DOCUMENTATION

Retina Network Security Scanner

User Guide

Revision/Update Information: January 2017
Software Version: Retina Network Security Scanner 6.1
Revision Number: 0

CORPORATE HEADQUARTERS
5090 N. 40th Street
Phoenix, AZ 85018
Phone: 1 818-575-4000

Contents

Introduction

This guide shows system administrators and security administrators how to configure and use BeyondTrust Retina Network Security Scanner (RNSS). This guide provides an overview of how Retina works and instructions for Retina configuration and use.

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

Additional Information

For more information, see the documentation list and support information listed in the following sections.

Documentation Set for RNSS

Documentation Set for Retina Network Security Scanner

The complete Retina Network Security Scanner documentation set includes the following:

- *Retina Network Security Scanner Installation Guide*
- *Retina Network Security Scanner User Guide*
- *Retina Network Security Scanner* Help

Overview

Retina Network Security Scanner provides vulnerability testing for multiple platforms, assessment 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 perform 30 unique audits of one machine.
- 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.

Architectural Overview

Retina's primary components are:

- **Retina Engine Windows Service —** retinaengine.exe provides the scanner and is comprised of:
  - Scanner — performs the discovery and auditing. It reads and writes data to the Queue Manager and writes data to the Named Pipe. Externally it reads from and writes to the RTD (Scan Results Database) files and writes the Scanner log.
  - Queue Manager — controls the scanning order. It communicates through queue files with the Scanner and reads data from and writes data to the RPC Interface. In addition, it retrieves jobs from the Scheduler.
  - Scheduler — tracks and queues scheduled jobs. It reads data from and writes data to the RPC Interface, writes data to the Named Pipe and calls the Product Updater directly at scheduled times.
  - Remote Procedure Call (RPC) Interface — provides the main control and communication from the service to the other executables and data stores. It is the main control and communication interface from the service to other executables, and data stores. The RPC interface receives data and control information internally from the Queue Manager and Scheduler and externally from the RPC Client. In addition, it writes and forwards data instructions to the Queue Manager, Scheduler and Named Pipe.
  - Named Pipe — provides the primary data interface for external functions. It receives response data from the Engine and forwards data to the RTD, RPC Client and Retina User Interface or command line.
- **Retina User Interface —** The retina.exe provides the local access to the functions of the engine. The UI manages Discover and Audit scans and scheduling and options by communicating with the engine using the RPC client. It reads data from and writes data to the RTD and writes to the UI and Message logs.
- **Application Bus —** Provides the data channel for information and control sequences to and from the engine. It reads and forwards data from the RTD to the Events Client.
- **Product Updater —** Communicates with the BeyondTrust servers to ensure the application and audit data files are current.

Scanning Process

During the scanning process, you enter the job information using the Retina interface. The interface writes the job information to a job file and a scan request. The scan request is passed to the scanner or Retina Engine Service.

Note: The following details on how a scan works is provided for information only. Do not change the Retina database tables.

The scanner receives the job file and begins the audit process. An audit scan consists of:

- **Targeting –** builds a scan list from the address group and Discovery options. Retina ascertains if the target is a device as well as the applications or services on the device.
- **Port Scanning –** determines the open, closed or filtered ports on each device.
- **Detecting Operating System –** performs registry checks, NetBIOS, ICMP fingerprinting or TCP fingerprinting to determine the target's operating system.
- **Auditing –** runs an audit of each port with the specified protocols. This is to access the vulnerabilities associated with the service on that port.

Initially Retina retrieves the list of IPs to be scanned and builds and writes its target list to the eeye_groups table. The job list contains the job start and stop information. Retina then begins running the scan.

As targets are scanned, the host completed entries are removed from the queue file. If the host is powered down for any reason, this ensures that a scan will complete.

At the conclusion of the scan, the scanner writes Completed to the eeye_groups table in the scan results database (RTD). If the user aborts the job, the scanner writes Aborted to that table.

Typical Bandwidth Usage

The following table provides scan results in a test environment.

Tested using RNSS 5.18.1.

Note: Results will vary based on target OS, applications installed, selected scan settings, and role (server, workstations).

	Null Session	**Authenticated**	**Discovery (PowerBroker for Windows)**
Audits	All Audits, Common Ports, Defaults	All Audits, Common Ports, Defaults, Local Scan Service	No Audits, All Enumerate
Traffic to Target	120 Kb	27.5 MB	3.4 MB
Event Traffic to Centralized Console	15 Kb	165 Kb	88 Kb
Time To Complete	9 minutes	14 minutes	1.5 minutes
Results	High:0 Medium:0 Low:0 Information:12	High:135 Medium:38 Low:47 Information:52	NA
Operating System	Windows XP, SP3		
Hardware	i7, 3GHz, 512MB RAM Virtual Machine		
Notes	Firewall Enabled	Remote Access Permitted	Remote Access Permitted

Managing Credentials

When you run a scan, you can select a stored credential. Using credentials with administrative rights for a scan provides more complete scan results.

In Retina, you can:

- Create a stored credential
- Create a credential group
- Add credentials to the group

Creating a Stored Credential

You can create a stored credential and select the credential when running the scan. You can also add the credential to a credential group.

You can create the following credential types:

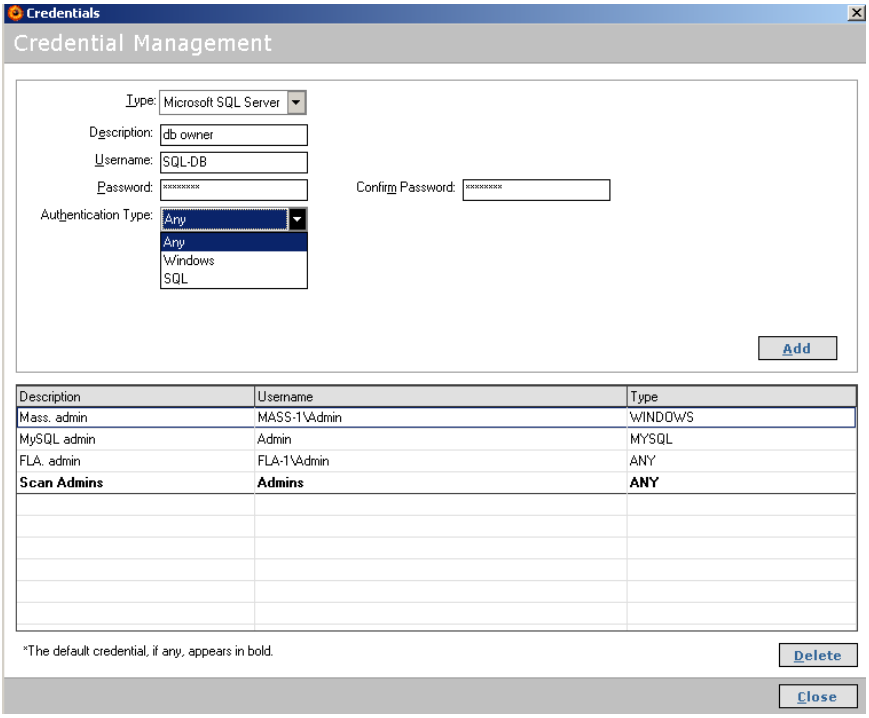
- SSH. See Creating an SSH Credential.
- Windows
- MySQL
- Microsoft SQL Server
- Oracle. See Creating Oracle Credentials.
- SNMP. See Creating SNMP Credentials.

A credential type is only used against scan targets that match the credential criteria.

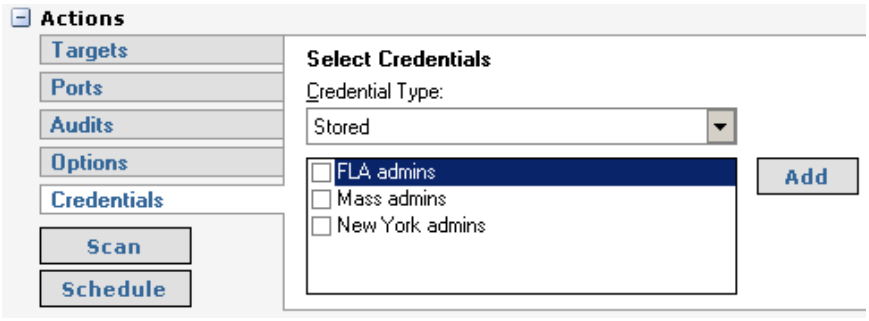
Use the following procedure to create Any, Windows, MySQL, and SQL Server credentials.

To create a stored credential:

1. Select **Tools > Credential Management**.
2. Select a credential type from the list.
3. On the Credentials Management dialog box, enter the user account information: username, password, description. The Default Credential check box is only available for type Any.
4. If you are creating Microsoft SQL Server credentials, select the authentication type.



5. Click **Add**.
6. Continue to add credentials as needed.
7. After you add stored credentials, you can select a credential when configuring a scan:



8. Click **Close**.
9. Default credentials are always used in a scan and are not displayed in the list.

Creating an SSH Credential

You can create Public Key Encryption credentials to connect to SSH-configured targets. You can select a credential that contains a public/private key pair used for SSH connections.

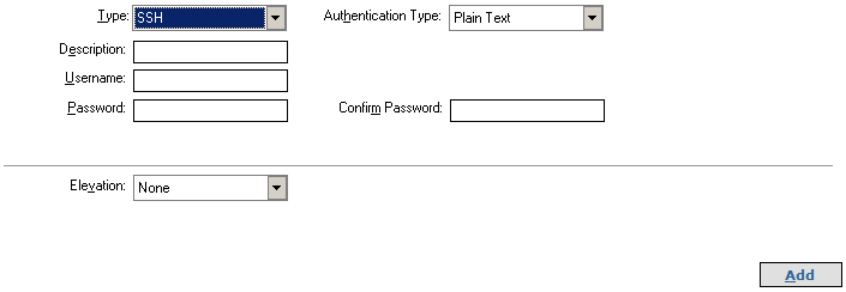
DSA and RSA key formats are supported.

Optionally, when configuring SSH, you can use sudo. Using sudo, you can access scan targets that are not configured to allow root accounts to log on remotely. You can log on as a normal user and sudo to a more privileged account. Additionally, you can use sudo to elevate the same account to get more permissions.

If you are using PowerBroker UNIX/Linux, you can elevate privileges using pbrun.

To create an SSH credential:

1. Select **Tools > Credential Management**.
2. From the Type list, select **SSH**.



3. Provide a description and user name.
4. Select an authentication type from the list: Plain Text or Public Key.
   - **Plain Text** - Enter a password.
   - **Public Key** - Enter the private key file name and passphrase. Click Browse to navigate to the file. A public key is generated based on the contents of the private key.
5. To elevate credentials, select one of the following:
   Using elevated credentials is optional.
   - sudo - Enter the sudo username and password. You can use the username provided in the Username box and leave the Sudo username blank.
   - pbrun - Enter the pbrun username.
   - Enable - Enter the credentials for Cisco devices. If you are auditing Cisco devices, you can elevate the credentials to privileged for more thorough scans.
6. Click **Add**.

