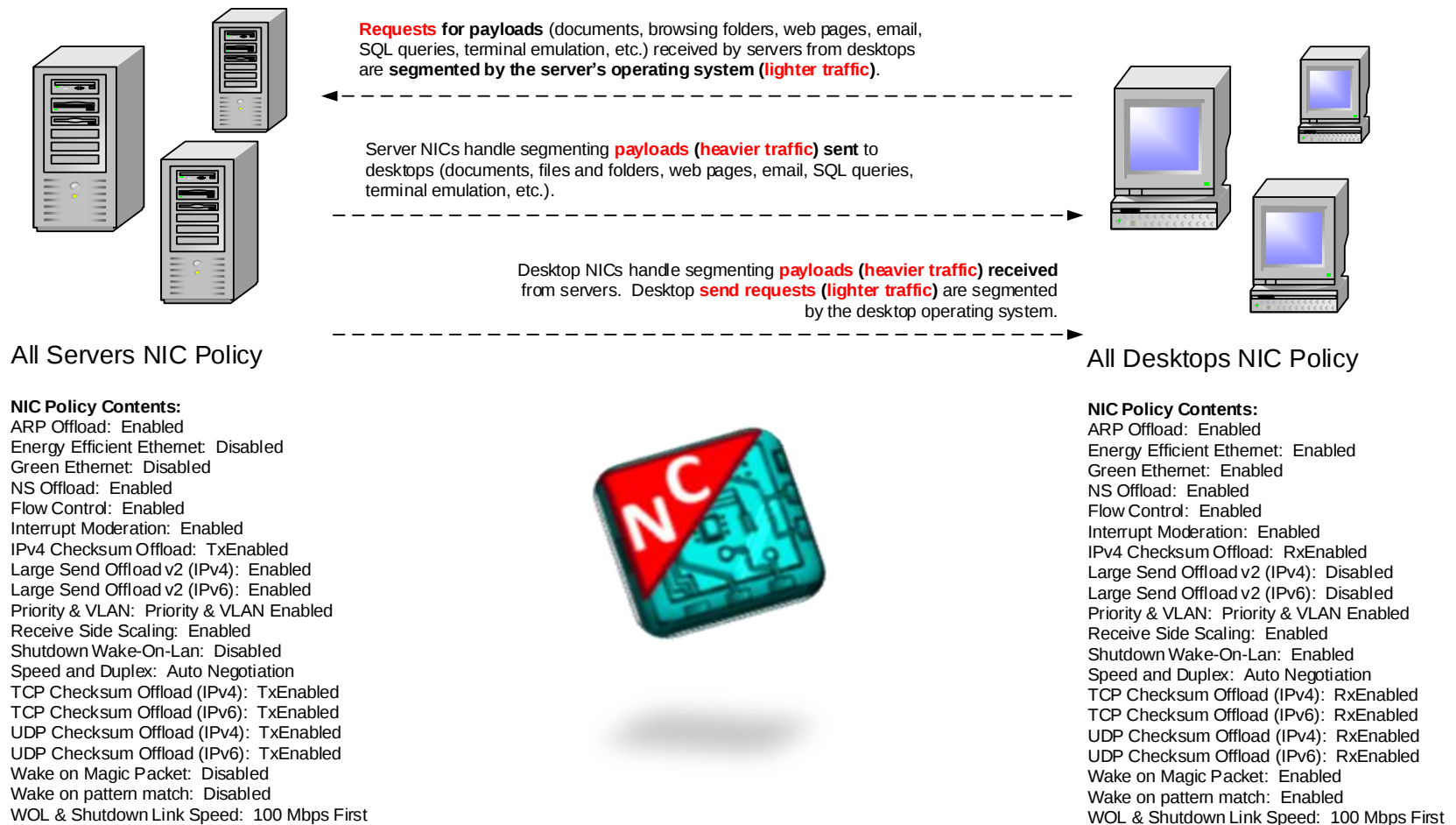




NIC Configurator 2026 Installation & Usage

NIC CONFIGURATOR 2026

(Maximizing Network Traffic Flow Between Servers and Desktops through NIC Policies)
(Reducing Operating System / CPU Load)

