



# Retina Network Security Scanner

## Installation Guide

Revision/Update Information: October 2017

Software Version: 6.4

Revision Number: 0

#### **Corporate Headquarters**

5090 N. 40<sup>th</sup> Street  
Phoenix, AZ 85018  
Phone: 1 818-575-4000

#### **COPYRIGHT NOTICE**

Copyright © 2017 BeyondTrust Software, Inc. All rights reserved.

The information contained in this document is subject to change without notice.

No part of this document may be photocopied, reproduced or copied or translated in any manner to another language without the prior written consent of BeyondTrust Software.

BeyondTrust Software is not liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages, including lost profit or lost data, whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. BeyondTrust Software is not associated with any other vendors or products mentioned in this document.

# Contents

<b>Introduction</b> .....	<b>iv</b>
<i>Documentation Set for Retina</i> .....	<i>iv</i>
Contacting Support.....	v
<i>Telephone</i> .....	v
<i>Online</i> .....	v
<b>Overview</b> .....	<b>1</b>
<b>Installing Retina</b> .....	<b>2</b>
Requirements.....	2
Installing Retina.....	3
Running the Configuration Utility .....	4
Setting Credentials for Retina in the Management Console .....	5
Uninstalling Retina .....	5
<b>Getting Started</b> .....	<b>6</b>
Logging on to Retina.....	6
Running a Quick Scan .....	7
<b>APPENDIX A Command Line Installation</b> .....	<b>10</b>
Installation Commands .....	10

## Introduction

This guide provides the installation instructions and software requirements for Retina Network Security Scanner. For information about its features, benefits, functionality, and basic procedures, see the *Retina User Guide*.

The following sections include a list of documentation for the product, and where to get additional product information and technical assistance.

### Documentation Set for Retina

The complete Retina documentation set includes the following:

- *Retina Installation Guide*
- *Retina User Guide*
- *Retina PowerShell Integration Guide*
- *Retina Scan Management Service Guide*

## Contacting Support

For support, go to our [Customer Portal](#) then follow the link to the product you need assistance with.

The Customer Portal contains information regarding contacting Technical Support by telephone and chat, along with product downloads, product installers, license management, latest product releases, product documentation, webcasts and product demos.

### Telephone

#### Privileged Account Management Support

Within Continental United States: 800.234.9072

Outside Continental United States: 818.575.4040

#### Vulnerability Management Support

North/South America: 866.529.2201 | 949.333.1997

+ enter access code

#### All other Regions:

Standard Support: 949.333.1995

+ enter access code

Platinum Support: 949.333.1996

+ enter access code

### Online

<http://www.beyondtrust.com/Resources/Support/>

## Overview

BeyondTrust's Retina Network Security Scanner provides vulnerability testing for multiple platforms, automatic fixes of vulnerabilities and the ability to create your own audits. In addition, Retina 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.

Using Retina, you can:

- Scan in parallel using the Retina queuing system to scan up to 256 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.

Retina 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.

## Installing Retina

You can download Retina from our client portal, located at:

[www.beyondtrust.com/Resources/Support](http://www.beyondtrust.com/Resources/Support)

A username and password are required.

## Requirements

The minimum system requirements for Retina are:

<b>Operating Systems</b>	Windows 7 (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)
<b>Processor</b>	Intel Dual Core 2.0Ghz (or compatible)
<b>Memory (RAM)</b>	8 GB
<b>Hard Drive</b>	4 GB minimum
<b>Software</b>	- 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
<b>Network</b>	- Ports 443 and 21690 are required for integration with BeyondInsight - Network Interface Card (NIC) with TCP/IP enabled
<b>Minimum Screen Resolution</b>	1024x768
<b>Notes</b>	Administrative access is required to perform scans.

## Installing Retina

You can install and uninstall using the command line as detailed in [Appendix A Command Line Installation](#).

To install Retina:

1. Double-click the Retina installer. The Install Wizard is displayed.
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 Retina, enter the serial number provided when you purchased the product. You can access your serial number on the client portal by selecting **Product Licensing > Managing Your Serial Numbers**.