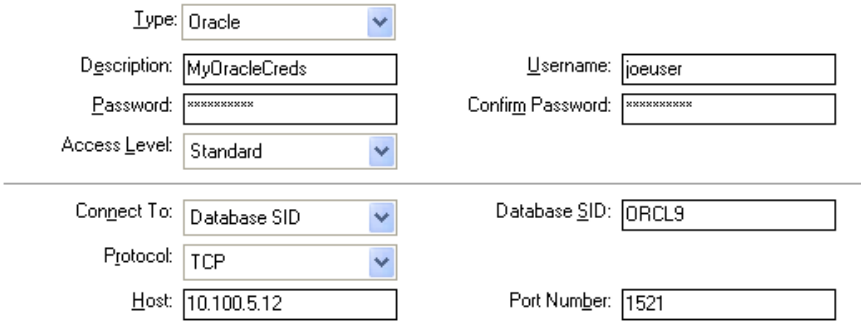
Creating Oracle Credentials

If you are scanning Oracle databases, you can create Oracle credentials.

The tsanames.ora file is updated automatically after you create an Oracle credential.

To create Oracle credentials:

1. Select **Tools > Credential Management**.
2. From the Type list, select **Oracle**.
3. Provide a user name, description, and password.
4. Select an access level from the list: Standard, SYSDBA, or SYSOPER.
5. Select additional connection options:
   - **Connect To** - Select from: Database SID, Named Service.
   - **Protocol** - Select a protocol: TCP, TCPS, NMP.
   - **Host** - Enter the host name where the Oracle database resides.
   - **Database SID** - Enter the database SID.
   - **Port Number** - Enter a port number.
6. Review your settings.



7. Click **Save**.

Creating SNMP Credentials

If you are scanning devices that are managed using an SNMP community, you can add your community strings here.

To add an SNMP community string:

1. Select **Tools > Credential Management**.
2. From the Type list, select **SNMP**.
3. Enter a description and the community string.
4. Click **Add**.

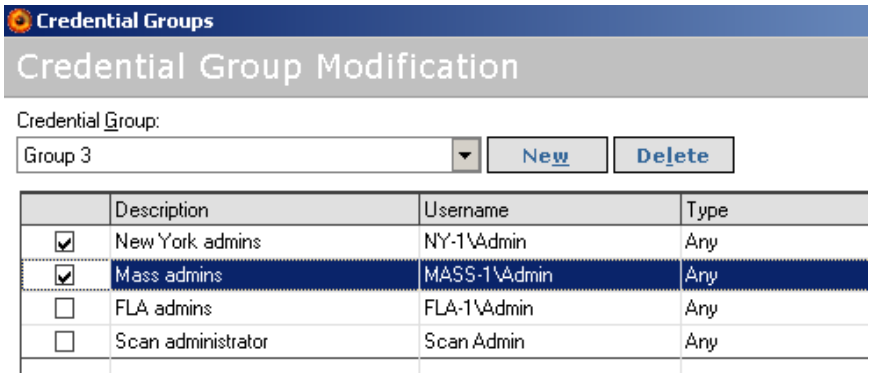
Creating a Credential Group

Before you can create a credential group, you must first create stored credentials.

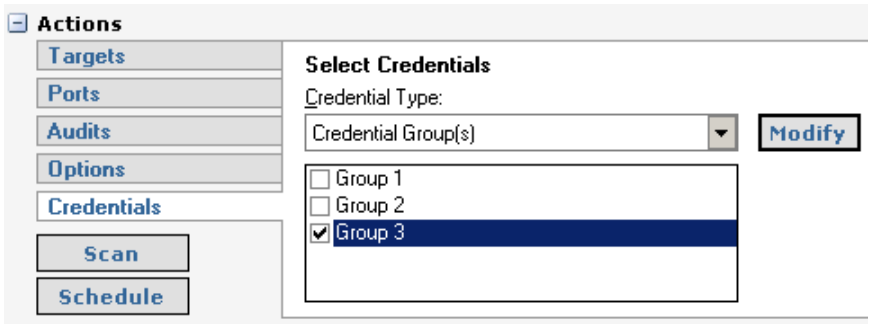
Note that credential groups cannot be used for XCCDF scans.

To create a credential group:

1. Select **Tools > Credential Groups**.
2. Click **New**.
3. Enter a group name and click **OK**.
   If there is more than one group name in the list, ensure the correct group is selected.
4. Select the check boxes for the stored credentials that you want to add to the group.



5. Click **Close**.
   After you add a credential group, you can select the group when configuring a scan:



Defining Address Groups

To ensure repeatable scans Retina uses address groups to sort assets by IP address, IP range, CIDR notation or named host.

You can create, modify and delete address groups, attach IP addresses, omit specific IP addresses and select credentials.

Note: If you are migrating from Retina 4 to Retina 5, you can import your address group data by clicking Import and selecting your .rti files.

To access address groups:

1. On the main toolbar, select **Tools** > **Address Groups**. The Address Group Modification window is displayed.

Using the Always Address Group

You can create an address group and name it *Always*. Retina is designed to recognize this address group name and includes the group in every scan (regardless if the group is selected in the scan job).

You can populate the Always address group with IP addresses that you want to scan and those that you want to ignore. The Always address group is recommended for IP addresses that you never want to include in a scan (select the Omit check box when creating the address group to ignore IP addresses).

For more information, see Creating Address Groups.

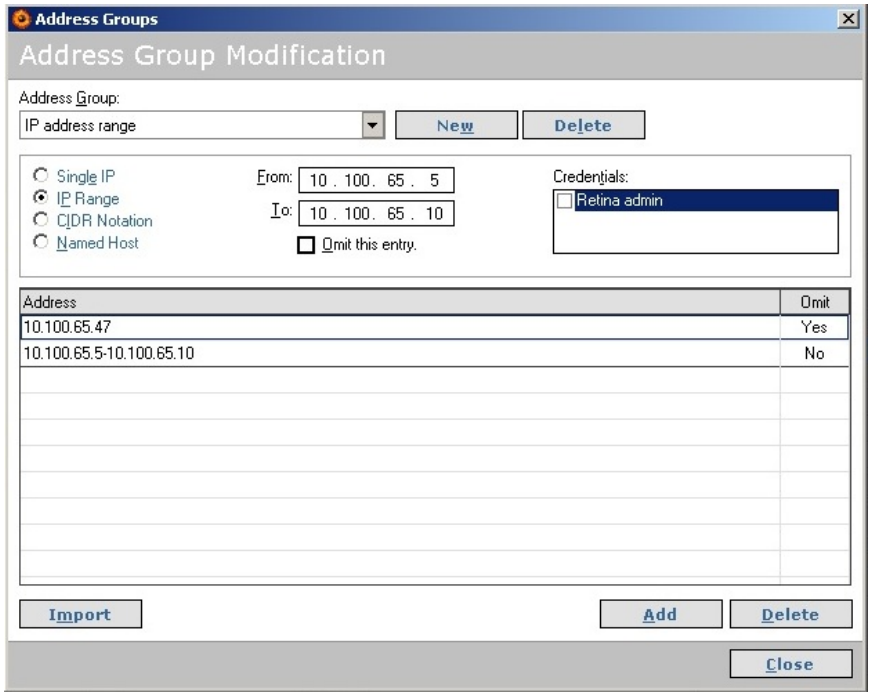
Creating Address Groups

Create an address group that includes particular IP addresses that you want in an audit. You can also include IP addresses in an address group that you want to ignore during the scan.

After you create an address group, you can select the address group as your target type when you are setting up an audit scan. See Configuring Audit Scans.

To create an address group:

1. On the Address Group window, click **New**.
2. Enter the name, then click **OK**. The Address Group Modification window displays the new name in the Address Group list.
3. Add IP addresses to an address group by selecting the address group, then entering the target type as:
   - **IP Address** - Scans using a single IP address.
   - **IP Range** - Scans using a range of IP addresses.
   - **CIDR Notation** - Scans using a Classless Inter-Domain Route or Supernet.
   - **Named Host** - Scans using the DNS or NetBIOS.
4. If you store credentials in Retina, you can select credentials for the address group in the **Credentials** list box.
5. To disable a specific target type, select the **Omit This Entry** check box. The IP address will be skipped, but remain in the database.
6. Click **Add**. The target types are added to the address group.



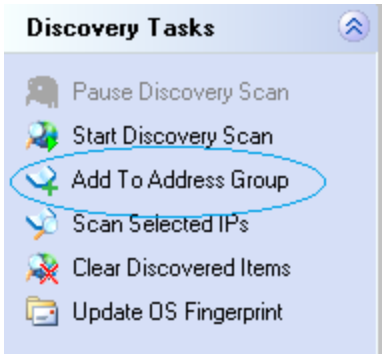
7. To save the address group, click **Close**.

Adding Audits to Address Groups

After a discovery scan runs, you can add IP addresses that are discovered to an address group.

To add IP addresses to address groups:

1. After the discovery scan runs, select one or more IP addresses in the Results pane.
2. Click **Add to Address Group** in the Discovery Tasks list. Alternatively, right-click the IP addresses and select **Add to Address Group**.



3. On the Add to Address Group dialog box, select one of the following:
   - **Append to Existing Address Group** - Select an address group from the list.
   - **Create New Address Group** - Enter an address group name to create a group.

For more information, see Defining Address Groups.

Running Audit Scans

Retina can scan any device with an IP address if the route between Retina and the IP address can be established. Retina can be used to scan internally within a DMZ or from outside inward.

You can scan VMWare ThinApp images.

For more information about how a scan works, see Scanning Process.

Configuring Audit Scans

You can define your scan parameters, then create a group to ensure scanning the same targets at a later date. You can schedule audit scans to track the vulnerability assessments.

Note: You can create an address group called Always that is included in all scans. For more information, see Using the Always Address Group.

You can run a scan without administrative rights on each target asset; however, administrative rights ensure more complete scan results.

Selecting Targets and Output Types

To select the target and output types:

1. On the Retina home page, select the **Audit** tab. The Audit page displays Actions, Scan Jobs and Scanned IPs.
2. In the Actions area, click **Targets**. The Target pane displays.
3. From the Target Type list, select the target type:
   - **IP Address** - Scans using an individual IP address. The default displays the scanner's IP address.
   - **IP Range** - Scans using a range of IP addresses. The default displays the network and subnet address from your workstation.
   - **CIDR Notation** - Scans using a Classless Inter-Domain Route or Supernet. Each IP address has a network prefix that identifies a gateway.
     The length of the network prefix is also specified and varies depending on the number of bits that are needed rather than any arbitrary class assignment structure.
   - **Named Host** - Scans using the domain name system (DNS) or NetBIOS.
   - **Address Group** - The group contains any combination of IP addresses, IP address ranges, subnets or other groups.
   - **Advanced** - Scans using any combination of nonconsecutive IP addresses, IP ranges, CIDR notation, named hosts or address groups. The addresses are separated by a single space.
4. Enter a file name and job name.

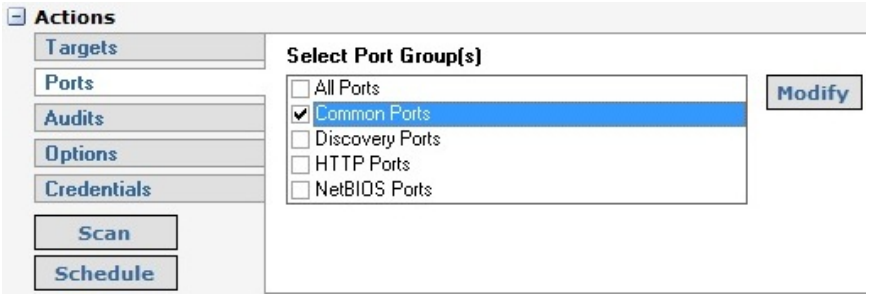
Selecting Ports

There are preconfigured port groups available. You can add or remove ports from a port group.

