Network Security Scanner

Installation Guide

Powered By Retina

TC:5/23/2019

Table of Contents

BeyondTrust Network Security Scanner Introduction and Overview

This guide provides the installation instructions and software requirements for the BeyondTrust Network Security Scanner.

> For information about its features, benefits, functionality, and basic procedures, please see the *BeyondTrust Network Security Scanner User Guide*.

BeyondTrust Network Security Scanner provides vulnerability testing for multiple platforms, automatic fixes of vulnerabilities and the ability to create your own audits. In addition, the BeyondTrust Network Security Scanner allows you to proactively secure your networks against the most critical vulnerabilities by incorporating the most up-to-date vulnerabilities database. Since vulnerability audits are added continually, this database is updated at the beginning of each session (although this feature is not enabled by default).

Using the scanner, you can:

- Scan in parallel using the scanner's queuing system to scan up to 128 targets simultaneously.
- Perform the majority of scans without administrative rights. This allows you to quickly and easily secure your globally distributed networks.
- Create custom audit scans to enforce your internal security policies, such as deployments and machine configurations.

The scanner uses Access or any ODBC data store for storage and a management and aggregation server to control remote scanners. In addition, multi-user authentication, summary and executive reporting capabilities, and a comprehensive tracking system are available.

Install the BeyondTrust Network Security Scanner

You can download the Network Security Scanner from our customer portal, www.beyondtrust.com/support.

> ***Note:*** *A username and password are required.*

System Requirements

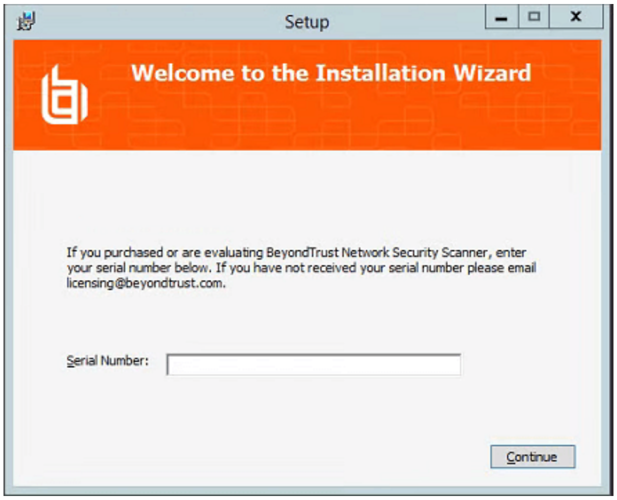
The minimum system requirements for Network Security Scanner are:

Operating Systems	Windows 7 SP1 or later (32-bit and 64-bit) Windows 8.1 (32-bit and 64-bit) Windows 10 (32-bit and 64-bit) Windows Server 2008 R2 SP1 or later (64-bit) Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 (64-bit) Windows Server 2019 (64-bit)
Processor	Intel Dual Core 2.0Ghz (or compatible)
Memory (RAM)	8 GB
Hard Drive	4 GB minimum
Software	Microsoft .Net Framework 4.5.2 or later Microsoft Visual Studio 2008 and 2017 C++ Redistributable (included with installer) Internet Explorer v9.0 (or later) for report rendering and viewing Universal C Runtime
Network	Ports 443 and 21690 are required for integration with BeyondInsight Network Interface Card (NIC) with TCP/IP enabled
Minimum Screen Resolution	1024x768
Notes	Administrative access required to perform scans

Installation

> ***Note:*** *You can install and uninstall using the command line as detailed in "Appendix: BeyondTrust Network Security Scanner Command Line Installation" on page 13.*

1. Double-click the scanner installer to display the **Install Wizard**.
2. An informational message is displayed warning you about using multiple firewalls. Close all other firewalls. Click **Continue**.
3. If you are installing a full version of the scanner, enter the serial number provided when you purchased the product. You can access your serial number on the customer portal by selecting **Product Licensing > Managing Your Serial Numbers**. If you are installing a demo version of the scanner, the **Serial Number** field remains blank.