If you are installing a demo version of Retina, the Serial Number field remains blank.

4. Click **Continue**. The End User Software License Agreement window displays.
5. After reading the license agreement, select the check box **I accept all terms of the preceding licensing agreement**. You must accept the licensing agreement for the installation to continue.
6. Click **Continue**. The Destination Folder window displays.
7. Accept the default location or click **Browse** and select a destination folder.
8. Click **Continue**. The Additional Tasks window displays.
9. Verify the **Create Desktop Icon** check box is selected, as needed.
10. Click **Continue**. The Ready to Install Application window displays.
11. To modify the previous information, click **Back**.

To continue, click **Install**. The install process begins with a progress bar displayed.

Once Retina is installed, the Successful Installation window displays.

After the Retina installation completes, you can choose to start the Retina Configuration Utility to create a connection to the BeyondInsight management console.

12. To run the Retina Configuration Utility after the install is complete, select the **Launch Retina Configuration Utility** check box.

## Running the Configuration Utility

Using the Retina Configuration utility, you can configure

- Licensing - Enter, update or transfer your Retina Network Security Scanner license key.
- Central Policy - The Central Policy server manages event logging, auto-updating audits, and performance settings for the Retina scanner engine. Event logging sends the scan information to the management console and includes: port, services and general scan information.
- Event Management – Sets up the Event Client. The management console needs to be aware of Retina as a supported application. Retina events are sent to the management console where you can then manage and review Retina activities.
- Automatic updates – The Auto-Update synchronizes Retina 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 will be asked to run Retina Network Security Scanner when you close the Retina Configuration Utility.

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

This guide assumes all of the required management console components are successfully installed. For more information, refer to the management console installation guide.

To configure:

1. Licensing
  - a) Click **Manage License**. The License Management window displays.
    - i) If Retina Network Security Scanner is not licensed, you will be prompted to enter the serial number.
    - ii) If Retina Network Security Scanner is licensed, you will be given a choice to Transfer or Update the license.
2. Central Policy
  - a) Click **Configure Central Policy**. The Central Policy Configuration window displays.
  - b) Click the **Enable Central Policy** check box.
  - c) Enter the host name or IP address for the management console. This is the server where the management console resides.
  - d) Enter the credential that can access the server.
  - e) Click **Test Central Policy** to ensure the machine where Retina is installed can connect to the management console server.
  - f) 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.
  - g) Click **Save Settings**.
3. Event Management
  - a) Click **Configure Event Client**. The Events Client Configuration window displays.
  - b) Select the **Enabled Applications** tab (if it is not already selected).

- c) Select the **Retina** check box, and then click **OK**.
4. Automatic Updates
  - a) Click **Check for updates**. The Auto-Update window displays.
  - b) To configure Auto-Update, click **Configure**. The Configuration Properties window displays.
  - c) 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, refer to the Enterprise Update Server documentation.

- d) To download updates, click **Next**. The updates begin installing, then the Update Summary window displays.

## Setting Credentials for Retina in the Management Console

Retina 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.

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

## Uninstalling Retina

Using the Retina Uninstall wizard, you can complete the following steps to remove Retina from your system.

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

To uninstall Retina:

1. Select **Start > Settings > Control Panel**, then click **Add/Remove Programs**.
2. Select **BeyondTrust Retina**, then click **Remove**. The Add/Remove Programs dialog displays.
3. Click **Yes**.
4. To retain the license for future use on the same machine, click **No**.
5. 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.

## Getting Started

You can run a quick scan using the default values. This allows the Retina 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.