You can create a port group and add ports. See Managing Ports.

To select a port group:

1. On the Ports pane, select a port group. You can select more than one port group.



Selecting Audits

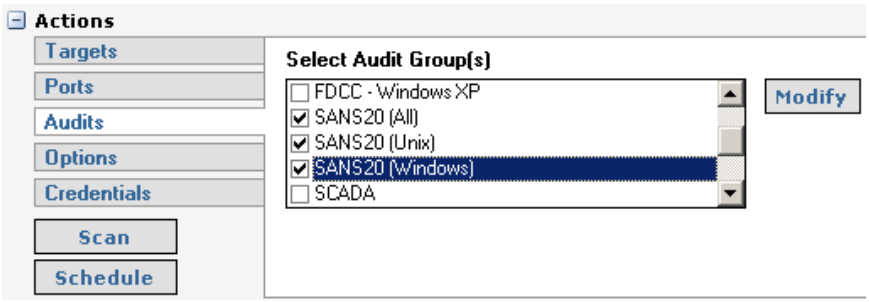
When you select audit group scan settings, you can:

- Select one or more audit groups to include in the scan
- Change the audits in an audit group as you configure the scan settings.

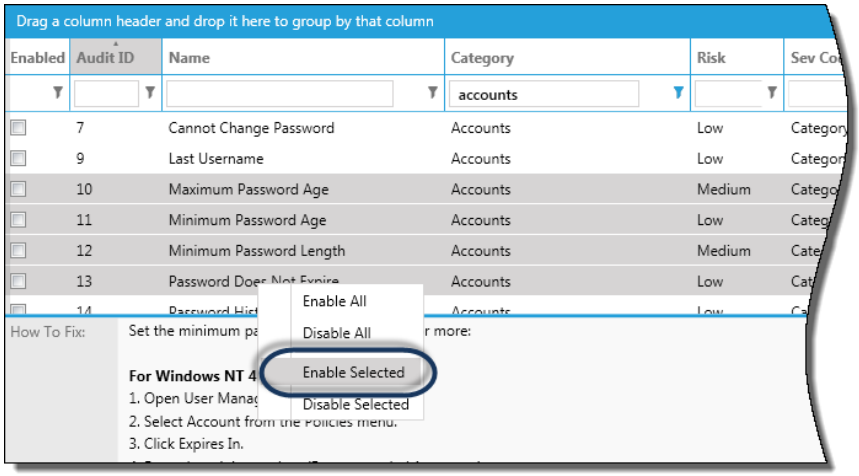
To search the audit database, see Searching the Audit Database.

To select the audits for the scan:

1. Select the **Audit** tab, then select **Audits**.
2. Scroll through the list and select audit groups.



3. To change the audit groups, click **Modify**. The Audit Group Modification window is displayed.
4. To create an audit group, click **New**, then type the group name and click **OK**. The audit group name is displayed.
5. To add audits to the group:
   a. Select the **Automatically enable new audits in this group** check box to automatically add all audits received when you update your database with the latest audits.
   b. Select an audit group then select the check boxes for the audits that you want to add to the group.
   c. Right-click an audit and select **Enable All**; all audits in the audit group are selected.
   d. Shift+select audits to select more than one audit. Right-click and select **Enable Selected**.



6. To change an existing audit group, select or clear audit check boxes.
7. To save changes, click **Close**.

To restore the default settings for an audit group, click **Reset**. Click **Yes** on the confirmation dialog box. The default audits for the currently selected audit group are reset.

Selecting Audit Options

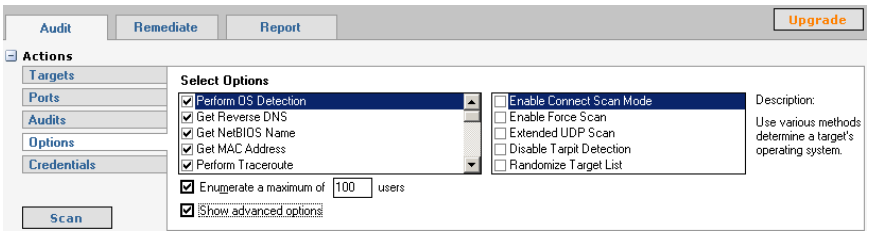
To select audit options:

1. Select the **Audit** tab.
2. Select **Options**.
3. Select scan options from the following list:
   - **Perform OS Detection** - Determines the operating system of the target.
   - **Get Reverse DNS** - Scans for reverse Domain Name System (rDNS) and retrieves the domain name for the target's IP address.
   - **Get NetBIOS Name** - Determines the Network Basic Input/Output System.
   - **Get MAC Address** - Retrieves the Media Access Control address or unique hardware number.
     In addition, Retina can use the MAC address to detect if a target is running in a virtualized environment.
   - **Perform Traceroute** - Determines the paths that packets travel to the target.
   - **Enumerate [parameter] Using NetBIOS** - Uses the NetBIOS protocol to determine and list audits specified in the Audit Group.
     The parameters include registry, users, shares, files, hotfixes, named pipes, machine information, audit policy, per-user registry settings, groups, processes, user and group privileges and hardware.
   - **Enumerate Users** - Find and enumerate users on the target assets.
   - **Enumerate Shares** - Using NetBIOS, finds and enumerates shared folders and resources on the target asset.
   - **Enumerate Groups** - Lists groups on target asset, includes SID, group scope, and group type information.
   - **Enumerate Processes** - Lists the processes running on the target asset.
   - **Enumerate Services** - Lists the services running on the target asset.

- **Enumerate Hardware** - Lists the hardware on the remote host using WMI.
- **Enumerate Software** - Using NetBIOS, determine the software installed on the target asset.
- **Enumerate Certificates** - Lists the certificates installed on the target asset.
- **Enumerate Databases** - Lists database instances, table and user information on a target. Includes SQL Server, Oracle, and MySQL databases.

  Note: The data is sent to BeyondInsight management console only.
- **Enumerate Scheduled Tasks** - Displays information about the scheduled tasks on that particular asset, including task name, task to run, last time the task ran, schedule type, etc. Applies to Windows assets only. BeyondInsight is required for this option.
- **Perform IP Protocol Scanning** - Lists open and filtered IP protocols.
- **Enumerate Ports via Local Scan Service** - Installs the local Retina agent and enumerates local ports using netstat. OFF by default.
  The Perform Local Scanning check box from the Advanced options must also be selected.
- **Enable Remote Registry Service** - Starts (and then stops) the remote registry on a target. Requires the local scan service (agent). OFF by default.
  The Perform Local Scanning check box from the Advanced options must also be selected.
- **Enable WMI Service** - Starts (and then stops) the WMI service. Requires the local scan service. OFF by default.
  The Perform Local Scanning check box from the Advanced options must also be selected.
- **Enumerate File Contents via Local Scan Service** - Detects personally identifiable information on remote Windows targets. Information includes financial information and personal information.
- **Randomize Port List** - Shuffles the port list so that ports are scanned in random order instead of sequentially.
- **Enumerate Wireless Access Points** - Detects access points. All access points detected are reported regardless of beacon status. This can help to identify rogue devices.
  Depending on the device, the following information is displayed: SSID, authentication method (for example, WEP, WPA), configuration data (for example, manufacturer, login).
- **Perform Database Application Scanning** - Scans remote database instances.

4. Select the **Enumerate a maximum of** check box and enter the maximum number of users to be audited. The maximum number is per target and applies to each of the user types that exist for that target. For example, a *nix target running Samba could have *nix users, domain users, and Samba users. If you set the number to 50, then a maximum of 50 *nix users, 50 domain users, and 50 Samba users could be returned for that target in the scan results.
5. To display the Advanced Options, select the **Show advanced options** check box.



Note: There are performance issues when running a connect scan, force scan and UDP scan simultaneously. The combination of the three instructs Retina to negotiate a full connection to each port on each device. On a Class B network, you could be waiting for 65,535 devices to time-out on a minimum of 65,535 connections each.

6. Optionally, select the following advanced scan types:
   - **Enable Connect Scan Mode** - Run if other methods, such as a slow dial-up, are unreliable. The operating system is negotiating a full connection to each device. Because multiple port scanning methods are not used, Retina cannot determine a number of items, such as operating system.
   - **Enable Force Scan** - Run if the targeted devices are not going to answer SYN or ICMP scanning. Forces Retina to run protocol discovery on each port of each device to determine the protocol. This should only be used in a highly locked down network where the standard port scanning methods will be filtered or blocked. Force Scan should not be used in IP ranges.
     Note: Using Force Scan assumes the selected target is live. Each selected target counts against your license count.
   - **Extended UDP Scan** - Runs a complete scan on all User Datagram Protocol without timing out. Forces Retina to expect an answer. The IP will eventually timeout.

     An extended UDP scan can take longer when the Windows target has Windows Firewall turned on. Turn off Windows Firewall for the duration of the scan.
   - **Disable Tarpit Detection** - Stops tarpit detection. A TCP tarpit program intentionally reduces the size of data packets to slow communication transmissions. This can cause incorrect scan results.
     To scan systems running tarpits, set the tarpit to allow unimpeded connections from the Retina scanner.
   - **Randomize Target List** - Shuffles IP addresses so that targets are scanned in random order instead of sequentially by IP address.
   - **Perform Local Scanning** - Uses the local scan agent to assist with the scan. This check box must be selected when selecting the Enumerate Ports via Local Scan Service, Enable Remote Registry Service, and Enable WMI Services check boxes.
   - **Disable OS Backport Detection** - Runs all remote audits on all targets including operating systems where there might be backported banners. By default, Retina will skip some remote audits when a backported banner is detected to avoid a false positive on that target.
   - **Enable Smart Credentials** - When there is more than one credential selected for a scan, the Retina scanner determines the best credential to use for each target. For example, a target asset might have SQL Server installed. For that particular target you would want the SQL Server credential used. In this case, using Smart Credentials ensures the SQL Server credential is used (if set in the scan settings. See Setting Credentials). Enable Smart Credentials is turned on by default.

Setting Credentials

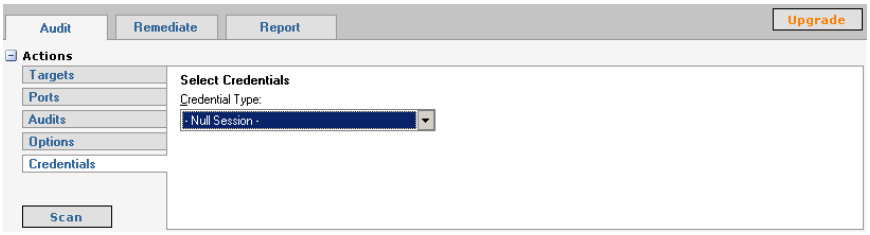
Credentials are used to secure access to the target assets, such as networks, workstations, servers, and printers. You can run a scan without administrative rights on each target asset; however, administrative rights ensure more complete scan results.