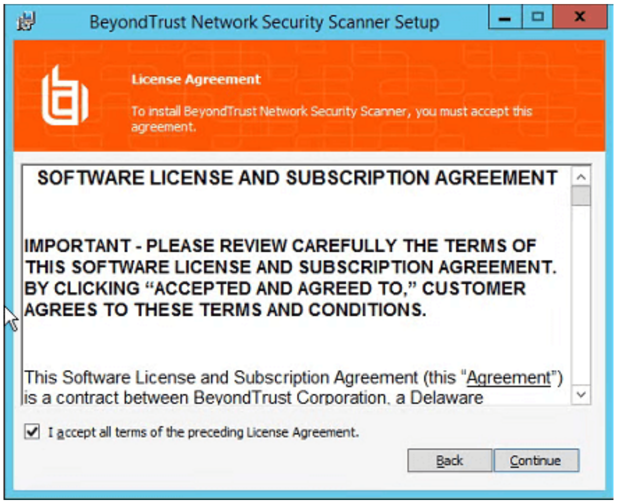


Welcome to the Installation Wizard

If you purchased or are evaluating BeyondTrust Network Security Scanner, enter your serial number below. If you have not received your serial number please email licensing@beyondtrust.com.

Serial Number:

4. Click **Continue**. The **End User Software License Agreement** window displays.
5. After reading the license agreement, select the **I accept all terms of the preceding licensing agreement** check box. You must accept the licensing agreement for the installation to continue.



License Agreement

To install BeyondTrust Network Security Scanner, you must accept this agreement.

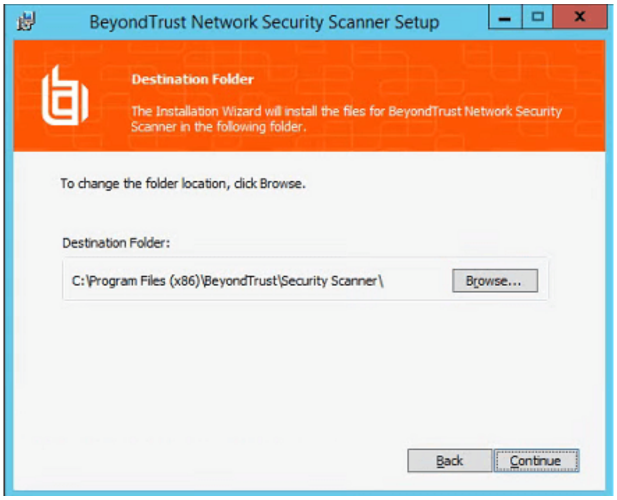
SOFTWARE LICENSE AND SUBSCRIPTION AGREEMENT

IMPORTANT - PLEASE REVIEW CAREFULLY THE TERMS OF THIS SOFTWARE LICENSE AND SUBSCRIPTION AGREEMENT. BY CLICKING "ACCEPTED AND AGREED TO," CUSTOMER AGREES TO THESE TERMS AND CONDITIONS.

This Software License and Subscription Agreement (this "Agreement") is a contract between BeyondTrust Corporation, a Delaware

☑ I accept all terms of the preceding License Agreement.

6. Click **Continue**. The **Destination Folder** window displays.
7. Accept the default location, or click **Browse** and select a destination folder.



Destination Folder

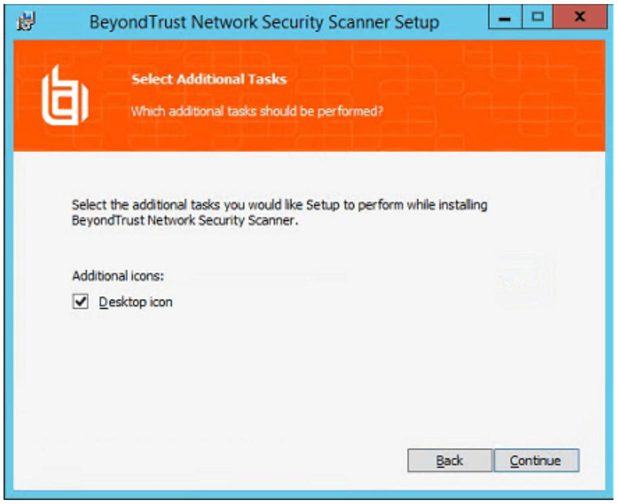
The Installation Wizard will install the files for BeyondTrust Network Security Scanner in the following folder.

To change the folder location, click Browse.

Destination Folder:

C:\Program Files (x86)\BeyondTrust\Security Scanner\

8. Click **Continue**. The **Additional Tasks** window displays.
9. You can select the **Create Desktop Icon** check box, if needed.