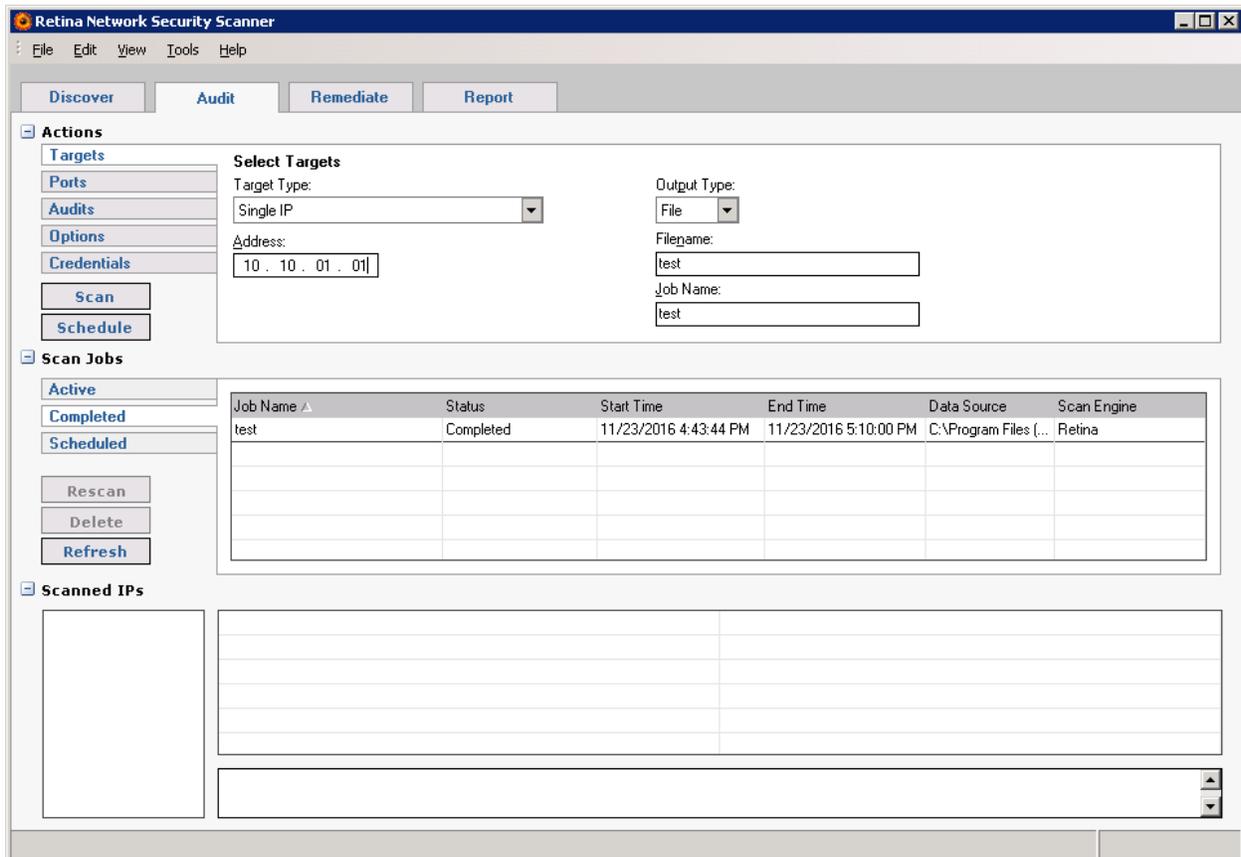
If you are not using the management console, you are ready to run scans. Otherwise, see [Adding Retina to the Management Console](#).

## Logging on to Retina

To log on to Retina:

1. Select **Start > Programs > BeyondTrust > Retina Network Security Scanner**.

The Retina home page displays.



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 fix the vulnerability.
- **Report** — provides executive overview reports and detailed summary reports of vulnerabilities and fixes.

## Running a Quick Scan

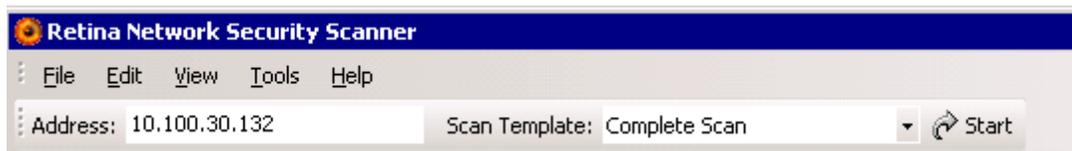
Using the Retina templates, you can quickly scan based on an IP address or sequential range of IP addresses and uses Complete Scan or FBI-SANS Top 20 template.

