Contents

Introduction ........................................................................................................................................ iv
Documentation Set for Retina ........................................................................................................ iv
Contacting Support ........................................................................................................................ iv
Telephone ........................................................................................................................................ iv
Online ................................................................................................................................................ iv
CHAPTER 1 Overview ......................................................................................................................... 1
CHAPTER 2 Installing Retina .............................................................................................................. 2
Requirements .................................................................................................................................... 2
Installing Retina ............................................................................................................................... 3
Uninstalling Retina ............................................................................................................................. 5
CHAPTER 3 Getting Started ................................................................................................................ 6
Logging on to Retina ........................................................................................................................... 6
Running a Quick Scan ......................................................................................................................... 8
CHAPTER 4 Adding Retina to the Management Console ................................................................. 11
Activating Central Policy in Retina .................................................................................................... 11
Setting up Retina Events Management ............................................................................................. 13
Setting Credentials for Retina in the Management Console ............................................................. 14
APPENDIX A Command Line Installation ....................................................................................... 15
Installation Commands .................................................................................................................... 15
**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*

**Contacting Support**

For support, go to our [Customer Portal](http://www.beyondtrust.com/Resources/Support/) 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, account, 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:

+ enter access code  
Platinum Support: 949.333.1996  
+ enter access code

**Online**

CHAPTER 1 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.
CHAPTER 2  Installing Retina

You can download Retina from our client portal, located at:
www.beyondtrust.com/Resources/Support

A username and password are required.

Requirements

The minimum system requirements for Retina are:

**Operating Systems**  
Windows Vista SP2 or later (32-bit and 64-bit)  
Windows 7 SP1 or later (32-bit and 64-bit)  
Windows 8 (32-bit and 64-bit)  
Windows 8.1 (32-bit and 64-bit)  
Windows Server 2003 SP2 or later (32-bit and 64-bit)  
Windows Server 2008 SP2 or later (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)

**Software**  
MSXML 6.0 SP1  
Microsoft .Net Framework 2.0 (included with installer)  
Microsoft .Net Framework 4.0 or later

**Network**  
TCP/IP – Required for communicating with the BeyondInsight console, License Validation, and scanning remote machines

**Processor**  
Intel Pentium IV 1.4 Ghz (or compatible)

**Memory (RAM)**  
4 GB

**Hard Drive**  
1 GB minimum
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.

12. To launch Retina after the install is complete, select the Launch Retina check box.

13. Click Finish. The Auto-Update window displays.
    The Auto-Update synchronizes Retina with the most up-to-date vulnerabilities database. These updates will continue to occur at the beginning of each session. This allows you to proactively secure your network against the latest vulnerabilities.

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

16  Click **Finish**. Retina launches, if selected.

Where do I go from here?

- I am using the management console.
  You must configure communication between Retina and the management console. See [Adding Retina to the Management Console](#).

- I am not using the management console.
  You are ready to run a scan! See [Getting Started](#).
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.
CHAPTER 3  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:

   The Retina home page displays.
The following tabs are available:

- **Quick Scan** — performs a scan based on an IP address or sequential range of IP addresses and uses Complete Scan or FBI-SANS Top 20 template.
- **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.

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, verify the Quick Scan toolbar displays.
   If not, select View, then Quick Scan. 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.
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.

6 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*. 
CHAPTER 4 Adding Retina to the Management Console

To manage Retina scans using the management console, you must configure:

- From Retina, event logging and Central Policy settings.
- From the Events Client Configuration tool, activate Retina as a supported application in the management console.

This chapter provides information on configuring the communication between Retina and the management console.

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

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 feature.

Activating Central Policy in Retina

The Central Policy server updates Retina with the latest version of audits. The Central Policy server also 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.

There are two versions of Central Policy:

- Version 1. Communicates to the management console using port 10001.
- Version 2. Communicates to the management console using https port 443.

You must turn on Central Policy in Retina.
To turn on Central Policy in Retina:

1. Log on to Retina.
2. Select **Tools > Options**.
3. Select the **Management** tab.

**Note:** If these options are not available, then your version of Retina might not support connections to the management console. Contact your BeyondTrust representative for more information.
4 Select the **Enable Central Policy** check box.

5 Select a Central Policy type.

6 Enter the name of the Central Policy server. This is the server where the management console resides.

7 Provide the credentials for the server.

8 Enter the agent name. This is the name of the server where the Retina scanner is deployed.

9 Click **OK**.

### Setting up Retina Events Management

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.

**Note:** When you initially install the management console, you configure the following client settings using the Events Client configuration wizard: host and port information, workgroup settings, certificate selection, and agent applications (for example, Retina).

For information on using the wizard, refer to the management console documentation. You can also configure client settings after you run the wizard. See the following procedure.
To configure Retina using the Events Client Configuration tool:

1. Start the Events Client Configuration tool.
   The default location is **Start > All Programs > BeyondTrust > Tools**.
2. Select the **Enabled Applications** tab (if it is not already selected).
3. Select the **Retina** check box.
4. Click **OK**.

**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.
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.

**/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=“...”
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.