Select Additional Tasks

Which additional tasks should be performed?

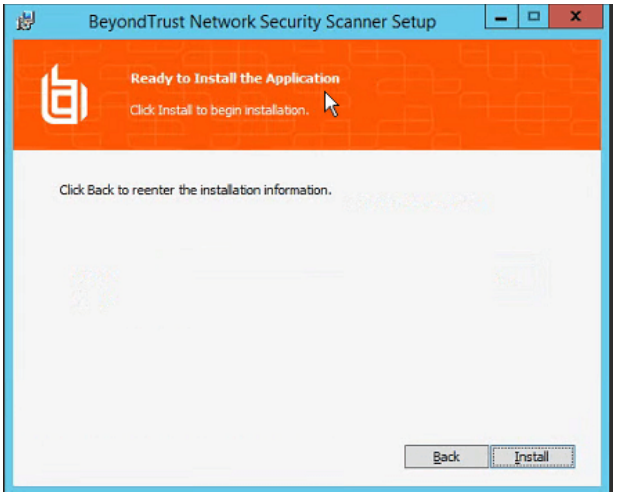
Select the additional tasks you would like Setup to perform while installing BeyondTrust Network Security Scanner.

Additional icons:

☑ Desktop icon

10. Click **Continue**. The **Ready to Install Application** window displays.

> ***Note:** To modify the previous information, click **Back**.*

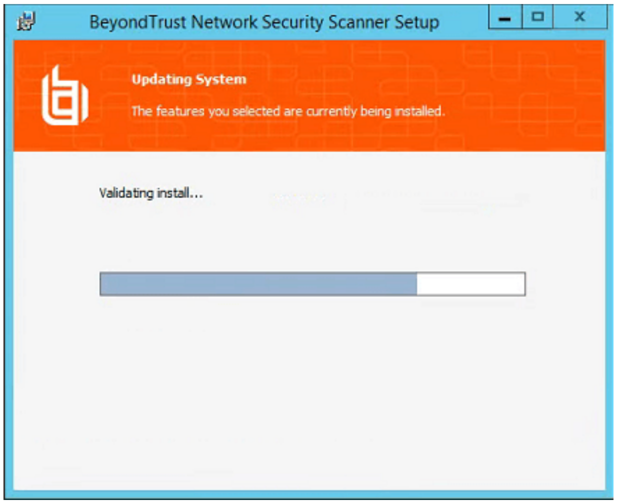


Ready to Install the Application

Click Install to begin installation.

Click Back to reenter the installation information.

11. To continue, click **Install**. Once the scanner is installed, the **Successful Installation** window displays.

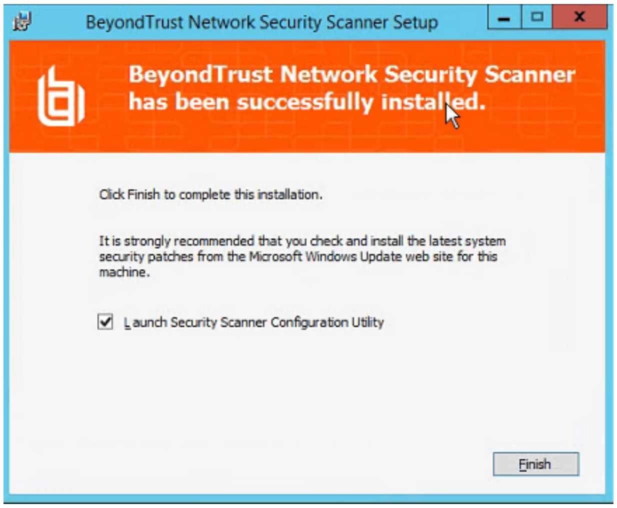


Updating System

The features you selected are currently being installed.

Validating install...

12. After the scanner installation completes, you can choose to start the Scanner Configuration Utility to create a connection to the BeyondInsight management console. Select the **Launch Configuration Utility** check box to start the Configuration Utility after installation.


BeyondTrust Network Security Scanner Setup

BeyondTrust Network Security Scanner has been successfully installed.

Click Finish to complete this installation.

It is strongly recommended that you check and install the latest system security patches from the Microsoft Windows Update web site for this machine.