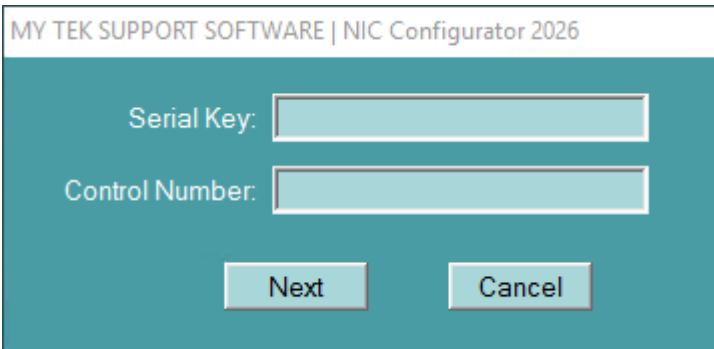
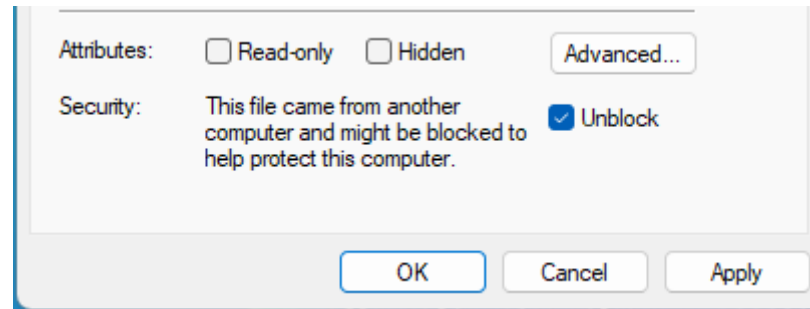


NOTE: NIC Configurator 2026 clients can maintain NIC policy settings automatically and notifies via Text and e-Mail if settings become non-compliant.

Installation

To install NIC Configurator 2026, simply login to your computer as a domain administrator, extract and double-click the NICConfigurator2026.exe file from NICConfigurator2026.zip that you downloaded after purchase.

Note: After downloading the zip file, you must unblock it before extracting its content. Simply right-click the zip file, click Properties, click the checkbox to unblock the file (as shown below), and then click Apply and OK.

A screenshot of the 'MY TEK SUPPORT SOFTWARE | NIC Configurator 2026' installation window. It has a teal background. There are two input fields: 'Serial Key:' and 'Control Number:'. Below these are 'Next' and 'Cancel' buttons.

When prompted, type in your serial key and control number that came with your purchase. These codes were sent to you via e-mail after your online purchase. Follow the instructions on-screen while the installation program installs into your default system programs directory. The setup program will install a NIC Configurator 2026 icon on your desktop toward the end of installation.

Before using NIC Configurator 2026, please follow the instructions below to allow NIC Configurator 2026 to find computers on your domains, install the NIC Configurator 2026 client, and to modify client network adapters based on your NIC Policy contents.

To begin, modify the Startup Type to Automatic for the Remote Registry service, enable Remote Administration service, and allow ICMP exceptions. This should be done for all computers by modifying Active Directory Group Policy at the domain organizational level. The following are instructions on how to perform this task.

Group Policy Object Creation (GPO) Instructions

1. In Group Policy Management, expand the following: Forest container > Domains container > Group Policy Objects container
2. Create a new group policy object called "NIC Configurator 2026"
3. Edit the NIC Configurator 2026 group policy object and expand the following: Computer Configuration > Policies > Windows Settings > Security Settings
4. Select the System Services folder
5. In the right window pane **double click Remote Registry** and put a check in the "Define this policy settings" checkbox
6. Select Automatic for the startup mode and click OK
7. Expand the following: Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security > Inbound Rules
8. Right-click Inbound Rules and select New Rule...
9. Select **Predefined**; click the drop down and select Remote Scheduled Tasks Management and then click Next
10. On the Predefined Rules box, ensure that **Remote Scheduled Tasks Management (RPC-EPMAP)** and **Remote Scheduled Tasks Management (RPC)** are selected and click Next
11. Select Allow the connection and click Finish
12. Right-click Inbound Rules and select New Rule...
13. Select **Predefined**; click the drop down and select Remote Service Management
14. On the Predefined Rules box, ensure that **Remote Service Management (RPC-EPMAP)**, **Remote Service Management (NP-In)**, and **Remote Service Management (RPC)** are selected and click Next
15. Select Allow the connection and click Finish
16. Expand the following: Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Defender Firewall
17. Select Domain Profile
18. In the right window pane, underneath Setting, double-click "Windows Defender Firewall: Allow inbound remote administration exception"
19. Click the enable button and inside the "Allow unsolicited incoming messages from" box, enter the IP Address of the computer where NIC Configurator 2026 has been installed.
20. Click OK and then double-click "Windows Defender Firewall: Allow ICMP exceptions"
21. Click "Enabled" and then make sure the "Allow inbound echo request" checkbox is checked
22. Click OK and then exit out of the Group Policy Management Editor

23. Link the NIC Configurator 2026 group policy object to the domain or to the appropriate organizational unit and enable the policy
24. Exit out of Group Policy Management

Verify that the Windows Firewall is enabling these rules on computers in your environment to ensure that NIC Configurator 2026 is able to query and modify remote computers successfully. Some computers may require forcing group policy updates and others may require a reboot.

