pathSolutions

# TotalView 14.1 Deployment Guide


NetOps | SecOps | Telecom Ops | RemoteInsight

PathSolutions, Inc.

www.PathSolutions.com | Support@PathSolutions.com | Sales@PathSolutions.com

# Contents



PathSolutions, Inc.
3080 Olcott Street #A210
Santa Clara, CA 95054
www.PathSolutions.com
Support@PathSolutions.com
Sales@PathSolutions.com

# System Requirements

The TotalView service installs on a Windows server (or workstation acting as a server), and can be viewed from web browsers on the network. The following are requirements for the server, client web browser, and Call Simulator.

## Virtual Server Requirements

Running the solution on a virtual server is fully supported for deployments below 100,000 interfaces. The server should be configured with a fixed (static) MAC address for licensing purposes.
Windows Service Account Required for Active Directory Authentication, DHCP/IPAM Integration and Server Monitoring:

Active Directory Authentication:

- Member of “Domain User” Global Security Group (Read Only)
- AD Security Group Created for TotalView UI access

Microsoft DHCP/IPAM Integration:

- Member of “DHCP Users” Global Security Group (Read Only)

Server Monitoring:

- Member of “Domain Admin” Global Security Group or Local Administrator on Servers

## Small Network Server Requirements

For networks 25,000 interfaces or less, the following hardware is required:

- ✓ Virtual Machine supported
- ✓ Multi Core Processor (2 VM Cores if Virtualized)
- ✓ 40 GB of free disk space
- ✓ 6 GB of RAM of free disk space
- ✓ 100 MBPS Network Interface Card
- ✓ Runs on 32- and 64-bit Windows
    - o Windows 10
    - o Windows 11
    - o Windows Server 2012
    - o Windows Server 2016
    - o Windows Server 2019
    - o Windows Server 2022

## Medium Network Server Requirements

For networks with more than 25,000 interfaces, but less than 100,000 interfaces, the following hardware requirements are recommended:

- ✓ Virtual Machine supported
- ✓ Multi Core Processor (4 VM Cores if Virtualized)
- ✓ 60 GB of free disk space (Flash storage)
- ✓ 8 GB of RAM for the service
- ✓ 1 Gbps Network Interface Card
- ✓ Runs on 32- and 64-bit Windows
    - o Windows Server 2012 (including Server 2012 R2) 64 Bit
    - o Windows Server 2016
    - o Windows Server 2019
    - o Windows Server 2022

## Large Network Server Requirements

For networks with more than 100,000 interfaces, the following hardware requirements are recommended:

- ✓ Dedicated hardware (Virtual machine not recommended)
- ✓ Quad-core 2 GHz processor or faster
- ✓ 100 GB of free disk space (Flash with RAID 0 striping)
- ✓ 8 GB of RAM
- ✓ 1 Gbps Network Interface Card
- ✓ Runs on 32- and 64-bit Windows
  - o Windows Server 2012 (including Server 2012 R2) 64 Bit
  - o Windows Server 2016
  - o Windows Server 2019
  - o Windows Server 2022

## Web Browser Requirements

Any modern HTML5-compliant browser can be used to view the web pages including Chrome, Firefox, and Microsoft Edge. Internet Explorer 11 is not supported. This is due to IE not being fully compliant with W3C and WHATWG standards, and Microsoft discontinuing support for this browser.

## Call Simulator Requirements

The call simulator is a stand-alone executable that does not require software installation or uninstallation. It requires local administrator rights to be able to run.

- ✓ Dedicated hardware (Virtual machines are not recommended*)
- ✓ Pentium 1 GHz processor or faster
- ✓ 10 MB of free disk space
- ✓ 1 GB of RAM**
- ✓ 10 MBPS Network Interface Card (Wireless not recommended***)
- ✓ Runs on both 32-bit and 64-bit Windows deployments
  - o Windows Server 2008
  - o Windows Server 2012
  - o Windows Server 2016
  - o Windows Server 2019
  - o Windows Server 2022
  - o Windows 7
  - o Windows 8
  - o Windows 10
  - o Windows 11

* The call simulator will run on a virtual machine, but the latency and jitter measurements may be incorrect because the physical hardware is shared with other servers/applications.

** More memory is recommended if multiple call simulators are run on the same computer, and/or if call simulations are run for more than 24 hours.

*** Wireless networks can experience packet loss induced by the fact that WiFi is a shared media channel. Additional loss may be created by environmental factors like access point locations and loading, as well as building materials and equipment.

It is recommended to close all other applications on the computer to avoid having other software introduce testing anomalies. This should also include disabling background tasks like antivirus scans, disk defragmentation and other scheduled tasks like Windows updates.

**Notes regarding Call Simulator load testing**
When loading a network with more than one call, the following additional requirements should be considered:

- Laptops are generally designed for battery savings and do not have fast/wide busses for moving large amounts of data. In general, a low-end netbook PC should be able to generate 25 simultaneous calls from a call simulator before it becomes the limiting factor and starts to introduce latency/jitter/loss.
- High-end laptops should be able to safely generate up to 200 simultaneous calls if they have a dedicated Ethernet adapter, a USB 2.0 or a USB 3.0 Ethernet adapter.
- Desktops and dedicated servers should be able to generate up to 250 simultaneous calls

The target for an end-to-end test should also be considered, as the destination device might not be able to respond to a load:

- Network devices like switches, routers, and access points should be able to respond to 10 calls but might have problems if additional traffic is sent to them, since management processes are not designed to *respond* to large volumes of traffic.
- VoIP phones generally have small CPUs designed to handle traffic equivalent to 1-2 calls at the same time. They might fail to respond if more traffic is sent then they can process. Additionally, some VoIP phones may be configured with firewalls that block 90% of non-SIP-registered traffic.
- If the target computer is a virtual machine, it may show large latency and jitter spikes due to the virtualization process.

When running more than one call simulator on the same computer, the timing and bus bandwidth between the call simulators is shared, and an additional number of resources are lost as a result of Windows task switching. This additional overhead loss may be significant depending on the computer's resources.

For example, 200 simultaneous calls might be able to be run with one call simulator. If two call simulators run with 100 calls each, it may start to show latency/jitter/loss on one or both call simulators. This effect may be reduced by assigning processor affinity to each call simulator:
https://www.windowscentral.com/assign-specific-processor-cores-apps-windows-10

# Installation

Installation and configuration of the PathSolutions TotalView takes approximately 12 minutes for most networks.

You must have a valid PathSolutions TotalView License to use the software. This will usually arrive in the form of an email from PathSolutions:

pathSolutions

Don't Turtle Your Network

**PathSolutions License**

Thank you for acquiring PathSolutions software.

```
Customer Name:   Cindytv8
Start date:      8/21/2017 12:00:00 AM
End date:        9/5/2018 12:00:00 AM
Interfaces:      10000
```

**Requirements**

- Make sure that the computer where the software is installed meets the system requirements.
- All network switches, routers, gateways, and servers should have IP addresses and SNMP read-only community strings configured. Contact support@PathSolutions.com if you need help with configuring SNMP on your network devices.