To run a fully credentialed scan of a UNIX device, you must enable SSH access using the root or admin username.

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

To specify credentials:

1. Select the **Audit** tab, then select **Credentials**.



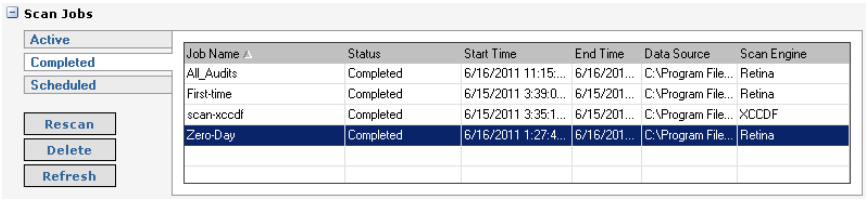
2. Select the credentials to use for this scan:
   - Null Session - Requires no credentials.
   - Stored - Provides a selection list of stored credentials.
     To create a stored credential, click **Add**. For more information, see Creating Stored Credentials.
   - Single-use - Allows a single session for one user based on user name and password.
   - Credential Group - Select a group from the list.
     For information about credential groups, see Creating a Credential Group.

Running Scans

You can scan the target immediately.

The Scan Jobs section displays active, completed, and scheduled scans.

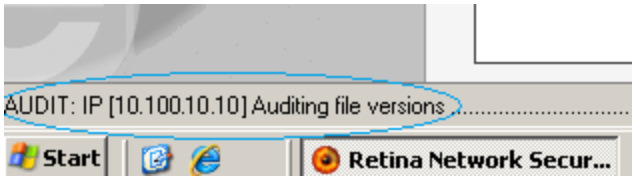
You can rescan, delete, and refresh the list of scans.



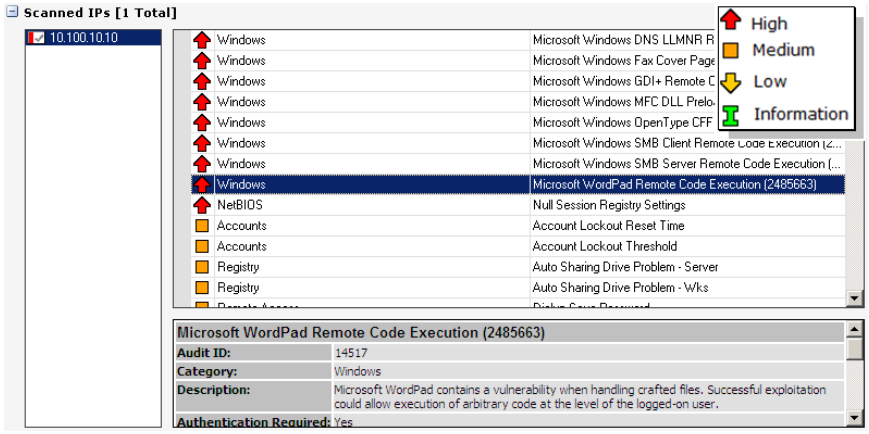
Scanning Immediately

To scan the targets now:

1. Select the **Audit** tab.
2. Click **Scan**.
3. You are prompted to enter a scan name and credentials. Enter the scan name or credentials (both are optional).
   The audit begins. You can view the scan progress details in the Status bar, including: IP address scanned, type of scan, and update messages.



4. After the scan runs, select a vulnerability in the Scanned IP section to view more details such as description and fix information. Use the legend as a quick aid to interpret vulnerability severity level.



You can fix the vulnerabilities using the remediation process. See Remediating Vulnerabilities.

1. Select the **Audit** tab, then click **Schedule**. The Scan Job Scheduler window displays.
2. Enter a job name.
3. Select the start time and date.

> The scan duration is calculated from the scheduled start time, not the time the job actually begins.
>
> For example, if this job is delayed because the machine was restarting, other jobs running or service was stopped, this job will still complete based on whether the job started within the time duration. If the delays exceed the specified time duration, the job will not run.

4. Select the frequency:
   - Once - Schedules jobs to run one time. From the Start list, select the time and date.
   - Daily - Schedules jobs for weekdays only, every x number of days or by the start date. From the Start list, select the time and date, then select Every Day, Weekdays or Every x days and specify the number of days.
   - Weekly - Schedules jobs every x number of weeks or by the start date. From the Start list, select the time and date, then select the number of weeks and the day of the week.
   - Monthly - Schedules jobs every nth weekday of the month or by the start date. From the Start list, select the time and date. Select either the day of the month by day number or the day of the week and the week, then select the months.
     For example, you can schedule a job for the 26th day of August and September or the Second Thursday in April and June.
5. Click **OK**. The scan runs as scheduled.
6. To limit the scan to a specific length of time, select the **Abort the scan if it runs longer than** check box. Enter the number of minutes the job can run after the scheduled start time.

7. Select the **Enable job specific scan restrictions** check box to set a scan restriction.
8. Click the squares to set the restricted time frame, and then click **OK**.
9. If a scan is running when the scan restriction time starts, you can abort or pause the running scan. Select **Aborted** or **Paused**.
10. Click **OK**.

Remediating Vulnerabilities

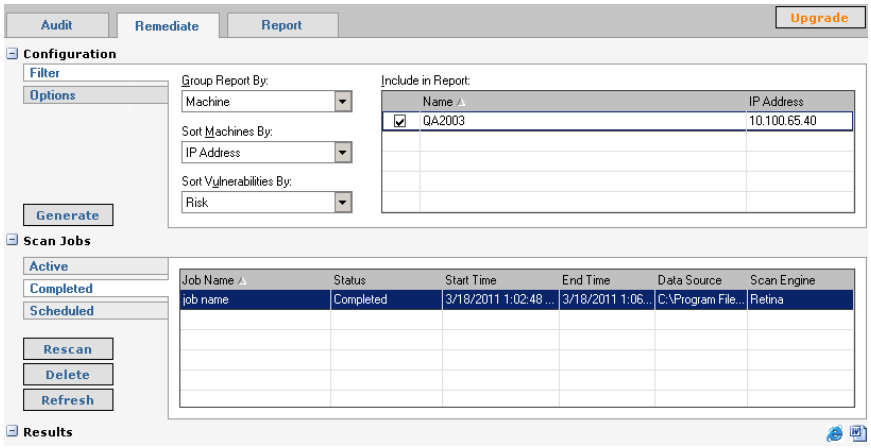
You can access the jobs scanned in the Audit tab and generate a Remediation Report that lists the vulnerability information and recommends methods to fix the vulnerability as well as the Risk Level, Severity Code, PCI Severity Level.

Generating Remediation Reports

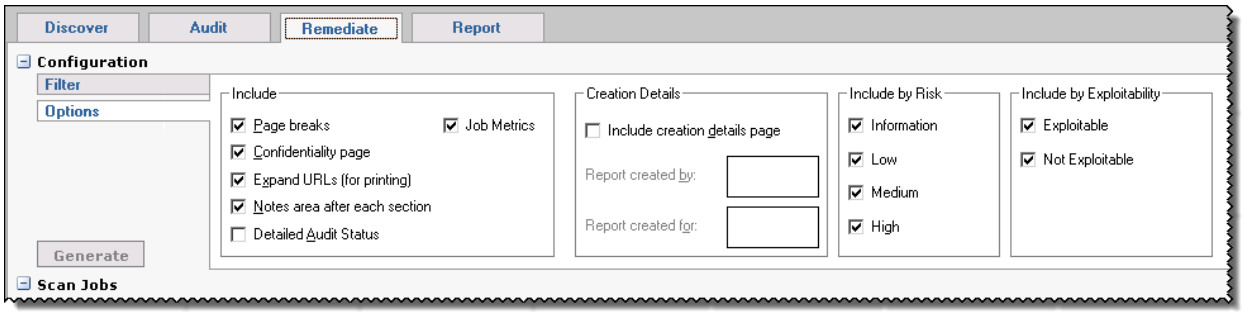
Note: On systems with a low monitor resolution (1024x768), you might need to disable the Explorer Bar to see all of the remediation report options. From the View menu you can turn off the Explorer Bar.

To create a remediation report:

1. Click the **Remediate** tab, and select the job name in the Scan Jobs area. The Remediate pane displays the Include in Report section.
   The data to include in the Remediation report changes based on the filter.

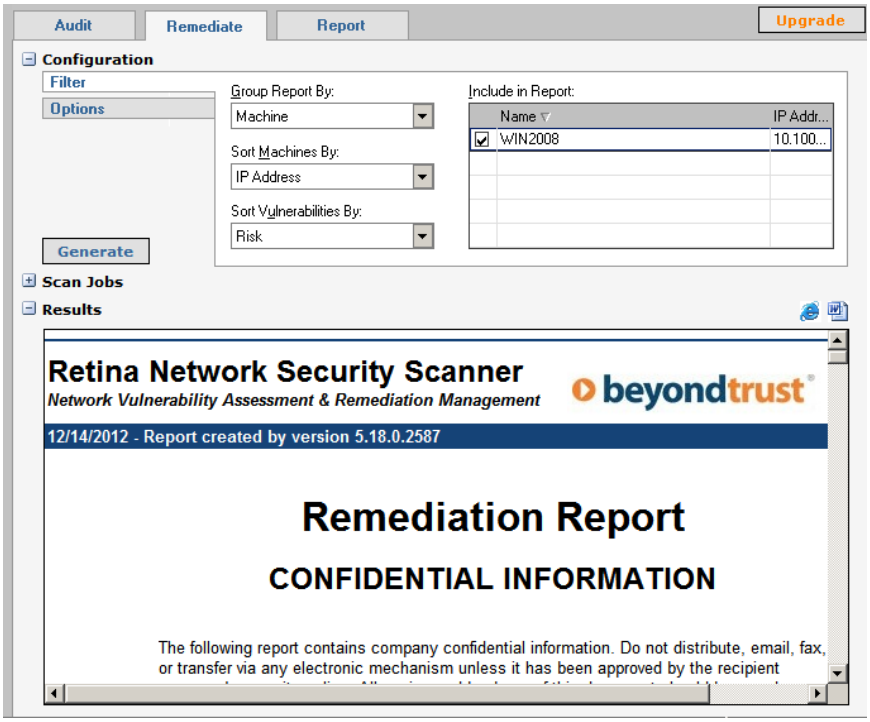


2. Select filtering options:
   - Group Report By list - Vulnerability, Machine, CVE
   - Sort Machines By list - IP Address, Name
   - Sort Vulnerabilities By list - Risk, Name
3. Select the specific vulnerabilities or machines.
4. Select the **Options** tab. The Options pane displays the section headings and creation details.