☑ Launch Security Scanner Configuration Utility

Run the Configuration Utility

The Scanner Configuration utility allows you to configure:

- **Licensing:** Enter, update, or transfer your Network Security Scanner license key.
- **Central Policy:** The Central Policy server manages event logging, auto-updating audits, and performance settings for the scanner engine. Event logging sends the scan information to the management console and includes: port, services, and general scan information.
- **Event Management:** Configures the Event Client. The management console needs to be aware of the scanner as a supported application. Scanner events are sent to the management console where scanner activities can be reviewed and managed.
- **Automatic updates:** The Auto-Update feature synchronizes the scanner with the most up-to-date audits. These updates will continue to occur at the beginning of each session. This allows you to proactively secure your network against the latest vulnerabilities.

You are asked to run the Network Security Scanner when you close the Scanner Configuration Utility.

***Note:** Connections to the management console are not supported on the following Network Security Scanner solutions: **Community** and **Unlimited**. Contact your BeyondTrust representative to learn more about management console features.*

This guide assumes all of the required management console components are successfully installed.

For more information, please see the *Management Console Installation Guide*.

Licensing

1. Click **Manage License**. The **License Management** window displays.
    a. If Network Security Scanner is not licensed, you are prompted to enter the serial number.
    b. If Network Security Scanner is licensed, you are given the choice to **Transfer** or **Update** the license.

Central Policy

1. Click **Configure Central Policy**. The **Central Policy Configuration** window displays.
2. Click the **Enable Central Policy** check box.
3. Enter the hostname or IP address for the management console. This is the server where the management console resides.
4. Enter the credential that can access the server.
5. Click **Test Central Policy** to ensure the machine where the scanner is installed can connect to the management console server.
6. Optionally, you can select the **Enable legacy Central Policy support** check box to communicate to the management console using port 10001. By default, Central Policy uses port 443.
7. Click **Save Settings**.

Event Management

1. Click **Configure Event Client**. The **Events Client Configuration** window displays.
2. Select the **Enabled Applications** tab, if it is not already selected.
3. Select the **Network Security Scanner** check box, and then click **OK**.

Automatic Updates

1. Click **Check for updates**. The **Auto-Update** window displays.
2. To configure Auto-Update, click **Configure**. The **Configuration Properties** window displays.
3. To integrate with Enterprise Update Server, select the **Update Server for All Applications** radio button, then modify the server name to match the **Enterprise Update Server** name and click **OK**.

> For additional information, please see the *Enterprise Update Server documentation*.

1. To download updates, click **Next**. The updates begin installing, and then the **Update Summary** window displays.

Set Credentials for the Scanner in the Management Console

Network Security Scanner uses credentials to access target assets, such as networks, workstations, servers, and printers.

You can run a scan without administrator access; however, administrator access ensures a thorough scan.

> ***Note:*** *To run a fully credentialed scan of a UNIX device, SSH access is required. For SSH, provide the root or admin username.*

> ***Note:*** *To run a fully credentialed scan of a Windows device, NetBIOS access is required. NetBIOS is enabled by default.*

Uninstall the Scanner

Using the **Uninstall** wizard, you can complete the following steps to remove Network Security Scanner from your system.

We recommends that you exit all Windows programs before you run the uninstall.

1. Select **Start > Settings > Control Panel**, then click **Add/Remove Programs**.
2. Select **BeyondTrust Network Security Scanner**, then click **Remove**. The **Add/Remove Programs** dialog displays.

3. When prompted if you are sure you want to uninstall, click **Yes**.
4. To retain the license for future use on the same machine, click **No**.To remove the configuration data, click **Yes**.

The progress of the uninstall is displayed. When complete, the progress dialog closes. Some system configurations can require a system restart to complete the uninstall. If so, a prompt displays stating you must restart to complete the uninstall.

Get Started Using BeyondTrust Network Security Scanner

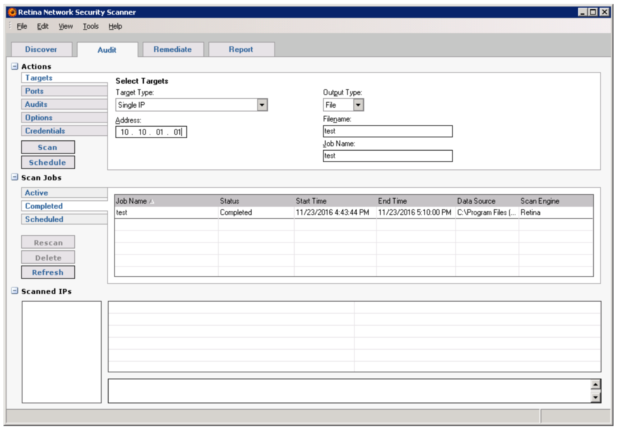
You can run a quick scan using the default values. This allows the scanner to locate responsive nodes, then launch pre-defined scans against the targets. The result is a list of vulnerabilities and remediation that can be viewed online or exported and saved.