**Installation**

1. Download and run the installer
   (use the email link in your email)
2. After the program is installed, the QuickConfig wizard will run. Enter the following information into the QuickConfig wizard to activate the license:

```
Customer number:   12850524
Customer location: hq
```

If you have any questions, please contact Support@PathSolutions.com or call us at 1-877-748-1444.

License information can be obtained from your PathSolutions reseller or directly from PathSolutions.

PathSolutions license support: 1-877-748-1777 Support@PathSolutions.com

To set up the PathSolutions TotalView on your machine, use the link provided in the email to download the latest version from the PathSolutions website.

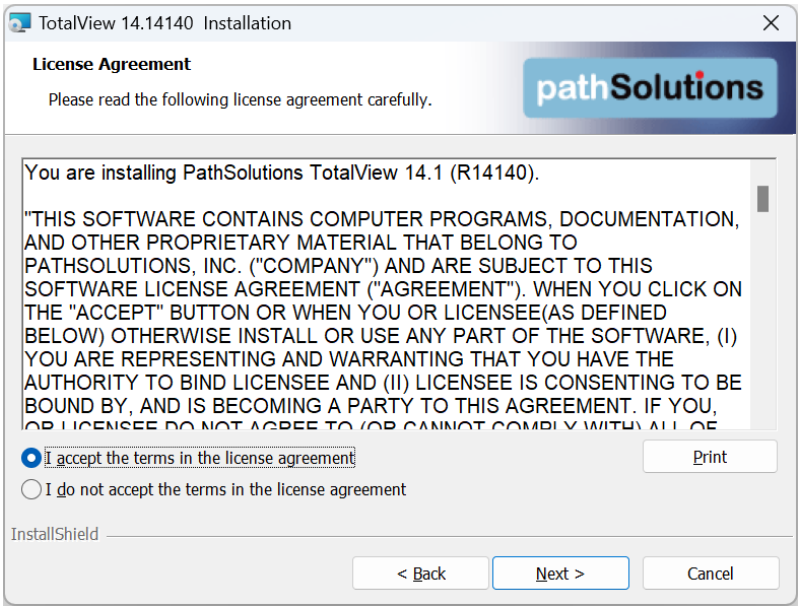
TotalView should be installed on a server or workstation that has a permanent connection to the network.

# Installer

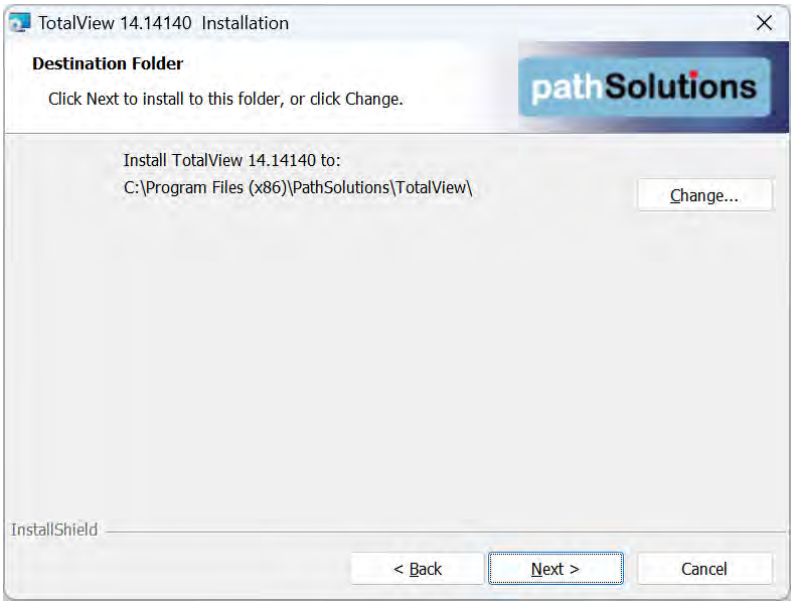
The software installer is a Microsoft MSI file and requires local administrator privileges to install the software on a computer. Open and select **Next**.


Select the **I accept the terms in the license agreement** radio button, and then select the **Next** button.

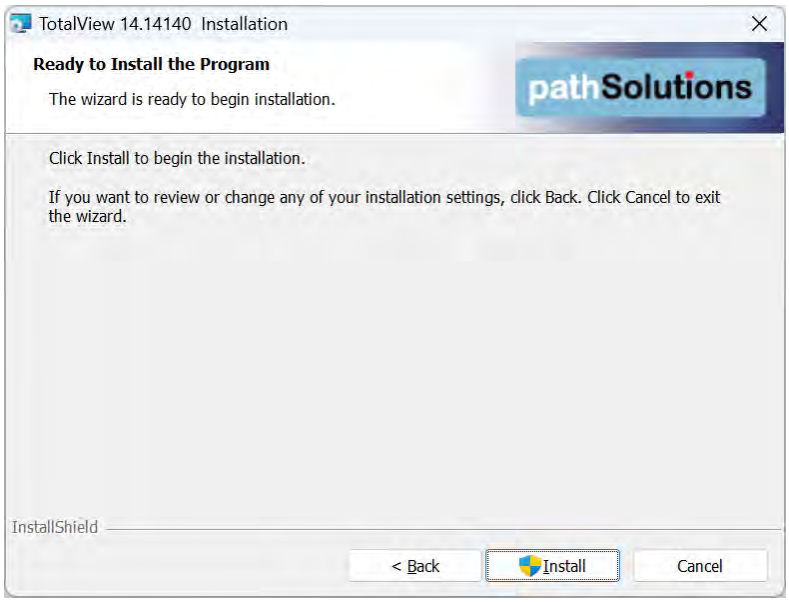
Follow the steps of installation as instructed on screen.



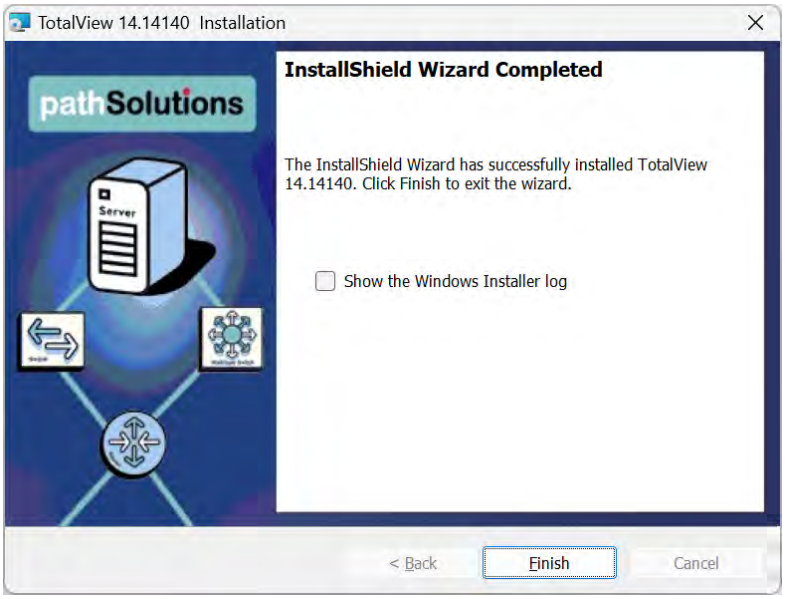
On the next screen, note the destination folder where the program will install. If you wish to change the location, select **Change**. When finished, select **Next**.