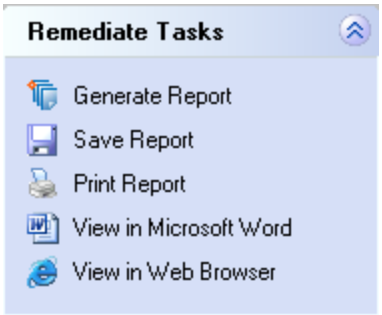


5. In the Include box, select the headings to include in the report:
   - Page Breaks - Displays the information into standard 8-1/2 x 11” pages.
   - Job Metrics - Provides a summary of the scan.
   - Confidentiality Page - Adds the following text to the cover page:
     The following report contains company confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.
   - Expand URLs - Provides links and website address in the Related Links section.
   - Notes area - Provides blank space for adding notes.
   - Detailed Audit Status - Displays the detailed audit status.
6. In the Creation Details section, select the **Include Creation Details Page** check box to include a created by page.
   In the Report Created By and Report Create For text box, enter the names or other text information.
7. In the Include by Risk section, select the type of vulnerabilities to include:
   - **Information** - Details host information that does not necessarily represent a security threat, but can be useful to the administrator to assess the security.
   - **Low** - Defines risks associated with specific or unlikely circumstances.
   - **Medium** - Describes serious security threats that would allow a trusted but non-privileged user to gain access to sensitive information.
   - **High** - Indicates vulnerabilities that severely impact the overall safety and usability of the network.

8. In the Include by Exploitability section, select the check boxes.
   Note: You must select at least one option from the Exploitability section to run the remediation report.
   - **Exploitable** - Includes a flag in the report that the vulnerability can be exploited.
   - **Not Exploitable** - Includes a flag in the report that the vulnerability can not be exploited.
9. Click **Generate**. The Remediate report displays in the Results pane.



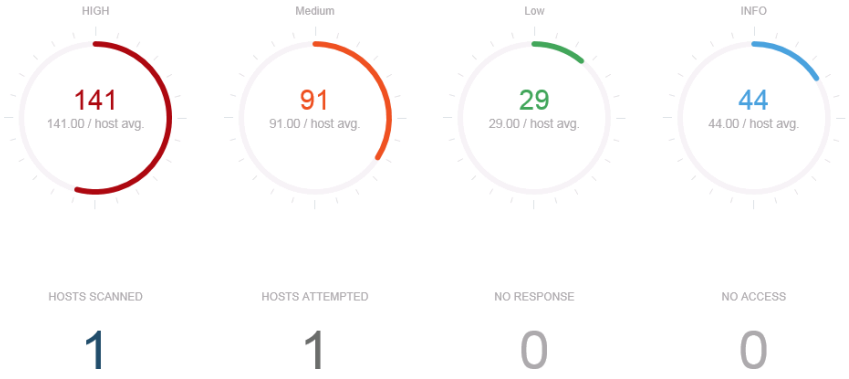
10. On the Remediate Tasks pane, select viewing and printing options:



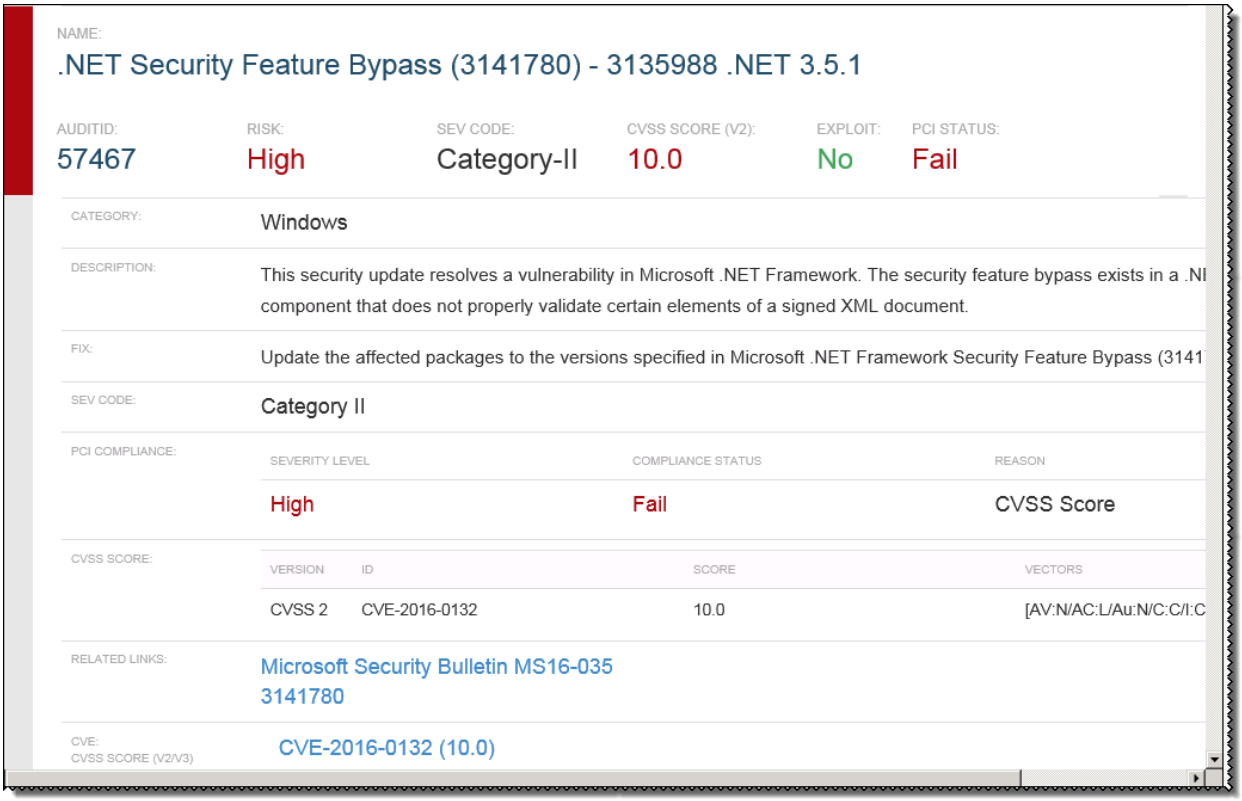
Reviewing Remediation Reports

The Remediation Report lists the vulnerability information and recommends methods to fix the vulnerability as well as the Risk Level, Severity Code, PCI Severity Level and CVSS Score.

View high level summary information:



View more detailed information that can help you determine how to remediate the vulnerability:



Using CVSS Scores

Retina uses the Common Vulnerability Scoring System (CVSS) to provide the CVSS score and a vector that describes the components from which the score was calculated. The CVSS vectors always include the base metric and may contain temporal metrics.

An example of how the CVSS Score displays is:

CVSS Score: 9.3 [AV:N/AC:M/Au:N/C:c/I:C/A:C]

In the HTML format, the 9.3 is a hyperlink that displays the CVSS Version 2 Scoring Page where you can refine the CVSS base score.

Generating Reports

You can generate the following reports:

- Executive report provides an overview of your network and graphs of vulnerabilities.
- Summary report provides a more detailed overview of vulnerabilities and fixes.
- Vulnerability Export report summarizes vulnerabilities for reporting purposes.
- Access report lists assets that are inaccessible.
- PCI compliance report displays security requirements for merchants and service providers that manage cardholder data.
- Dashboard report provides a high-level overview of a scan.
- Alert report displays any alerts detected on the asset.
- Consolidated Remediation report displays only the current applicable audits.

Running Executive Reports

The Executive Report provides an overview of the vulnerabilities discovered on your network. You can sort the data by scan summary, vulnerabilities by audit categories and vulnerabilities discovered on ports, running services, operating systems, user accounts and network shares.

To generate an Executive report:

1. Select the **Report** tab.
2. From the Report Type list, select **Executive**.
3. Select the report category check boxes that you want in the report:
   - **Scan Summary** - Provides a recap listing the scanner name, version, start time and date, duration, name and status. In addition, you can view the number of machines scanned, total number of vulnerabilities and high, medium, low and information vulnerabilities and credentials.
     The vulnerabilities by host and number, percentage and average of vulnerabilities by risk display in graphs.
   - **Vulnerabilities by Categories** - Provides an overview of vulnerabilities by audit categories. The data is also provided in a graph.
   - **Top/Bottom Vulnerabilities** - Displays the highest or lowest number of vulnerabilities, sorted by audit categories. The data is also provided in a graph.
   - **Top/Bottom Open Ports** - Displays vulnerabilities, sorted by audit categories, affecting the highest or lowest number of open ports.
   - **Top/Bottom Running Services** - Displays vulnerabilities, sorted by audit categories, affecting the highest or lowest number of services.
   - **Top/Bottom Operating Systems Summary** - Displays vulnerabilities, sorted by audit categories, affecting the highest or lowest number of operating systems.
   - **Top/Bottom User Accounts** - Displays vulnerabilities, sorted by audit categories, affecting the highest or lowest number of user accounts.

- **Top/Bottom Network Shares** - Displays vulnerabilities, sorted by audit categories, affecting the highest or lowest number of user accounts.
- **Glossary** - Displays a list of terms.

4. In the Creation Details section, select the **Include Creation Details Page** check box to include a created by page.
5. Enter the report details that you want to include in the report.
6. Click **Generate**. The Executive report is displayed in the Results pane.
7. Use the Report Tasks pane to do the following:
   - **Save Report** - Saves as a text or html file.
   - **Print Report** - Prints to default printers.
   - **View in Microsoft Word** - Opens report in Word.
   - **View in Web Browser** - Opens report in default web browser.

Running Summary Reports

Summary reports provide a detailed overview of vulnerabilities and recommends methods to fix the vulnerability and the Risk Level, Severity Code, PCI Severity Level and CVSS Score. You can define the details, such as ports, services, shares and users, and output type as screen, HTML or text.

To generate a summary report:

1. Select the **Report** tab.
2. From the Report Type list, select **Summary**.
3. From the Output Type list, select **Screen**, **HTML**, or **Text**.
4. In the Include in Report list box, select the job names.
5. Select **Options**. The Options pane is displayed.
6. In the Include box, select the headings to include in the report:
   - **General** - Provides summary of the scan information, such as IP address, report date, ping response, time to live and operating system.
   - **Audits Vulnerable** - Lists the discovered vulnerabilities by Audit ID, Risk Level, CVSS, BugTraq and CVE.
   - **Certificates** - Displays information about the certificates on the target.
   - **Job Metrics** - Provides a summary of the scan.
   - **Ports** - Lists the TCP and UDP ports.
   - **Services** - Lists the network services for the IP address. Common network services include authentication servers, directory services, email and printing.
   - **Shares** - Lists all locations on a network that allow multiple users to have a centralized space.
   - **Users** - Lists all the users discovered on the target system.
   - **Software** - Lists all software programs discovered on the target system.
7. Click **Generate**.
8. Use the Report Tasks pane to do the following:
   - **Save Report** - Saves as a text or html file.
   - **Print Report** - Prints to default printers.

- **View in Microsoft Word** - Opens report in Word.
- **View in Web Browser** - Opens report in default web browser.

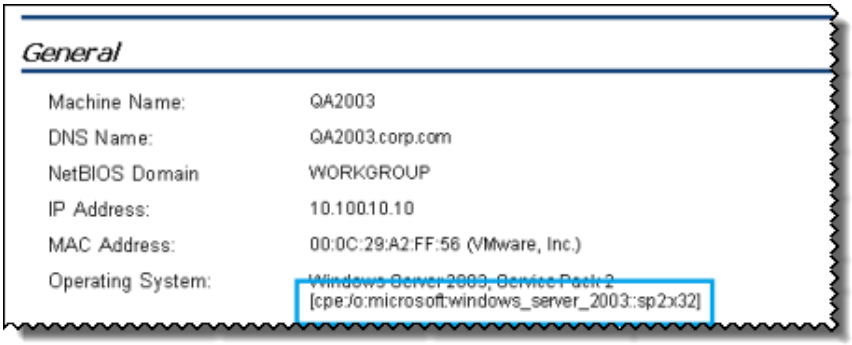
Running Vulnerability Export Reports

Vulnerability export reports provide an overview of audits and hosts. You can define the details, such as ports, services, shares and users, and output type as screen, HTML or text.