You can then:

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

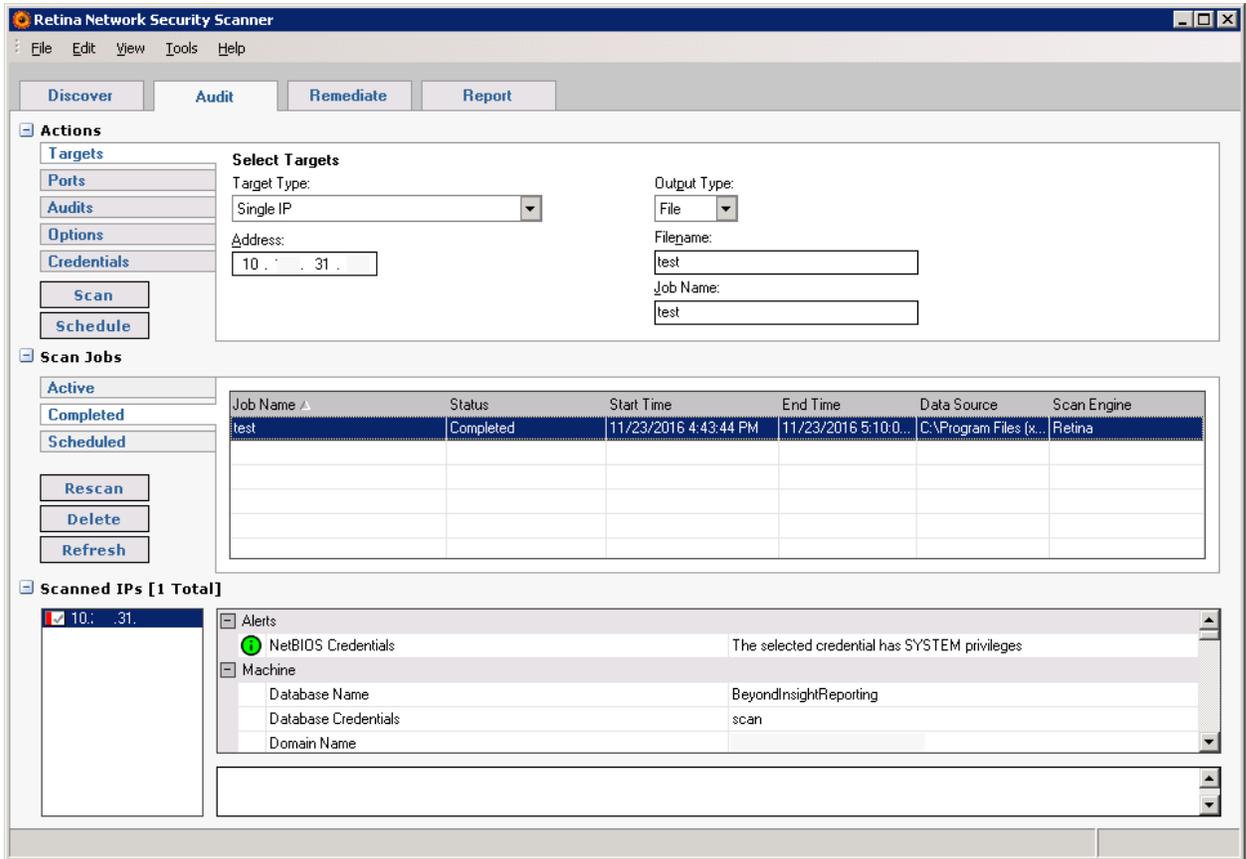
To run a quick scan:

1. On the Retina home page, select **View > Quick Scan** to display the Quick Scan toolbar. The Quick Scan toolbar displays the Address and Scan Template fields.