At this point the program is ready to be installed. Select **Install** to install the program.



Select **Finish** to complete the installation.




**Note**: The QuickConfig Wizard will automatically begin after you finish these steps.

# QuickConfig Wizard

The **QuickConfig Wizard** will auto-configure the PathSolutions TotalView for you and begin monitoring in just a few minutes.

Depending on which features/modules have been licensed, there may be additional steps presented.

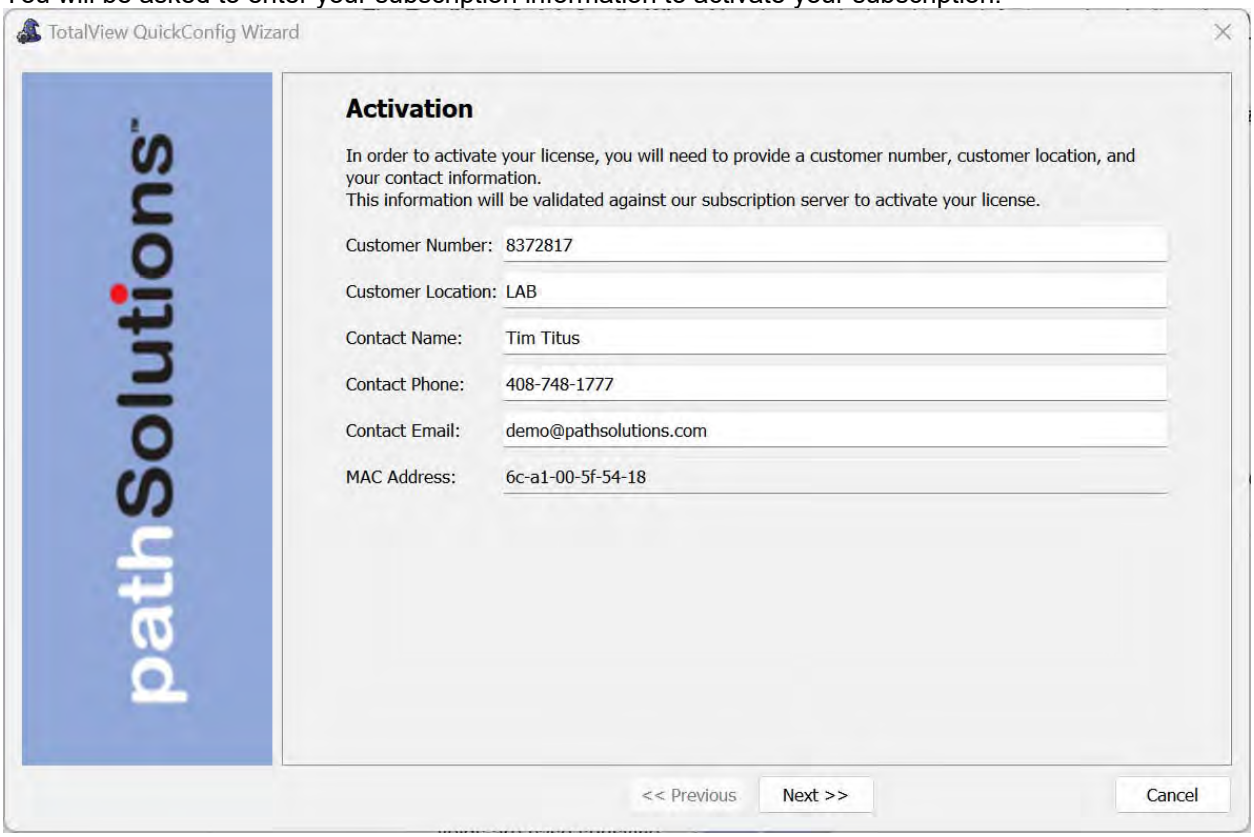
The **QuickConfig Wizard** has nine steps after activation:

Start: Activation
Step 1: SMTP Server
Step 2: Windows Domain Authorization
Step 3: Monitor Network Devices
Step 4: Discovery Methods
Step 5: SNMP Security
Step 6: Emailed Reports: “Nightly Weather Report”
Step 7: Monitor Windows Server
Step 8: Emailed Reports: “Nightly Security Report”
Complete: Start Discovery

After installation is complete, the PathSolutions TotalView will scan your network for devices and begin monitoring.

## Activation

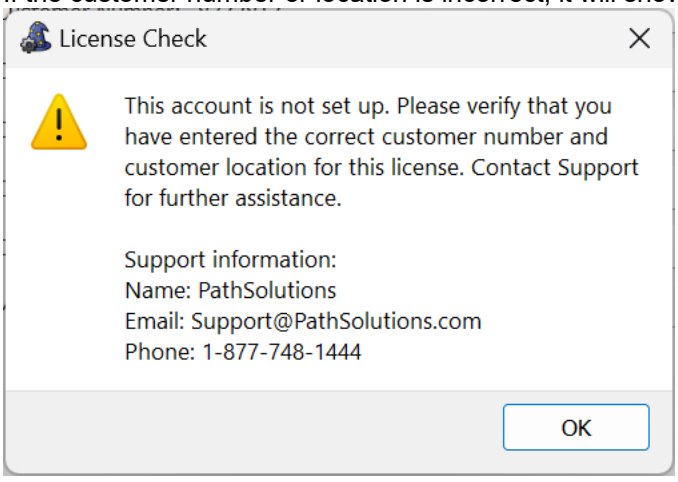
You will be asked to enter your subscription information to activate your subscription.




Enter all fields from your subscription email.

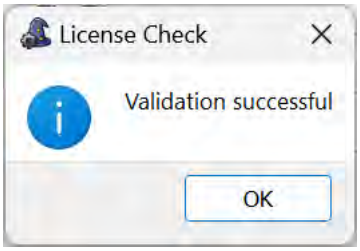
**Note:** **The Customer Number** and **Customer Location** fields are case sensitive. These fields must be entered exactly as they are specified in the subscription email.

If the customer number or location is incorrect, it will show the following:




Verify that the Customer Number and Customer Location are correct or contact support@pathsolutions.com for assistance.