To generate a report:

1. Select the **Report** tab.
2. From the Type list, select **Vulnerability Export**.
3. From the Output Type list, select **Screen**, **HTML**, **XML** or **CSV**. Screen displays in a separate window. HTML, XML, and CSV prompt you to save the file.
4. Select **Options**.
5. Select the check boxes for the information that you want to include in the report.
6. To include a summary of the scan, select the **Job Metrics** check box.
7. Click **Generate**.
8. Use the Report Tasks pane to do the following:
   - **Save Report** - Saves as a text or html file.
   - **Print Report** - Prints to default printers.
   - **View in Microsoft Word** - Opens report in Word.
   - **View in Web Browser** - Opens report in default web browser.

If you select the CPE check box, the operating system is displayed as a CPE reference in the General section of the report output. CPE can also be viewed on the Summary report.



Running Access Reports

An Access report lists machines that are flagged with no ssh access or no remote registry audits. You can view the report on screen or in an HTML format.

To generate a report:

1. Select the **Report** tab.
2. From the Report Type list, select **Access Report**.
3. From the Output Type list, select **Screen** or **HTML**. Screen displays in a separate window. HTML prompts you to save the file.

4. From the Sort Field list, select to sort the report by: **IP**, **NetBIOS**, **DNS Name**, **MAC**, **Access Info** or **Scan Info**.
5. Select **Options**. The Options pane is displayed.
6. To include a summary of the scan, select the **Job Metrics** check box.
7. Click **Generate**.
8. Use the Report Tasks pane to do the following:
   - **Save Report** - Saves as a text or html file.
   - **Print Report** - Prints to default printers.
   - **View in Microsoft Word** - Opens report in Word.
   - **View in Web Browser** - Opens report in default web browser.

Running a Dashboard Report

A dashboard report provides a high-level overview of the scan, including: overall score, scan summary details, scan engine information, target response summary, and vulnerability overview.

SCAP Scanning

You can run scans based on the Extensible Configuration Checklist Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL) specifications.

The steps to running SCAP scans are:

- Copy SCAP Content (Optional)
- Run the SCAP Scan Wizard
- View the scan results
- Export the scan results

Copying SCAP Content (Optional)

Because Retina includes more than 150 SCAP benchmarks covering various operating systems, databases and applications, it is unlikely that you will need to manually add SCAP content. If, however, you want to scan with a benchmark that is not included with Retina, copy its SCAP Data Stream Content (such as FDCC checklists) to the Retina benchmarks directory.

For new installations of Retina 6.0 or later, the usual location is:

C:\Program Files (x86)\BeyondTrust\Retina\Database\XCCDF\Benchmarks

For systems on which a Retina version prior to 6.0 is installed, the typical location is:

C:\Program Files (x86)\BeyondTrust\Retina 5\Database\XCCDF\Benchmarks

Note that on 32-bit Windows systems, the top-level directory will be the ”C:\Program Files” directory, rather than the “C:\Program Files (x86)” directory shown above. Note also that the directory portion preceding “Database” (“C:\Program Files (x86)\BeyondTrust\Retina”) is referenced by “%Retina%” in the paragraphs below.

When copying SCAP content, include all items associated with the SCAP content, including XCCDF, OVAL and supporting XML files.

Running SCAP Scans

Note that credential groups cannot be used for SCAP scans.

Using the Local Scan Service

By default, SCAP scanning will deploy the Retina Local Scan Service dissolvable engine on the scan target to improve the accuracy of scan results. For some combinations of benchmark and target operating system, not using the Local Scan Service can lead to error findings for Password Policy and Audit Policy checks, so we highly recommend keeping the Local Scan Service enabled. Note that the Local Scan Service is only present on the target during an assessment and is removed on completion. Moreover, it is only deployed when using benchmarks, including those for most Windows operating systems, for which it is known to improve scan results.

Configuring a SCAP Scan

Go through the SCAP Job Wizard to select the scan job settings.

Note: Avoid scanning duplicate IP addresses until the previous scan running on those IPs are completed. This reduces load and network traffic on those machines.

To run a SCAP scan:

1. On the Retina home page, select **Tools** > **SCAP Job Wizard**. The SCAP Job Wizard displays.
2. Click **Next**. The Target Selection window displays.
3. Select the target assets. The Address field changes based on your selection.
   - **Single IP** - Scans using a single IP address.
   - **IP Range** - Scans using a range of IP addresses.
   - **CIDR Notation** - Scans using a Classless Inter-Domain Route or Supernet. Each IP address has a network prefix that identifies a gateway.
     The length of the network prefix is also specified and varies depending on the number of bits that are needed rather than any arbitrary class assignment structure.
   - **Named Host** - Scans using the DNS or NetBIOS.
   - **Address Groups** - Select one or more address groups that contain any combination of computer IP addresses, IP address ranges, subnets or other groups.
   - **Advanced** - Typically, this is used to scan individual targets in an IP range or CIDR block, but this field can also include names, ranges and CIDRs. Address entries should be separated with a space. For example, “10.102.25.10 curly.corp.int-eeye.com 10.202.6.0/24”.
   - **Single IP (IPv6)** - Enter a single IPv6 address. This capability was introduced in Retina 6.1.0.
4. Click **Next**. The Credential Selection page displays.
5. Select the credentials, and then click **Next**.
   The best results are obtained using credentials that have Administrator rights on the target machine..
   - **Null Session** - Requires no credentials.
   - **Stored** - Provides a selection list of stored credentials.
     To create a stored credential, click **Add**. For more information, see Creating Stored Credentials.
   - **Single-use** - Allows a single session for one user based on user name and password.

     Note that it is possible to select multiple credentials, in which case the SCAP Scan Engine will attempt to use the most appropriate credential for each target.
6. Select XCCDF benchmark(s), and then click **Next**.
   The XCCDF Benchmark Selection page displays the XCCDF files from the %Retina 5%\Database\XCCDF\Benchmarks folder. If no benchmarks are displayed, ensure that the XCCDF files are in this directory. Note that it is possible to select multiple benchmarks, in which case the SCAP Engine will evaluate all applicable combinations of benchmark and scan target specified in this job.
7. Select profile(s), and then click **Next**.
   For each selected benchmark, the wizard will display a corresponding Profile Selection page. These pages will be displayed consecutively.
8. On the Details Selection page, type a name for the scan job and then select the following settings:
   - **Create output files when target platform does not match benchmark platform** - Turn this setting off so that output files will not be created if the target platform does not match the benchmark platform.

- **Perform Local Scanning** - Local scanning uses a dissolvable agent that is deployed on the target for the duration of the scan. This applies primarily to Windows operating system scans and secondarily to scans of Red Hat 5 and 6 targets using older STIG benchmarks.
- **Enable Remote Registry Service** - Turn on the Windows Remote Registry service. If the dissolvable agent starts the Remote Registry service, then it will stop it after completing the scan.

9. Click **Next**.
10. Schedule the scan to run immediately once or specify a frequency, time and date.
11. Click **Next**. The Success window displays. The scan will run as scheduled.
12. Click **Finish**.
13. To verify the job is running, select the **Audit** tab.
    In the Scan Jobs section, select **Active**, **Completed** or **Scheduled** to track the job progress.

Saving Scan Results as PDF

You can save the scan results as a PDF file. The PDF includes all results in the scan.

To save the scan results to a PDF file:

1. Select the **Audit** tab, and then select the **Completed** tab.
2. Select a completed SCAP scan.
3. Select **File > Save Report As**.
4. Type a name for the report, and then click **Save**.

Viewing SCAP Scan Results

To view a report of the scan results:

1. Select the **Audit** tab.
2. Select a scan from the Completed list.
3. Select an IP address from the Scanned IPs list.
   Note that if the scan used multiple benchmarks, then “IP addresses” will be displayed with the benchmark name (with spaces removed) concatenated to the IP address. For example, “127.0.0.1-CIS_Microsoft_ Windows_8.1_Benchmark”.

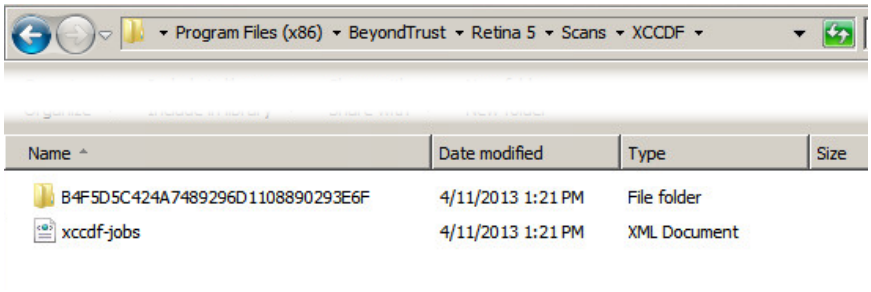
Converting SCAP Output to ARF Format

You can use the command line interface (CLI) to convert SCAP output to the Assessment Results Format (ARF).

The supported output schemas are: ARF 0.41 Micro, ARF 0.41 Full, and ARF 1.1 NIST (Beta).

The CLI parameters are:

- ARF type: MicroARF, FullARF, NISTARF
- SCAP scan instance ID (obtained from Windows explorer as shown below)



From the command line, run the following:

C:\Program Files (x86)\BeyondTrust\Retina 5\Tools> BenchmarkReports <Report Type> <SCAP scan instance ID>

```
c:\Program Files (x86)\BeyondTrust\Retina 5\Tools>BenchmarkReports MicroARF B4F5
D5C424A7489296D1108890293E6F
```

When run from the Tools directory shown above, the report is saved in the following directory:

C:\Program Files (x86)\BeyondTrust\Retina 5\Reports\Temp\XCCDF

Setting Retina Options

You can configure general parameters such as logging, auto update, and timeout values.

To access options:

1. On the toolbar, select **Tools** > **Options**. The Options and Settings window displays.
   You can set the following options:
   - **General** - set appearance, logging and auto updating parameters.
   - **Scanner** - modify the scan engine performance and set ping and data timeout values.

Note that if you click Reset then all tab values are reset.

Generating Log Files

Retina generates log files, including:

- RetinaStatus.log
- RetinaUI.log

The log files are saved to %Retina 5%\Logs.

Logging is turned on by default.

To turn off logging:

1. Select **Tools > Options**.
2. Select the **General** tab.
3. In the Logging section, clear the **Generate a log file of Retina operations** check box.
4. Click **OK**.

Automatically Check for Updates

Scheduling updates ensures you proactively secure your network against the latest vulnerabilities.

To automatically check for updates:

1. Select **Tools > Options**.
2. Select the **General** tab.
3. Select when to check for updates:
   - **Check for updates according to a Schedule** - Select a start time and frequency.
   - **Check for updates when launching Retina** - Set the number of seconds to wait before starting the updater.
4. Click **OK**.

Scanning Multiple Targets Simultaneously

You can specify the number of targets to scan simultaneously and the scan speed. The maximum number of targets is 256. The maximum scan speed is 5.