Even though Group Policy has been configured to set the Remote Registry service for your domain computers to Automatic, some computers affected by this change may not have those services started until they have been rebooted.

Add NIC Configurator 2026 Custom Group as Local Administrator

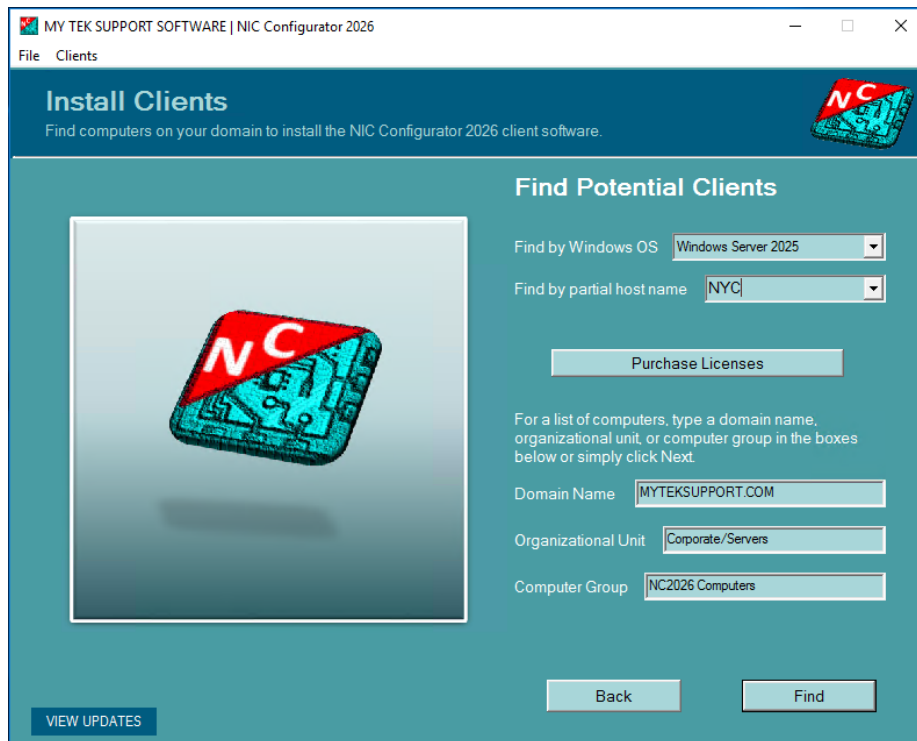
If you chose to enter a custom NIC Configurator 2026 group when setting up the server, you can follow the instructions in this section to add the group as local administrator on computers managed by NIC Configurator 2026 console.

1. In Group Policy Management, expand the following: Forest container > Domains container > Group Policy Objects container
2. Edit the NIC Configurator 2026 group policy object and expand the following: Computer Configuration > Preferences > Control Panel Settings
3. Right-click Local Users and Groups and click New > Local Group
4. Click the Group name drop-down and select Administrators (built-in)
5. In the Members box click Add and in the Name box, browse for the custom group you entered in the NIC Configurator 2026 setup program and click OK
6. Click OK again to close the New Local Group Properties window
7. Close out of Group Policy Management

Using NIC Configurator 2026

When using NIC Configurator 2026, login to your computer as either domain\administrator, a user in the Domain Admins group, or login as a user that has local admin rights on computers where the NIC Configurator 2026 client will be installed (Typically, this would be a member of the NIC Configurator 2026 custom group used above).

- **Example:** For the domain “VEGAS”, login to your computer as VEGAS\Administrator, and then run the NIC Configurator 2026 program icon on your desktop.



Client Installation

First you must find Active Directory computers to install the NIC Configurator 2026 client. From the opening dialog box, click Clients > Install from the menu bar. The Install Clients dialog box pictured to the left will appear on your screen:

Optionally, type your Domain Name, Organizational Unit, or Computer Group in the format as listed in the example below:

- **Domain:** MYTEKSUPPORT.COM
- **Organizational Unit:** Corporate/Servers
- **Computer Group:** NC2026 Computers

NIC Configurator 2026 works across firewalls, multiple domains, and multiple forests, as long as the appropriate trusts and permissions are in place, and your firewall ports are configured as displayed in this

documentation.