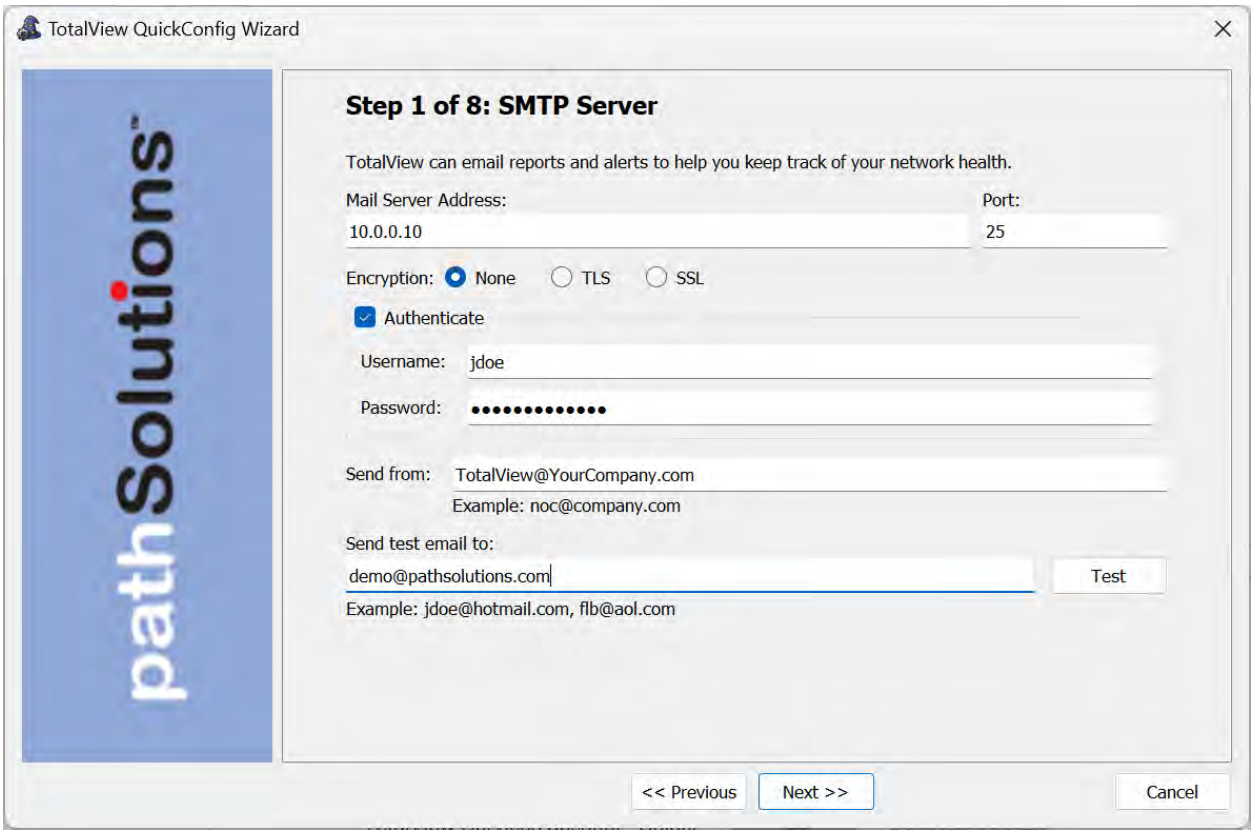
Once the license information has been correctly entered, you will see the following:




Click “OK” to see the next step of the wizard.

## Step 1: SMTP Server

The first step sets up the mail server address for email reports and alerts. Enter your Email SMTP Server information.




You will need to enter the IP address or DNS hostname of your SMTP mail server address or a mail relay server. This mail server should allow SMTP forwarding if you intend to send to individuals at other domain names. See The Administration Manual, **SMTP email Forwarding** for additional information on SMTP email forwarding.

Click the **Test** button to validate that emails can be sent.

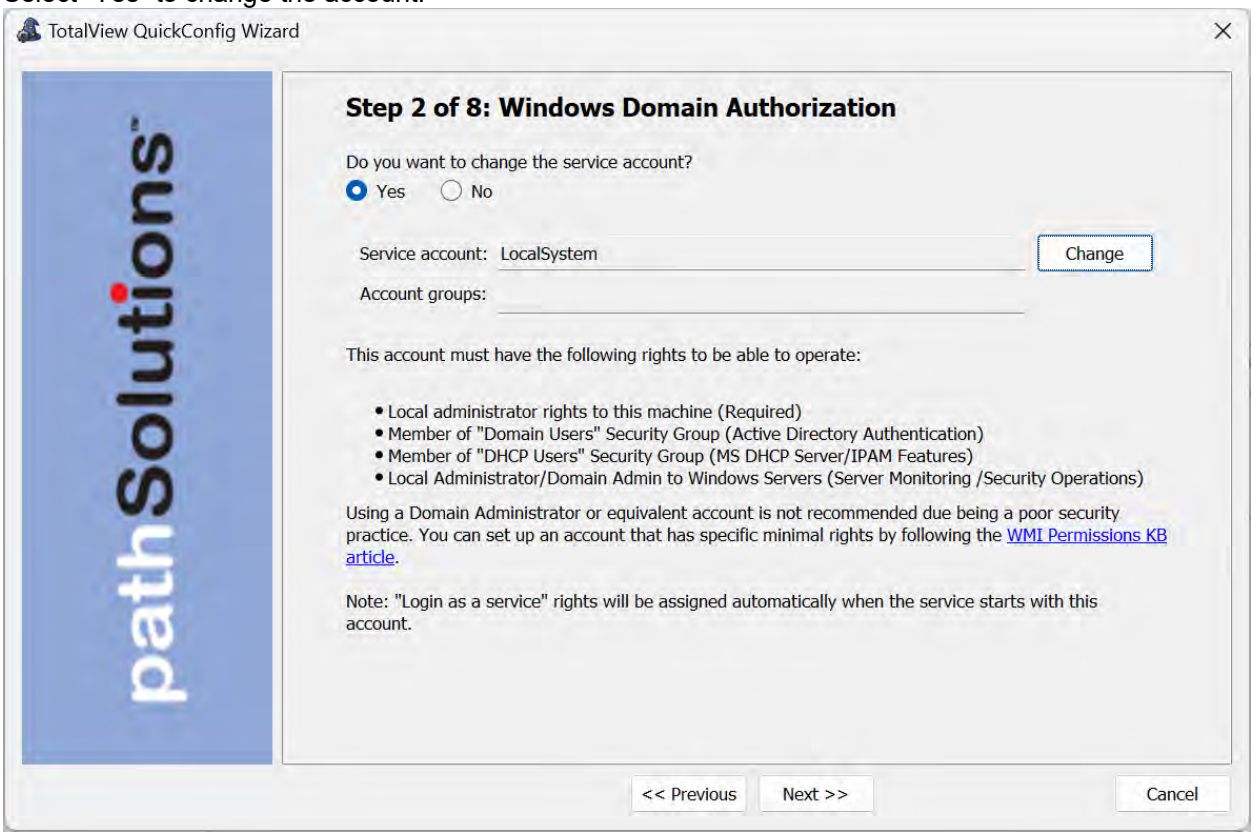
Select **Next** to continue to the next step.

## Step 2: Windows Domain Authorization

Windows domain authorization is required for the following features:

- IPAM: Monitoring of Windows DHCP scopes
- Authentication: AD integration for logins
- Server Monitoring: Monitoring of Windows servers in the domain
- SecOps: SOAR interrogation of Windows client computers

Select “Yes” to change the account.