The number of targets can affect server performance and scan quality. The result is an unresponsive or slow server or poor scan quality, such as known services not being found or known open ports not being identified.

To alleviate this, you can reduce the number of targets, adjust the scan speed downward or override the TCP connection limit which causes Retina to scan much faster.

However, if you override the TCP connection limit, the TCP incomplete connections limits are removed for all applications during the scan.

To scan multiple targets:

1. Select **Tools > Options**.
2. Select the **Scanner** tab.
   - **Scan** - Set the number of targets to scan simultaneously. The maximum is 128 targets.
   - **Adaptive Scan Speed** - Set the delay between bursts of packets sent during a SYN scan.
     1 = longest delay
     5 = almost no delay
   - **Enable TCP connection limit override** - Select the check box limit TCP connection overrides.
     Note: The TCP Connection Limit Override is available on Windows XP SP2 and later and Windows 2003 SP1 only. This selection is not available for Windows NT or Windows 2000.
3. Click **OK**.

Setting Timeout Values

Configuring ping and data timeout values allows Retina to compensate for network latency.

If pings are not returning in time for Retina to detect them, increase the ping timeout value.

If Retina is not receiving complete data from devices or hosts when services are under heavy load, increase the data timeout value.

To set timeout values:

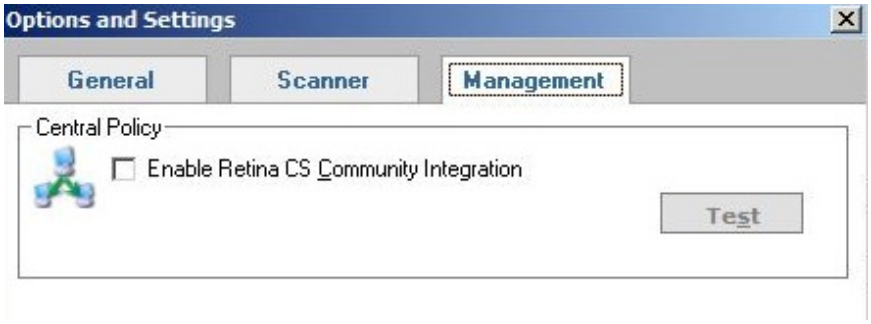
1. On the **Options** page, select the **Scanner** tab.
2. Enter timeout values for ping and data operations. The default is 3 seconds.
3. Click **OK**.

Integrating Retina CS Community

If you install Retina CS Community, you must turn on Central Policy in Retina Community to establish a connection between the applications.

To turn on Central Policy:

1. Select **Tools > Options**.
2. Select the **Management** tab.



3. Select the check box, and then click **OK**.

Click the **Test** button to ensure there is a connection between Retina Community and Retina CS Community.

Configuring Email Notification for Events

You can configure email notifications to alert users when particular events occur. You can select the events that will trigger the email alert.

Setting Alerts

Email alerts can be delivered to selected users when certain events occur, such as Job Start, Job Stop, and High Risk Audit. Alerts can be triggered by actions occurring, such as Event Logs, SMTP, SMMP and SysLog.

To set alerts:

1. Select **Tools** > **Alerting**. The Alerting window displays.
2. Click the **Events** tab, and then select the check boxes for the events that trigger an alert.
3. Click the **Actions** tab. Select the actions that you want to occur in response to the event.
4. Expand **Event Log**. You can enable event logs and system logs for the selected events. The logs are sent to the email address set in the SMTP section.
   a. Select **True** from the Enabled field.
   b. In the Host field, enter the domain name or IP address.
5. Expand **SMTP**. You can specify the mail server.
   a. To activate alerts, select **True** in the Alert Enabled field.
   b. To activate reports, select **True** in the Reports Enabled field.
   c. In the **Relay** field, enter the SMTP server.
   d. In the **Sender** field, enter the From field for the email message.
   e. In the **Recipient** field, enter the To field for the email message.
6. Expand **SNMP**.
   a. Select **True** from the Enabled list.
   b. Enter the host and community.
7. Expand **SYSLOG**.
   a. Select **True** from the Enabled list.
   b. Enter the host. Syslog alerts use UDP port 514. To use an another port, add ":port number" to the end of the Syslog IP address.
   c. Select the priority and facility.
8. Click **OK**.

Exploiting Vulnerabilities

In Retina, you can view vulnerabilities that can be exploited. For any vulnerability with a CVE-ID, exploit information associated with the CVE-ID is also displayed. In some cases, exploits are displayed that are not associated with a CVE-ID.

You can view exploit information where you view vulnerability details (for example, on the Audit Groups dialog box, Scan Results pane, and report results).

Click the Yes link in the Exploit Database column to visit the Exploit Database web site and learn more about the exploit.

Exploits

CVE-ID	Exploit Database	Core Impact	CANVAS	Metasploit
CVE-2003-0309	No	No	No	No
CVE-2003-0344	Yes	No	No	Yes

The Microsoft Exploitability Index is also included in the Exploits information. The index values correspond to the values that are provided in security bulletins issued from Microsoft. For more information on interpreting the index values, refer to Microsoft documentation.

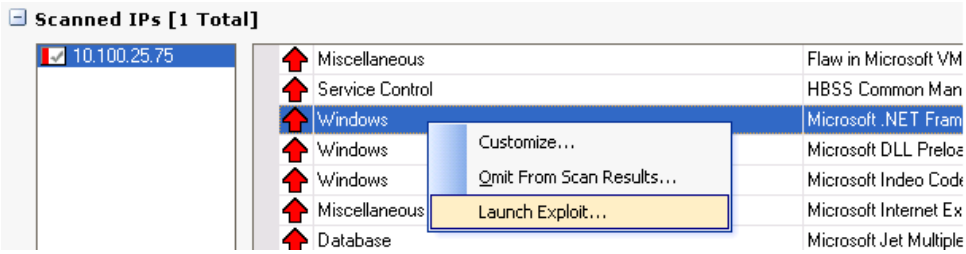
CVE-ID	Exploit Database	Core Impact	CANVAS	Metasploit	Microsoft Exploitability Index
CVE-2010-0249	Yes	Yes	No	Yes	1 - Consistent exploit code likely

Exploiting a Vulnerability

Integrating Metasploit with Retina, you can exploit a vulnerability found during a scan. API calls can be sent to remote and local Metasploit installations. Metasploit can also be called using the command line when installed locally.

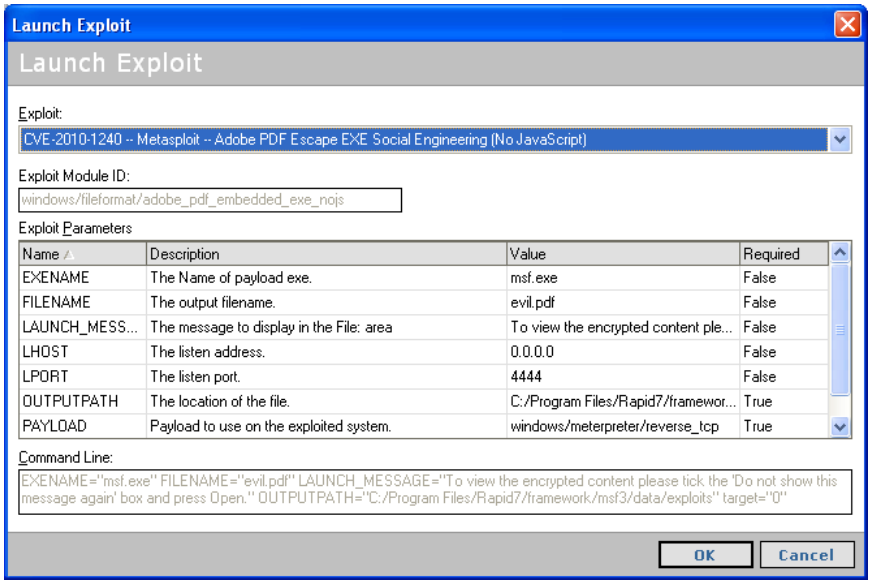
To exploit a vulnerability:

1. On the Scan results pane, right-click a vulnerability and select **Launch Exploit**.



2. On the Launch Exploit dialog box, change the parameters as required.
   The default value for Payload is windows/meterpreter/reverse_tcp.

   For more information about the parameters that you can customize, refer to the Metasploit product documentation.



3. Click **OK**.

Integrating with Metasploit

You can integrate Metasploit with Retina. This saves time when loading exploits.

To integrate Metasploit with Retina:

1. Select **Tools > Exploit Framework Integration**.
2. Select an integration method:
   - **MessagePackbased API** - Enter a user name, password, and the server URL for Metasploit.
   - **XML-RPC** - Enter a user name, password, and the server URL for Metasploit.
     Note: Metasploit no longer supports the XML-RPC API. As of Metasploit v. 4.0.0, using the MessagePack-based API is recommended.
   - **Command Line** - Click Browse to navigate to the directory where Metasploit is installed.
3. Click **OK**.

Database and XML Schema

This appendix provides information about the Retina database and XML schema.

Retina RTD Schema

Table 1. eeye_Activity

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier for each scanned IP address.
GroupID	String [32]	Unique ID assigned per scan. Used to group multiple ID_ fields. The ID is a generated GUID used by each table as the Activity_ ID.
DTS	SmallDateTime	Date and time stamp indicating the scan start.
dtsScanEnd	SmallDateTime	Date and time stamp indicating the scan completion.
RunStat	String [255]	Status of last scan. Indicates success, aborted or empty for unknown reason.
ActivityModule	String [255]	Scanner that is currently the activity module in Retina. Extensions will be added as modules are added to Retina.
IP	String [255]	IP address of target being scanned.
RequesterIP	String [255]	Reserved for future use
RequesterMac	String [255]	Reserved for future use

Table 2. eeye_Alerts

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier for each scanned IP address.
ActivityID	String [32]	Link to eeye_activity:ID_
Path1	String [255]	Subsystem, e.g., “Remote Agent”
Path2	String [255]	Blank or internal classification, such as “Error”
Path3	String [255]	Not Used
DisplayField	String [255]	Data label, such as “SSH Credentials”
ValueField	String [255]	Optional further explanation of DisplayField
Risk	Integer	Not Used

Table 3. eeye_AuditExtend

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier
ActivityID	String [32]	Link to eeye_Activity:ID_
Audit_ID	String [32]	Link to eeye_Audit:ID_
Rthnum	Long Integer	Audit ID as referenced in audits.xml.
PosNeg	Long Integer	0: Target NOT vulnerable 1: Target vulnerable
context	String [255]	Context of the instance of the audit (share name, user name)
Checked	Long Integer	0: Audit NOT performed against target. 1: Audit performed against target.
Description	String [255]	Description of data that was checked for on the remote target.
TestedValue	String [255]	Data that was checked for on the remote target.
FoundValue	String [255]	Data that was found on the remote target.