If you are not using the management console, you are ready to run scans.

Start the Scanner

Select **Start > Programs > BeyondTrust > Network Security Scanner**. The scanner application opens. The following tabs are available:

- **Discover**: locates devices, such as workstations, routers, and printers, by single or multiple IP addresses.
- **Audit**: scans any device with an IP address and returns a list of vulnerabilities and fixes.
- **Remediate**: generates a list of vulnerability information and recommends methods to resolve the vulnerability.
- **Report**: provides executive overview reports and detailed summary reports of vulnerabilities and fixes.



Select Targets

Target Type: Single IP

Address: 10 . 10 . 01 . 01

Output Type: File

Filename: test

Job Name: test

Job Name	Status	Start Time	End Time	Data Source	Scan Engine
test	Completed	11/23/2016 4:43:44 PM	11/23/2016 5:10:00 PM	C:\Program Files (...	Retina

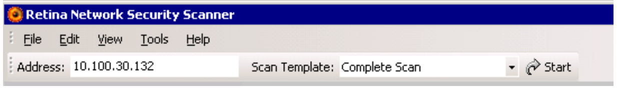
Run a Quick Scan

Using the scanner templates, you can quickly scan based on an IP address or sequential range of IP addresses. The quick scan results allow you to:

- Review the vulnerability results on the **Audit** page.
- Analyze the remediation results on **Remediate** page.
- View the data online or offline using the **Reports** page.

To run a quick scan:

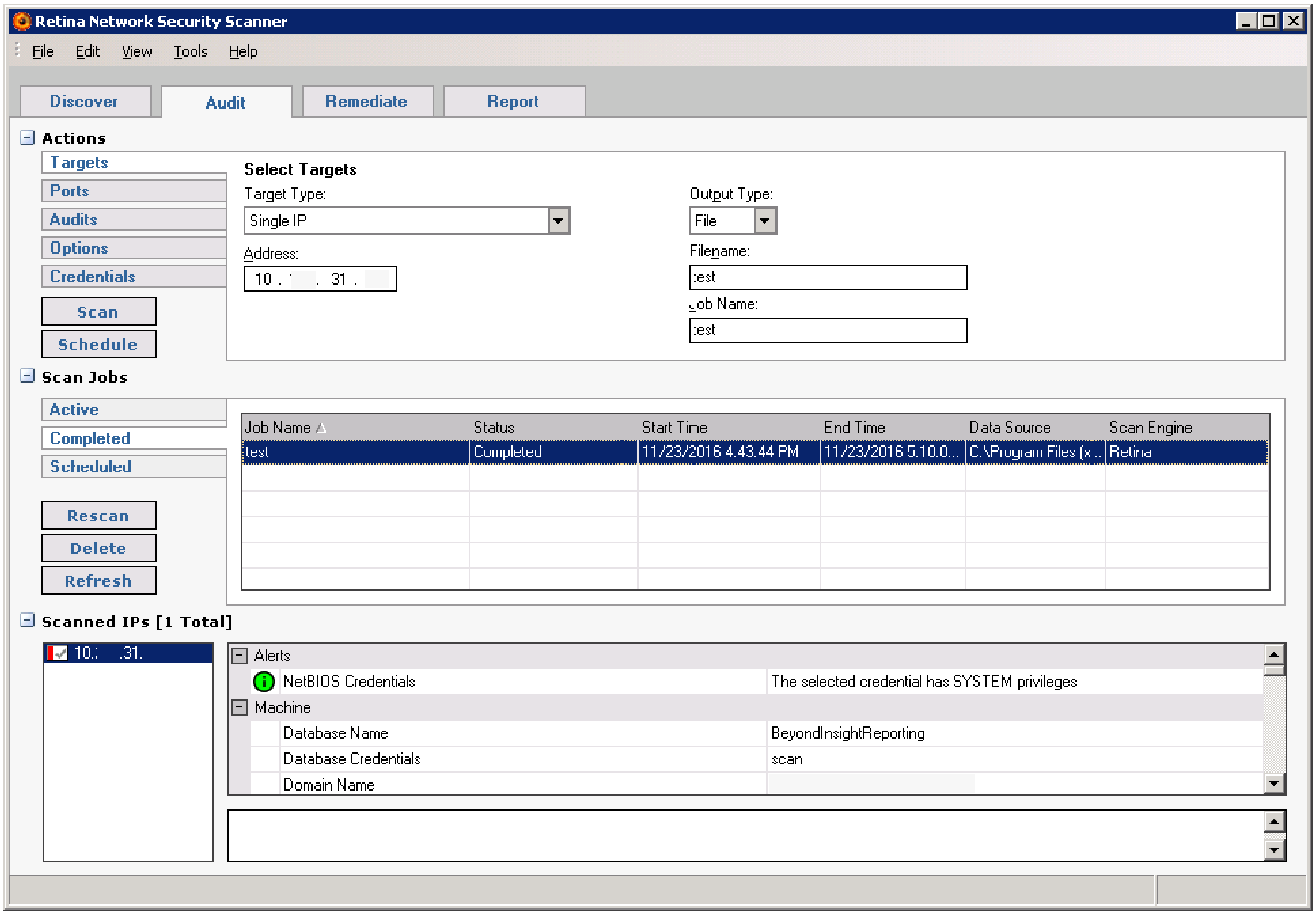
1. On the scanner's main page, select **View > Quick Scan** to display the **Quick Scan** toolbar. The **Quick Scan** toolbar displays the **Address** and **Scan Template** fields.