The rights for this account should have:

- Local administrator rights to the machine (Required)
- Member of “Domain Users” security group (Required for AD authentication)
- Member of “DHCP Users” security group (IPAM DHCP scope monitoring)
- Local Administrator/Domain Admin to Windows servers (Server monitoring/Security Operations)

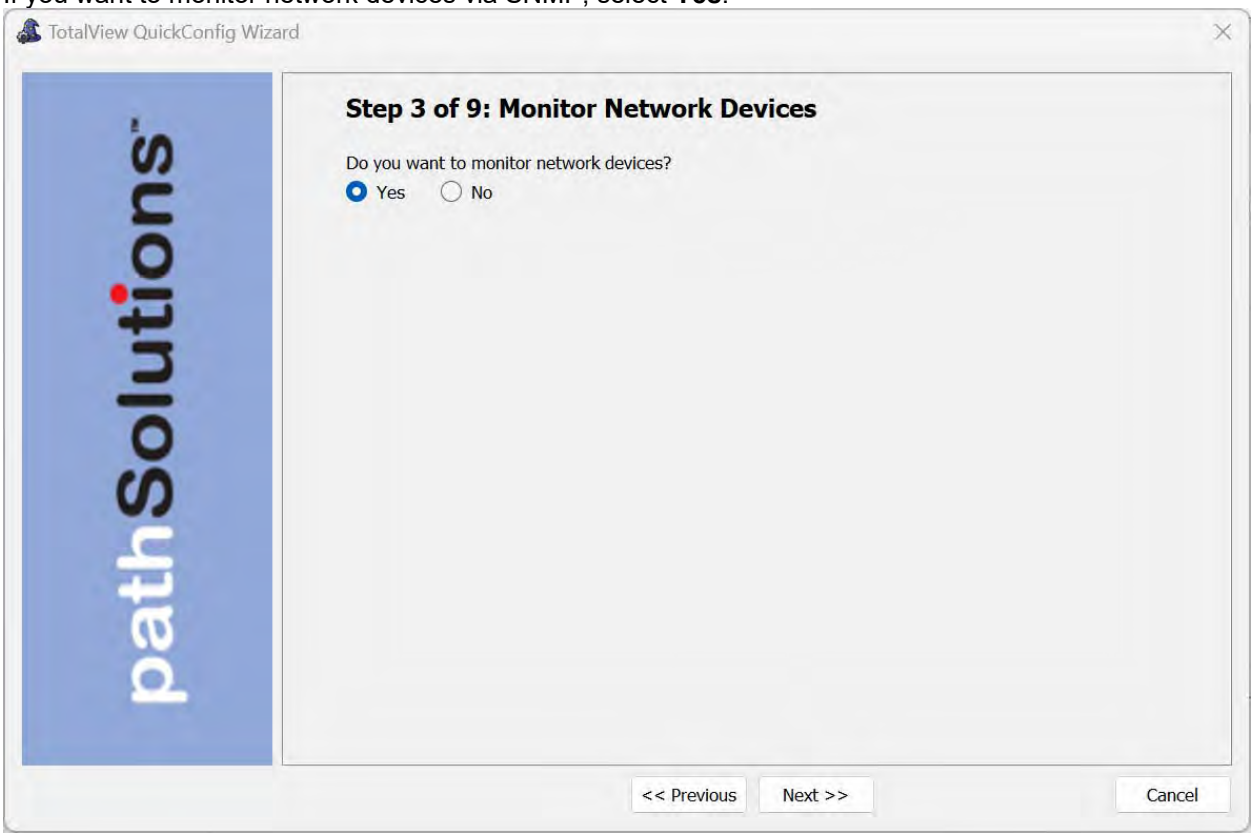
For more information on the specific rights to set up, refer to the knowledgebase article:
https://support.pathsolutions.com/support/solutions/articles/14000126149-wmi-permissions-for-secops-and-server-monitoring

Click “Change” to select the account to use.

Select **Next** to continue.

## Step 3: Monitor Network Devices

If you want to monitor network devices via SNMP, select **Yes**.



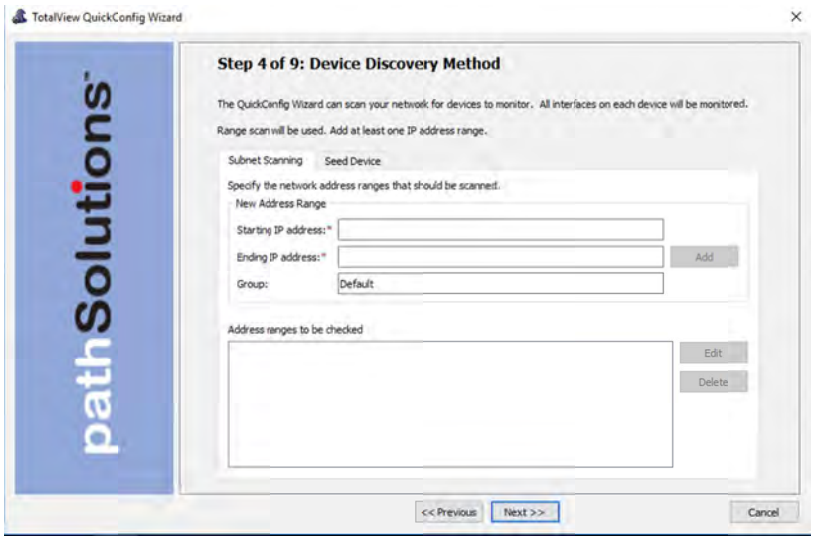

Select **Next** to continue.

## Step 4: Discovery Methods

Select the discovery method you want to use to scan your network for devices to monitor: either subnet scanning method or the Seed method? Then enter the details requested.

Subnet Scanning Method

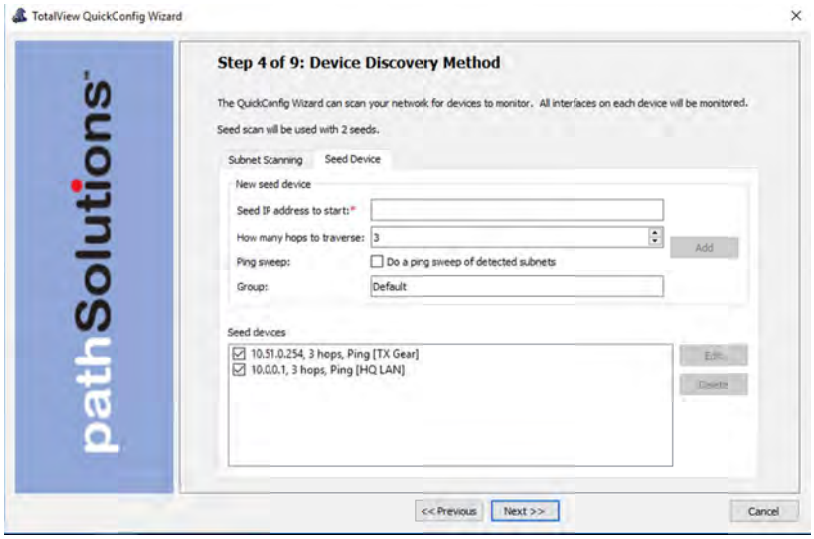
This method will scan portions of IP subnets to look for devices to manage/monitor. This method is best when you know the specific subnets that you want to scan to find devices.




Seed Device Method

This method will use SNMP to talk to a specific seed device that is known to communicate via SNMP and will query it for subnets that it knows about. It will then scan those subnets and continue for a specified number of hops out from that seed device.