Table 4. eEye_Audits

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier.
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	Audit Type: Field format: [risk][Name].rth Where: [risk] is a single digit number expressing the risk (0..9) [Name] is the audit name that corresponds to the Name element in the audits.xml. To input every possible value for this field, construct this format of string for each entry in the name and risk elements of audits.xml. Users and integrators should not need this field.
path2	String [255]	Audit ID as referenced in audits.xml.
path3	String [255]	Reference to RTH file. Contains Audits\<category>\<rth name>.rth. Integrators should not need this file.
DisplayField	String [255]	Audit Category

Identifier	Field Type	Description
ValueField	String [255]	Audit Name
Risk	Integer	0: Info 1 – 3: Low 4 – 6: Medium 7 – 9: High

Table 5. eeye_Devices

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Links to eeye_activity:ID_
path1	String [255]	Device Type
path2	String [255]	Not Used
path3	String [255]	Not Used
DisplayField	String [255]	Device Name
ValueField	String [255]	Device Description
Risk	Integer	Not Used

Table 6. eeye_Groups

Identifier	Field Type	Description
ID_	String [32]	Job ID
Name	String [255]	Job Name
ScanStart	Date/Time	Date time job started
ScanEnd	Date/Time	Date time job ended
Status	String [50]	Job status as Completed, Aborted, Running or Paused

Table 7. eeye_Hardware

Identifier	FieldType	Description
ID_	String [32]	Unique record identifier
ActivityID	String [32]	Link to eeye_activity:ID_
Path1	String [255]	Hardware category and instance count
Path2	String [255]	Internal data label classification
Path3	String [255]	Not Used
DisplayField	String [255]	Data label, such as “Drive Description” or “Processor”

Identifier	FieldType	Description
ValueField	String [255]	Captured data, such as “CD-ROM Disc” or “CPU0”
Risk	Integer	Not Used

Table 8. eeye_Machine

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier
ActivityID	String [32]	Link to eeye_activity:ID_
Path1	String [255]	Machine info
Path2	String [255]	Not Used
Path3	String [255]	Not Used
DisplayField	String [255]	Info type, such as OS, NetBIOS Name or Date/Time
ValueField	String [255]	Captured Data, such as Windows 2000
Risk	Integer	Not Used

No Audits

The following table lists the audits that discovered not to be vulnerable on the target device.

To enable reporting of No Audits, the user must create and set the following registry key:

HKLM\SOFTWARE\eEye\Retina\5.0\Settings\DoNoAuditEnabled

The type is string. Setting:

1 — Starts reporting and deleting the key.

0 — Stops reporting the key.

Table 9. eeye_NoAudits

Identifier	Field Type	Description
ID_	String [50]	Unique Record Identifier
ActivityID	String [50]	Link to eeye_activity:ID_
RTH_ID	Long Integer	Audit ID as referenced in audits.xml.

Table 10. eeye_Ports

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	Port Number in the format [Port type][Port Number] where port type is U or T for UDP or TCP

Identifier	Field Type	Description
path2	String [255]	If blank, DisplayField and ValueField contain the port number and protocol. If State, ValueField expresses the port state as Open, Closed, or Filtered. If Version, ValueField contains the port banner. The meaning of the banner varies based on protocol. If HTTP services, the banner is the Server HTTP response header field. If SMB, the banner is an identifier for the service, such as the operating system "Windows 5.1" for XP, or "Samba" for hosts running Samba. If FTP, SMTP, Telnet or miscellaneous, the banner is the greeting string sent back when Retina connects to the service.
path3	String [255]	Not Used
DisplayField	String [255]	Port info [port type]:[port number]; Port State for State Detected Protocol for Proto Version for Version
ValueField	String [255]	Port specific Field Value, such as name of service; open or closed; name of protocol or NetBIOS version string.
Risk	Integer	Not Used

Table 11. eeye_Processes

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	Process Number
path2	String [255]	PID, PIDParent, or StartTime
path3	String [255]	Not Used
DisplayField	String [255]	“Process “[Process Number], “Process ID”, “Parent PID”, or “Start Time”
ValueField	String [255]	Name of process, Process ID, Parent Process ID or time the process was started.
Risk	Integer	Not Used

Table 12. eeye_Protocols

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier

Identifier	Field Type	Description
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	IP Protocol Number: 0 to 255
path2	String [255]	If blank, ValueField contains the Protocol Name If State, ValueField expresses the protocol state as Open or Open/Filtered. If Reason, ValueField contains the reason for detection, such as: icmp-response, syn-ack, tcp-response, udp-respone or no-response
path3	String [255]	Not Used
DisplayField	String [255]	“IP: XXX”, “Response Type” or “Protocol State”
ValueField	String [255]	Protocol name, state or reason for detection
Risk	Integer	Not Used

Table 13. eeye_ReportNvp

Identifier	Field Type	Description
GroupID	String [32]	Unique Record Identifier
Key	String [50]	
Value	Memo	

Table 14. eeye_Services

Idenitifer	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	The short name of the service. For a process enumeration, it is the 8-digit zero-padded process ID in hexadecimal.
path2	String [255]	Includes the service attribute names.
path3	String [255]	Not Used
DisplayField	String [255]	Short name of the service or Process [pid]. For a process, where [pid] is a 5-or-more-character, space-padded process ID number.
ValueField	String [255]	For services [STOPPED] or [RUNNING] followed by the long name of the service, or, for process, the executable name.

Idenitifer	Field Type	Description
Risk	Integer	Not Used

Table 15. eeye_Shares

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	Share name, such as C$, ADMIN$ or MyShare
path2	String [255]	1Name, 2Serial, FS, or Options Numbers are for sorting purposes only.
path3	String [255]	Not Used
DisplayField	String [255]	Share Name, “Volume Name”, “Serial Number”, “File System”, “Supported Options”
ValueField	String [255]	Description of share, if available
Risk	Integer	Not Used

Table 16. eeye_Software

Identifier	Field Type	Description
Identifier	**Field Type**	**Description**
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	Software title
path2	String [255]	Internal data label classification
path3	String [255]	Not Used
DisplayField	String [255]	Data label, such as “Version” or “Installation Path”
ValueField	String [255]	Captured data, such as “BeyondTrust Retina”
Risk	Integer	Not Used

Table 17. eeye_Users

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	User Name
path2	String [255]	User attributes, such as Last Logon or Password Age
path3	String [255]	Not Used

Identifier	Field Type	Description
DisplayField	String [255]	User attributes, such as Last Logon, Password Age or name
ValueField	String [255]	Detected values for attributes and description, if available.
Risk	Integer	Not Used

Table 18. eeye_WinGroups

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeye_activity:ID_
path1	String [255]	User group name
path2	String [255]	User group attributes, such as SID
path3	String [255]	Not Used
DisplayField	String [255]	User group attributes
ValueField	String [255]	Detected values for attributes and description, if available.
Risk	Integer	Not Used

Table 19. Sample eeye_Device Entries

Path	DisplayField	ValueField
Date	Report Date	Date and time the device was discovered
Address	Address	IP address of the device
Traceroute	Traceroute	Comma separated list of IP addresses denoting hops to host
Time To Live	Time To Live	TTL from ping response
Ping	Ping Response	Message indicating whether or not the device responded
Ping2	Avg Ping Response	Average number of milliseconds between ping and reply
DNS	Domain Name	Reverse-lookup DNS or NetBIOS name of host

Table 20. Sample eeye_Machine Entries

path1	path2	DisplayField	ValueField
zOpen		Open Ports	Displays the number of open TCP ports detected on the target device
OSDETECT		OS Detected	Retina's description of the machine's operating system Entries depend on how the OS was detected. - Discovered using Windows registry, the registry information is entered.

path1	path2	DisplayField	ValueField
			- Discovered using NetBIOS, the string in the NetBIOS return data is entered. - Discovered using ICMP discovery, the string contained in the fingerprint.xml file located in the <Retina Installation>\Database\Reference\ICMPOSD_FP directory is entered. - Discovered using TCP fingerprinting, the string from the retfp file located in the <Retina Installation>\Database\Reference directory is entered.
OSDETECT	OS	OS Name	NetBIOS name, if available.
OSDETECT	Method	Detection Method	The OS discovery method, such as registry, NetBIOS, ICMP or TCP.
OSDETECT	Vendor	Vendor	Company that develops or distributes the OS
OSDETECT	Version	Version	OS version number
OSDETECT	Type	Device Type	Either Workstation for Windows devices or devices defined in the ICMP or TCP footprints.
RDATE		Remote Date	Target device system date in GMT
RTIME		Remote Time	Target device system time in GMT
RMAC		Remote MAC	Target's MAC address on the network interface being scanned
RNBNAME		NetBIOS Name	NetBIOS name of target
RNBGROUP		NetBIOS Domain	
DNS		Domain Name	IP domain name of the target
zTCPOpen		Open TCP Ports	Number of open TCP ports discovered on the target device
zUDPOpen		Open UDP Ports	Number of open UDP ports discovered on the target device
XAuditing		Event Auditing	Enabled
XAuditing	00000000	Audit system events	Success or Failure

path1	path2	DisplayField	ValueField
XAuditing	00000001	Audit logon events	Success or Failure
XAuditing	00000002	Audit object access	Success or Failure
XAuditing	00000003	Audit privilege use	Success or Failure
XAuditing	00000004	Audit process tracking	No Auditing
XAuditing	00000005	Audit policy change	Success or Failure
XAuditing	00000006	Audit account management	Success or Failure
XAuditing	00000007	Audit directory service access	Success or Failure
XAuditing	00000008	Audit account logon events	Success or Failure
Risk	Risk	Integer	Not Used

Table 21. Sample eeye_User Entries

path2	ValueField
a1AccountDisabled	If account is disabled, True
a1AccountLocked	If account is locked out, True
a1Fullname	If user's password never expires, True
a1UF_DONT_EXPIRE_ PASSWD	Full name of user
a1UF_PASSWD_CANT_ CHANGE	If user cannot change his password, True
b1Lastlogon	Last time user logged in or Never
c1Lastlogoff	Last time user logged off or Unknown
d1PasswordAge	Age of user's current password in days
e1Expires	Time when user account expires or Never
e1Homedir	User's home directory
f1Homedrive	User's home drive
g1Logonserver	Name of server where logon requests are sent

path2	ValueField
h1Maxstorage	User's storage limit or Unlimited
numlogons	Number of times user has logged on or Unknown
Privilege	User's privilege level: Guest, User or Administrator
Profilepath	Path to user's profile
PWexpired	If user's password has expired, Yes If user's password has not expired, No
RID	RID component, such as last number, of user's SID identifier
Workstations	List of workstations where user is allowed to log on
z1BadPWcount	Number of bad login attempts allowed before user lock-out or Unlimited
z2Countrycode	Country or region code for the user's language
Risk	Integer

OS returns information in WinGroups.

Group is the name of the group.

Z8GroupMember is a list of CRLF group names that the user belongs to.

Zones are the Internet zones the user is allowed access to.

Troubleshooting Retina

You can create a package of files that you email to BeyondTrust Technical Support.

Submitting Support Files

To help troubleshoot debug problems, you can package support files to send to the BeyondTrust online support system. These files are saved in a WinZip format.

The Retina Support Tool automatically captures the support log files associated with the selected scan using the following two methods.

To create a support package from the Help Menu:

- From the main menu, select **Help** > **Package Support Files**.

  The support tool packages all debug files.

To create a support package from the Completed pane:

1. Select the **Audit** tab.
2. Select **Completed** in the Scan Jobs section.
3. Right-click a completed scan and select **Package Support Files**.
4. The support tool captures the log files from the selected scan.

Upgrading Retina Community

You can upgrade Retina Community to Retina, in the following ways:

- from the Retina Community home page when you start up Retina Community
- from the main application window
- from the Help menu