To display a smaller group of computers or a single computer, type the first few characters of the computer name or the full computer name in the host name filter box. For example, to display only active directory computers that begin with the letters "chi", such as "chi-mx-01" and "chi-dba-01", type "chi" in this box and then click Next.

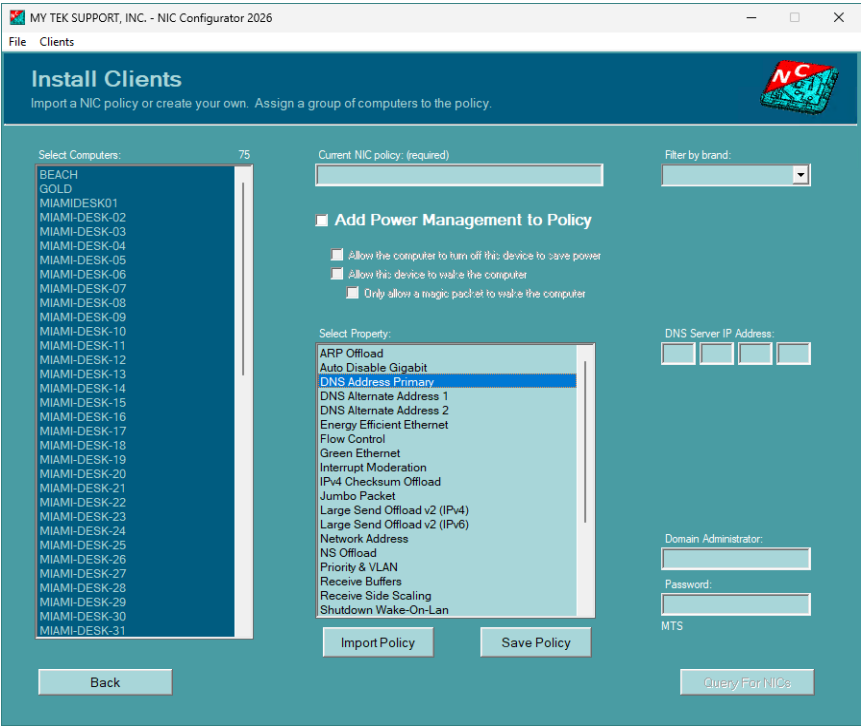
Select the dropdown for a list of Windows operating systems to choose from. Filtering by Operating System will only display computers hosting the selected Windows operating system.

To only list members of a particular computer group, fill in the Domain Name entry box, clear the Organizational Unit entry box and type a group name in the Computer Group box, and then click Next.

To only list members of a computer group that reside within a specific Organizational Unit, fill in the Organizational Unit and the Computer Group name entry boxes.

Click Next to continue Client Installation.

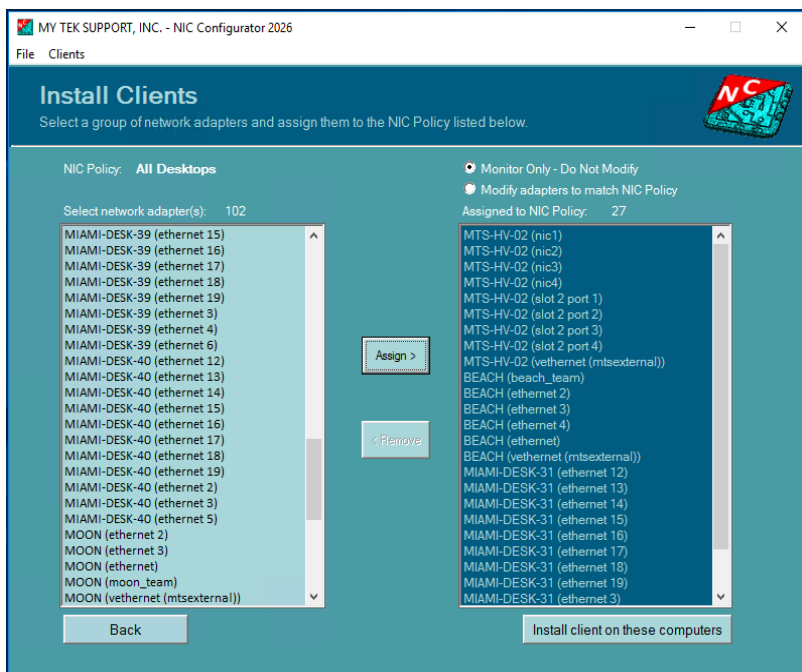
Import a NIC Policy or create your own. Assign a group of computers to the policy.