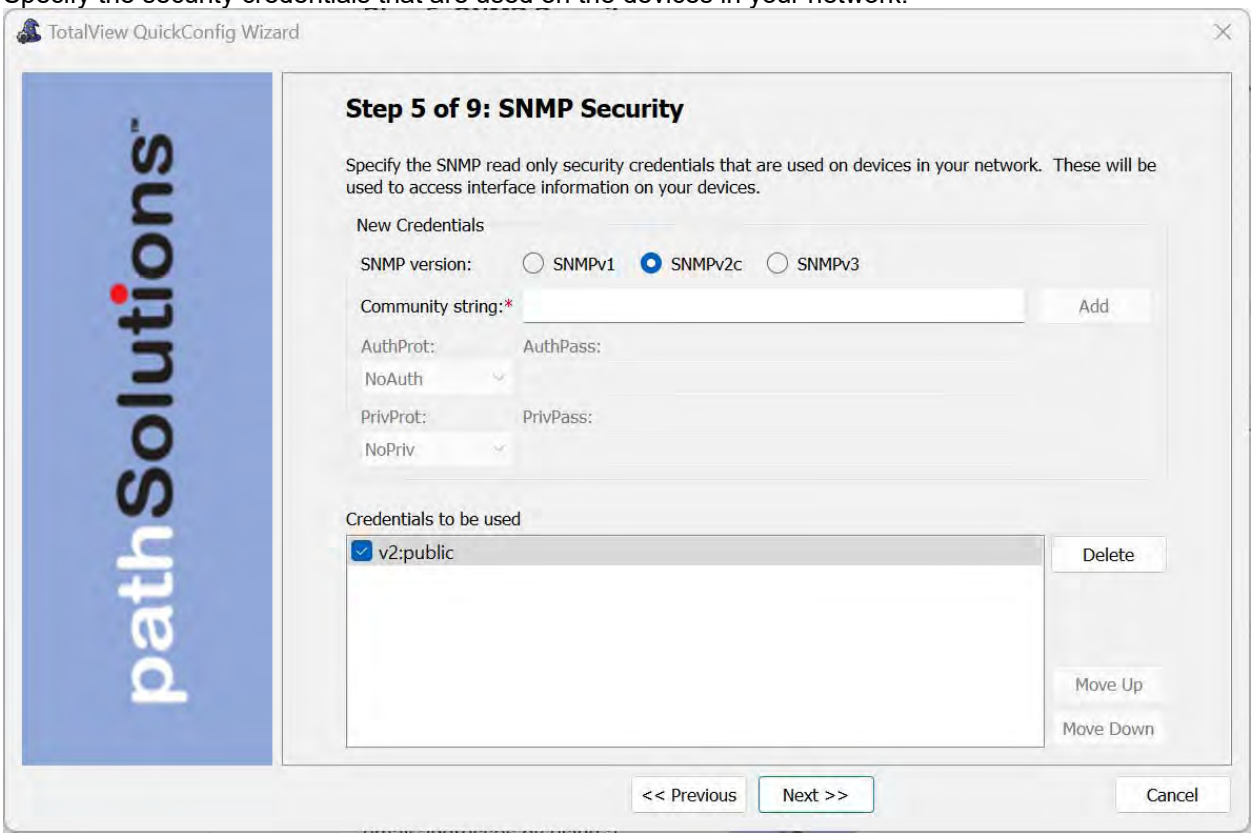
This method may not work if a remote firewall does not have SNMP support, or does not support the IP-MIB (mib-rfc4293).




Select **Next** to continue.

## Step 5: SNMP Security

Specify the security credentials that are used on the devices in your network.



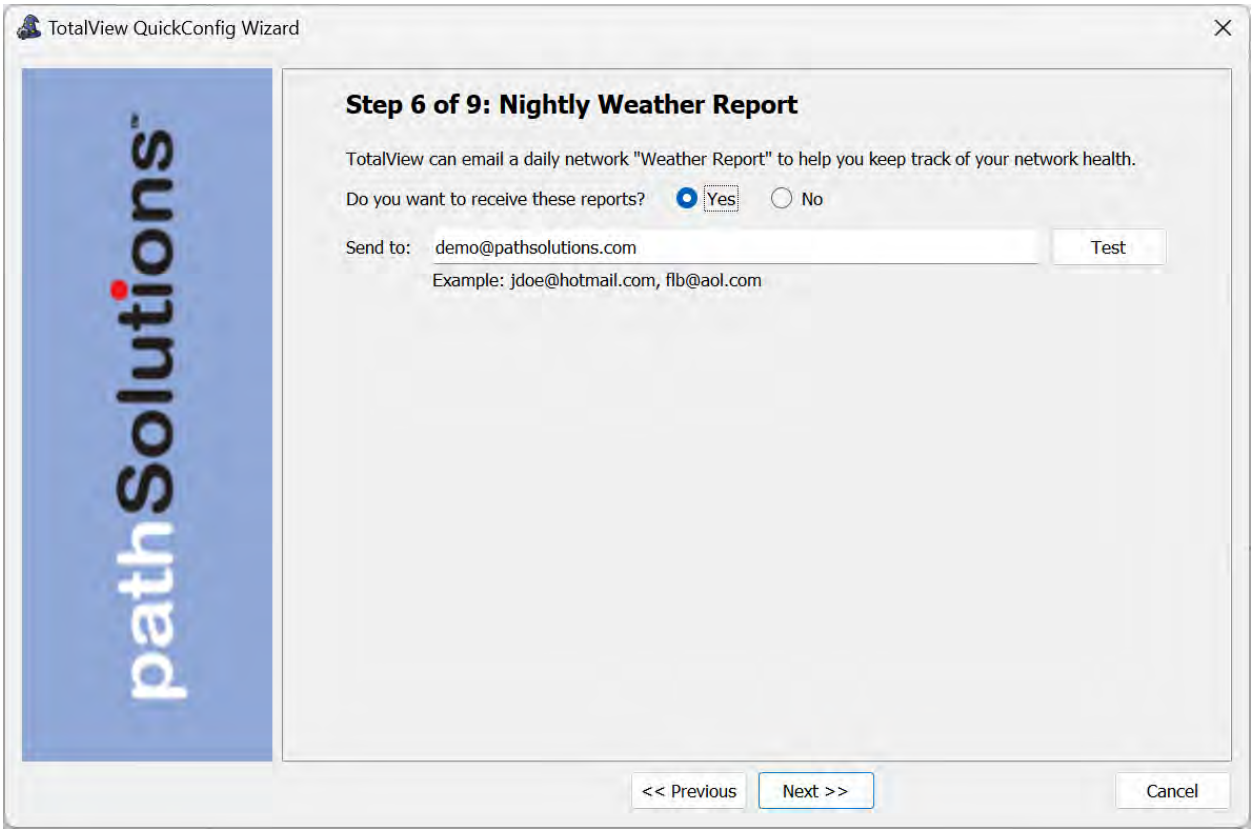

TotalView can use SNMP v1, SNMP v2c, or SNMP v3.

You can enter multiple different credentials and then move each up or down in the list to have it prefer one over another.

Select **Next** to continue.