Address: 10.100.30.132

Scan Template: Complete Scan

2. Verify the IP address in the **Address** field.
3. In the **Scan Template** list box, select **Complete Scan** or **FBI-SANS Top 20**.
    - **Complete Scan** scans the IP address for every vulnerability audit in the **Vulnerabilities** database.
    - **FBI-SANS Top 20** scans for the SANS list of vulnerabilities that require immediate remediation.
4. Click **Start**. The scan begins.
5. To view the scan progress and a summary of the vulnerabilities based on the scanned IPs, select the **Audit** tab. The scan results display in the **Scanned IPs** area.



Select Targets

Target Type: Single IP

Address: 10 . ' . 31 .

Output Type: File

Filename: test

Job Name: test

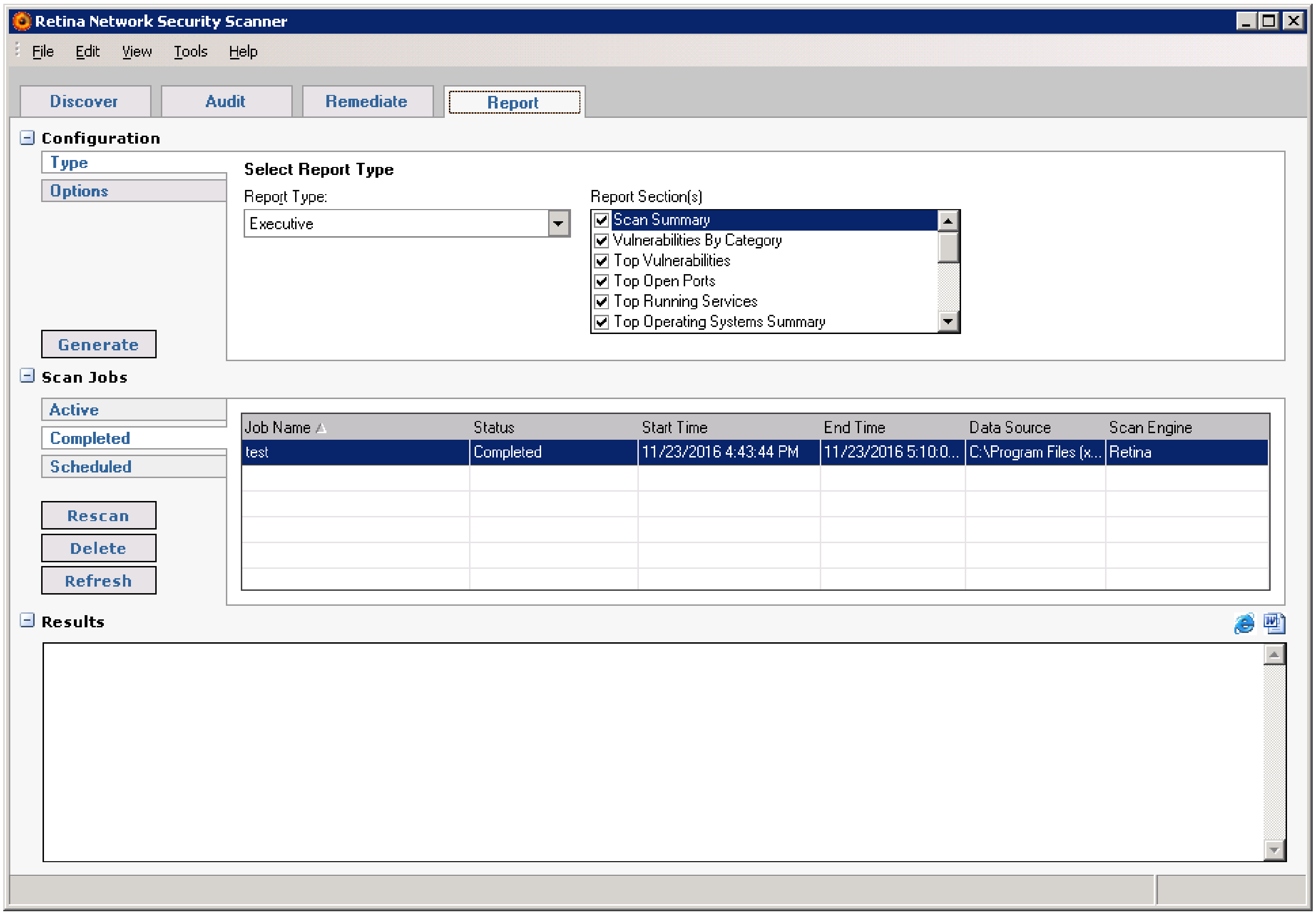
Job Name	Status	Start Time	End Time	Data Source	Scan Engine
test	Completed	11/23/2016 4:43:44 PM	11/23/2016 5:10:0...	C:\Program Files (x...	Retina

Scanned IPs [1 Total]

10.: .31.

Alerts	
NetBIOS Credentials	The selected credential has SYSTEM privileges
Machine	
Database Name	BeyondInsightReporting
Database Credentials	scan
Domain Name	

6. To generate a **Summary** or **Executive** report, select the **Report** tab. The **Report** page displays.



Select Report Type

Report Type: Executive

Report Section(s)

- ☑ Scan Summary
- ☑ Vulnerabilities By Category
- ☑ Top Vulnerabilities
- ☑ Top Open Ports
- ☑ Top Running Services
- ☑ Top Operating Systems Summary

Job Name	Status	Start Time	End Time	Data Source	Scan Engine
test	Completed	11/23/2016 4:43:44 PM	11/23/2016 5:10:0...	C:\Program Files (x...	Retina