Import a NIC policy to continue to the next dialog box. You can import an existing NIC policy or you can configure network adapter advanced settings and save those settings as a new NIC policy, go back into Import Policy and import the policy you just saved.

To save a NIC Policy, select a NIC Property and configure a value for that property. Do this for each property you wish to add to your new NIC policy and then click the Save Policy button. Clicking the Save Policy button displays the NIC Configurator 2026 - Save Policy dialog box. This dialog box allows you to view the contents of your new NIC Policy before you give it a name and save it. At the "Save NIC policy as:" edit box, type in a name for your policy and then click Save. If you wish to use this policy click the Import Policy button, select your new policy from the dropdown box, and then click Import. You can now select computers so that NIC Configurator 2026 can find network adapters and give you the option of assigning selected network adapters to the policy you just imported. Type in your domain administrator username and password, then click the Query for NICs button.

Select a group of network adapters and assign them to the imported NIC Policy



Here, you can select specific network adapters and assign them to the NIC Policy listed on this dialog box. You can also choose to have NIC Configurator 2026 self-manage these adapters performance settings by selecting “Modify adapters to match NIC Policy”.

Once you've assigned network adapters to the Imported NIC policy you can click the “Install client on these computers” button. Client installation will begin on the selected computers and your NIC policy assignments will be set.

Once installation has been completed, the NIC Configurator 2026 opening dialog box appears. You can now view NIC Compliance Monitor by clicking the Clients > Monitor > NIC Compliance menu items.

Firewall Service Ports

If there is a firewall between NIC Configurator 2026 and the computers managed by NIC Configurator 2026 (clients), the below ports must be opened on the firewall. NIC Configurator 2026 uses the below service ports to connect to computers in your

network.

SOURCE	DESTINATION	PORT	PROTOCOL
NIC Configurator 2026 Console Computer	DNS Server	53	UDP
	DNS Server	53	TCP
	Domain Controller	88	TCP
	Domain Controller	123	UDP
	Domain Controller	135	TCP
	Domain Controller	389	UDP
	Domain Controller	389	TCP

	Domain Controller	445	TCP
	Domain Controller	1025	TCP
	NIC Configurator 2026 Clients	135	TCP
	NIC Configurator 2026 Clients	445	TCP
	Subnet Broadcast Address	137	UDP

To Remove NIC Configurator 2026 Clients

From the NIC Configurator 2026 opening dialog, click the Clients menu item, and then click Remove. Fill in the fields on this dialog page to search for computers that have the NIC Configurator 2026 client installed and click the Find button.

When the computer list is returned, select computers where you want to remove the NIC Configurator 2026 client and click the Assign button. Click the Remove Client Software button. The clients will be scheduled for immediate removal.

Once the Opening Dialog box appears again, you can go into Compliance Monitor or Traffic Flow Monitor and watch the data from clients begin to remove from the monitor. Once all computer listings are removed from the monitors, you can close out of all NIC Configurator 2026 dialog boxes.

To Remove NIC Configurator 2026 from your computer

You will now need to go to Control Panel to uninstall the main NIC Configurator 2026 software from your computer.

Operating Systems, Memory, Network

The following 64-bit operating systems are supported:

Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 11, Windows 10.

Virtual versus physical machines:

NIC Configurator 2026 server console and client software can be installed on physical and virtual machines.

NIC Configurator 2026 server console can be installed on VMWare ESXi virtual machines and Microsoft Hyper-V virtual machines.

NIC Configurator 2026 client software can be installed on VMWare ESXi virtual machines, Microsoft Hyper-V Servers (physical hosts), and Microsoft Hyper-V virtual machines (guests).

Recommend installing NIC Configurator 2026 server console on Windows Server 2025 or Windows Server 2022.

Server Console System Resources Recommendations:

Memory: 32 GB

vCPU: 4

Disk Drive: SSD

Network: 1 Gigabit

This product is for Windows enterprise environments where computers are part of an Active Directory forest/domain. NIC Configurator 2026 will only work on computers that are part of a Windows Active Directory domain.

Comments and Feedback

Please send all comments and feedback to the following email address: support@myteksupport.com.