## Step 6: Emailed Reports: “Nightly Weather Report”

Step 6 allows you to choose to receive the Nightly Weather Report. This report shows a summary of problems and issues that exist on the network so you can start your day with an understanding of things that are broken or impaired on the network.



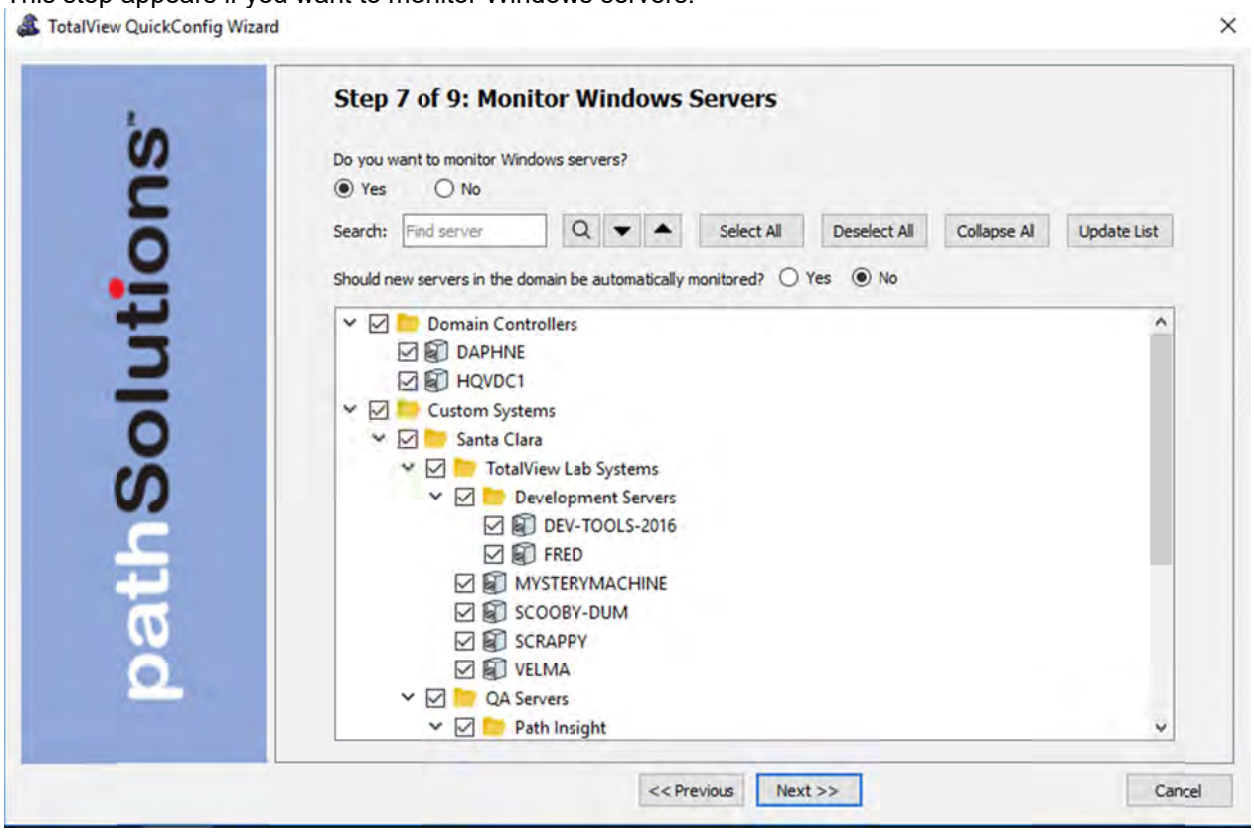

Enter the Internet SMTP email addresses that should receive the daily report. You can enter multiple email addresses by using a semicolon, comma or space character between each email address.

After entering this information, select **Test** to send a test email. If there is a problem sending an email, you will be presented with detailed information how to resolve the problem.

Select **Next** to continue.

## Step 7: Monitor Windows Servers

This step appears if you want to monitor Windows servers.



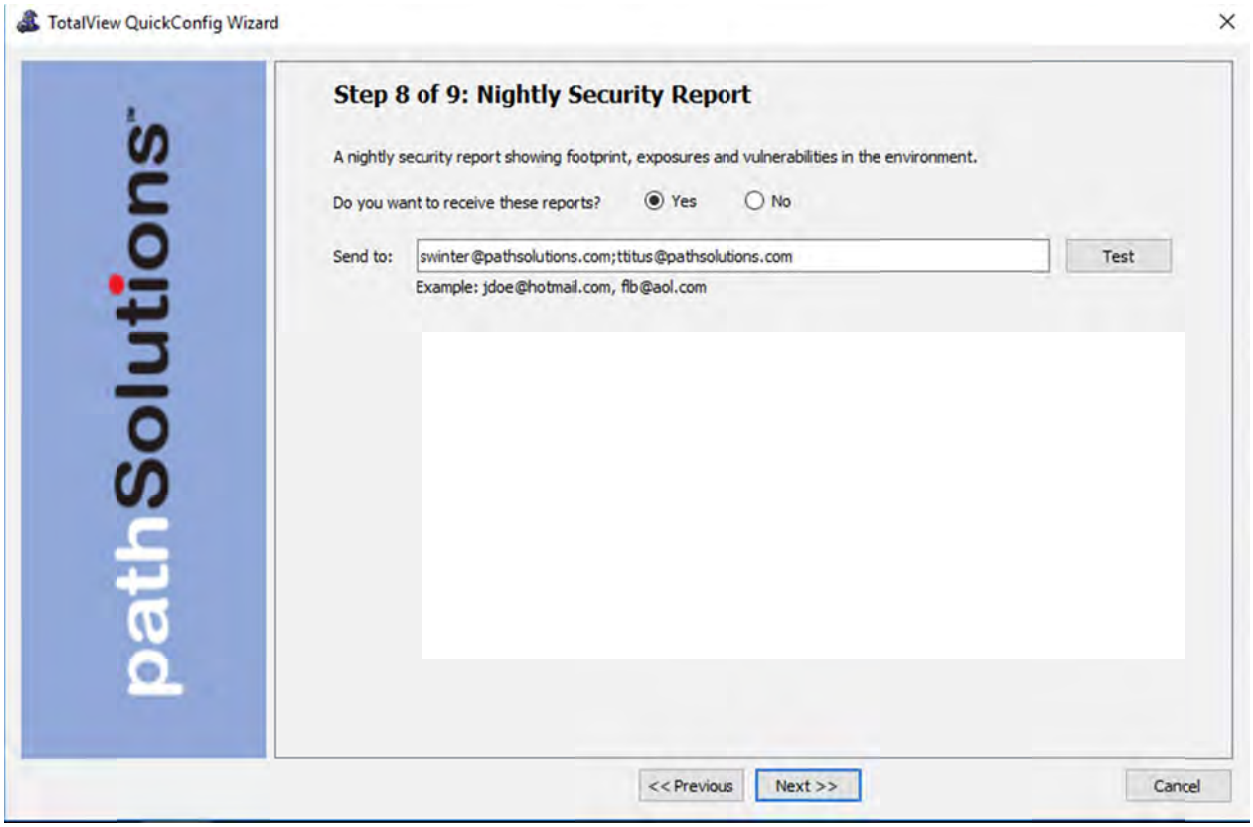

Select **Yes** or **No** to monitor Windows Servers.