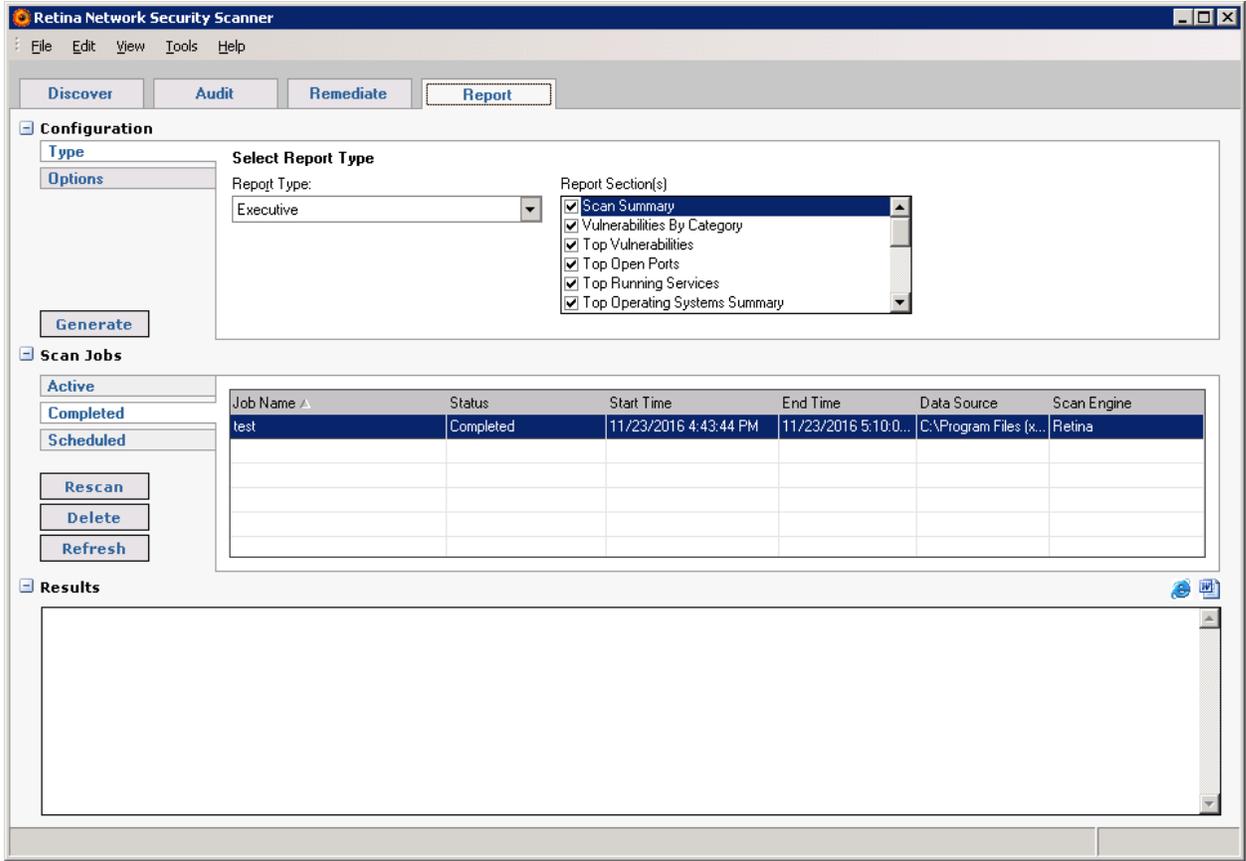


2. Verify the IP Address in the Address field.
3. In the Scan Template list box, select **Complete Scan** or **FBI-SANS Top 20**.
  - Complete Scan scans the IP address for every vulnerability audit in the Vulnerabilities database.
  - FBI-SANS Top 20 scans for the SANS list of vulnerabilities that require immediate remediation.

- Click **Start**. The scan begins.
- 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.



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



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 Retina, refer to the *Retina User's Guide*.

## APPENDIX A Command Line Installation

### Installation Commands

The following command line options are available to install Retina.

#### **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="..."**

Installation folder where ... is the path to install.

Set this property to change the default installation path.

#### **CREATEDESKTOPICON="0"**

Disables creation of a desktop icon for Retina.

This option is enabled by default. Set to 0 to prevent creation of the icon.

#### **/!v "C:\RetinalInstallLog.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="..."**

Sets the serial number where ... 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.