7. Select the scan job and report type, then click **Generate**. The report displays the scan results, including remediation information.

For more information about using the scanner, please refer to the BeyondTrust Network Security Scanner User Guide.

Appendix: BeyondTrust Network Security Scanner Command Line Installation

Installation Commands

The following command line options are available to install the Network Security Scanner.

COMMAND	FUNCTION
REINSTALLMODE="amus"	Cause all files to be overwritten.
/qn	Completely silent. User interface does not display. If a reboot is required, Windows Installer automatically reboots the system at the end of installation.
/qb	Basic user interface. Only a progress dialog is displayed to the user. If a reboot is required, Windows Installer prompts the user to reboot.
INSTALLDIR=<path>	Installation folder where <path> is the path to install. Set this property to change the default installation path.
CREATEDESKTOPICON="0"	Disables creation of a desktop icon for the scanner. This option is enabled by default. Set to 0 to prevent creation of the icon.
/l*v “C:\RetinaInstallLog.txt"	Enables full logging. This should only be used for debugging if problems occur during installation.
REBOOT="ReallySuppress"	Used to suppress the automatic reboot when using the /qn silent option. The reboot still needs to occur for the software to run properly.
SERIALNUMBER=<serial>"	Sets the serial number where <serial> is the actual serial number.
CFPATH="…"	Path for common BeyondTrust files, such as Auto-Update. If another BeyondTrust product is installed, this parameter is ignored since the common path must be the same for all BeyondTrust products.