Enter a server into the **Search** field. Select **Select All**, **Deselect All**, **Collapse All**, and **Update List** to modify the list.

Select **Next** to continue.

## Step 8: Emailed Reports: "Nightly Security Report"

Step 8 allows you to choose to receive the Nightly Security Report. This report shows a summary of security issues that should be addressed.




*This step appears if you have a license to a TotalView Security Operations Manager:*

Enter the Internet SMTP email address or addresses that should receive the alerts.

After entering this information, you can select **Test** to send a test email. If there is a problem sending an email, you will be presented with detailed information how to resolve the problem.

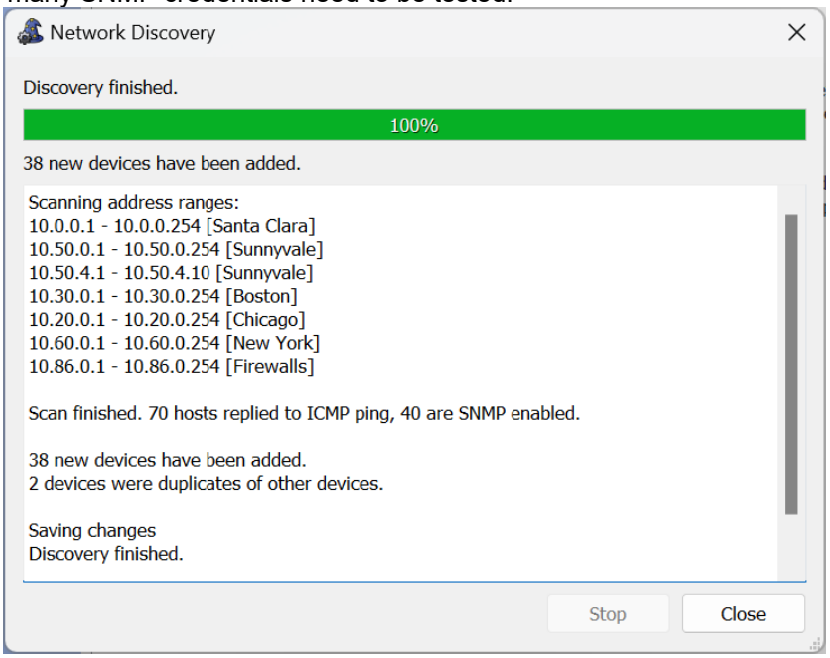
Select **Next** to continue.

## Step 9: Start Discovery

This step appears when the wizard is ready to scan the network to search for SNMP manageable devices:


Select **Start Discovery** to continue.

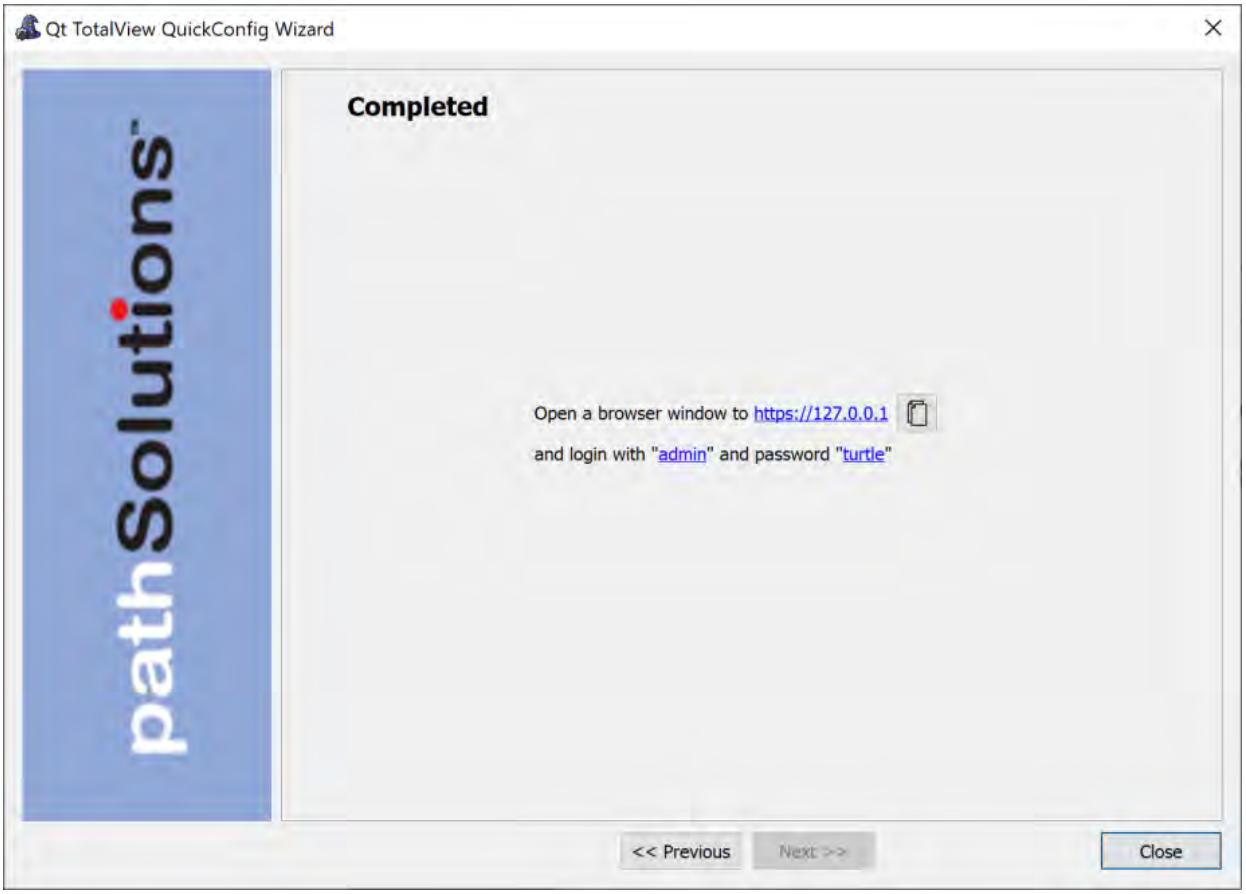
The scanning process may take a few minutes or a few hours depending on the number of subnets scanned and how many SNMP credentials need to be tested.




Click “Close” when you are ready to continue.

## Completed

This screen appears when the scan of your network is done, and the web pages are ready to view.




At this point you should be able to click on the URL or click the Copy button to copy the URL to your clipboard and then paste it into a browser to get started.

The default account is “admin” and the default password is “turtle”.

Select **Close** to complete the wizard.

That is all that is necessary to install and configure the program. You should be able to immediately start viewing your network and solving problems.

## Sales

Sales@PathSolutions.com
(877) 748-1777 (toll-free main)
(408) 748-1777 (main)
(408) 748-1666 (fax)

## Technical Support

Support@PathSolutions.com
(877) 748-1444 (7x24 tier 1 telephone support)
(408) 748-1777 Select 1 for tier 2 support