

Symantec Control Compliance - Vulnerability Manager Network Scanner

User Guide

Version 12.0



CCS-VM Network Scanner User Guide

Documentation version: 1.0

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

Contents

Chapter 1 Introduction	8
Documentation Set for CCS-VM Network Scanner	8
Chapter 2 Overview	9
Architectural Overview	10
Scanning Process	12
Typical Bandwidth Usage	13
Chapter 3 Changing the CCS-VM Network Scanner Home Page View	14
Chapter 4 Getting Started	15
Quick Scanning	15
Chapter 5 Managing Credentials	18
Creating a Stored Credential	18
Creating an SSH Credential	20
Creating Oracle Credentials	22
Creating SNMP Credentials	23
Creating a Credential Group	24
Chapter 6 Defining Address Groups	25
Using the Always Address Group	25
Creating Address Groups	26
Chapter 7 Managing Ports	28
Creating a Port Group	28
Reviewing Port Number	30
Chapter 8 Running Discovery Scans	31
Configuring a Discovery Scan	31

Running a Discovery Scan	32
Scheduling a Discovery Scan	33
Clearing Discovery Scan Data	34
Chapter 9 Running Audit Scans	35
Configuring Audit Scans	35
Selecting Targets and Output Types	35
Selecting Ports	36
Selecting Audits	37
Selecting Audit Options	38
Setting Credentials	42
Running Scans	43
Scanning Immediately	43
Scheduling Scans	44
Scanning File Contents on Windows Targets	46
Exporting Scan Results to CyberScope	48
Running a Wireless Scan	50
Deleting Scan Jobs	51
Aborting Large Scans	52
Chapter 10 Remediating Vulnerabilities	54
Generating Remediation Reports	54
Reviewing Remediation Reports	57
Using CVSS Scores	58
Chapter 11 Generating Reports	59
Running Executive Reports	59
Running Summary Reports	61
Running Vulnerability Export Reports	62
Running Access Reports	62
Running PCI Compliance Reports	63
Adding Your Logo to PCI Compliance Reports	65
Running a Dashboard Report	65
Running an Alert Report	65
Customizing Reports	67
Chapter 12 Customizing Audits	68

Searching the Audit Database	69
Changing Risk Levels	70
Modifying Customizable Settings	71
Resetting Audits to Default Values	72
Running Audit Customization Reports	72
Viewing Modified Audits	73
Creating Custom Audits	73
Updating the Scanner Database	78
Viewing Custom User Created Audits	79
Modifying Audit Groups	79
Exporting Audits	80
Creating Custom Audit Modules	81
Editing Custom Audit Modules	81
 Chapter 13 Exploiting Vulnerabilities	 83
Exploiting a Vulnerability	83
Integrating with Metasploit	85
 Chapter 14 OS Fingerprinting	 86
Updating TCP OS Fingerprints	86
 Chapter 15 Configuring Email Notification for Events	 87
Setting Alerts	87
 Chapter 16 SCAP Scanning	 89
Copying SCAP Content (Optional)	89
Running SCAP Scans	89
Using the Local Scan Service	90
Configuring a SCAP Scan	90
Saving Scan Results as PDF	92
 Chapter 17 Setting Options	 93
Generating Log Files	93
Automatically Check for Updates	94
Enabling Event Routing	94

Scanning Multiple Targets Simultaneously	96
Setting Timeout Values	97
Setting Scan Restrictions	98
Enabling Central Policy	98
Chapter 18 Run Database Application Scans	100
Running Database Application Scans	100
Review Database Application Vulnerabilities	100
Preparing Database Applications for Scans	102
Preparing Your MySQL Database for Scans	102
Chapter 19 Running Retina from the Command Line	103
Retina.exe CLI Switches	103
Run Reports from the CLI	104
Chapter 19 Retina.Report.Console.exe CLI	106
Parameters	106
Examples	106
RetRPC_client.exe CLI	107
Starting a Scan from the CLI	110
Chapter 20 Database and XML Schema	113
RTD Schema	113

Introduction

This guide shows system administrators and security administrators how to configure and use Symantec CCS-VM Network Scanner. This guide provides an overview of how CCS-VM Network Scanner works and instructions for CCS-VM Network Scanner configuration and use.

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

Documentation Set for CCS-VM Network Scanner

The complete documentation set includes the following:

- CCS-VM Network Scanner *Installation Guide*
- CCS-VM Network Scanner *User Guide*
- CCS-VM Network Scanner Help

Overview

CCS-VM Network Scanner provides vulnerability testing for multiple platforms, assessment of vulnerabilities and the ability to create your own audits. In addition, CCS-VM Network Scanner allows you to proactively secure your networks against the most critical vulnerabilities by incorporating the most up-to-date vulnerabilities database. Since vulnerability audits are added continually, this database is updated at the beginning of each session.

Using CCS-VM Network Scanner, you can:

- Scan in parallel using the CCS-VM Network Scanner 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.

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

Architectural Overview

The scanner'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 User Interface or command line.
- **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.
- **RPC Client** — Receives and forwards data from the UI or other applications to the RPC interface. In addition, the RetRPC_Client.exe is the return conduit for data to the UI.
- **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.

- **Events Client** — Forwards data to the Events Server, if the scanner is integrated with the centralized console.
- **Product Updater** — Communicates with the Symantec servers to ensure the application and audit data files are current.

Scanning Process

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

Note: The following details on how a scan works is provided for information only.
Do not change the 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. The scanner 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, the scanner retrieves the list of IP addresses to be scanned and builds and writes its target list to the eeeye_groups table. The job list contains the job start and stop information. The scanner then starts 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 end of the scan, the scanner writes Completed to the eeeye_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.

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

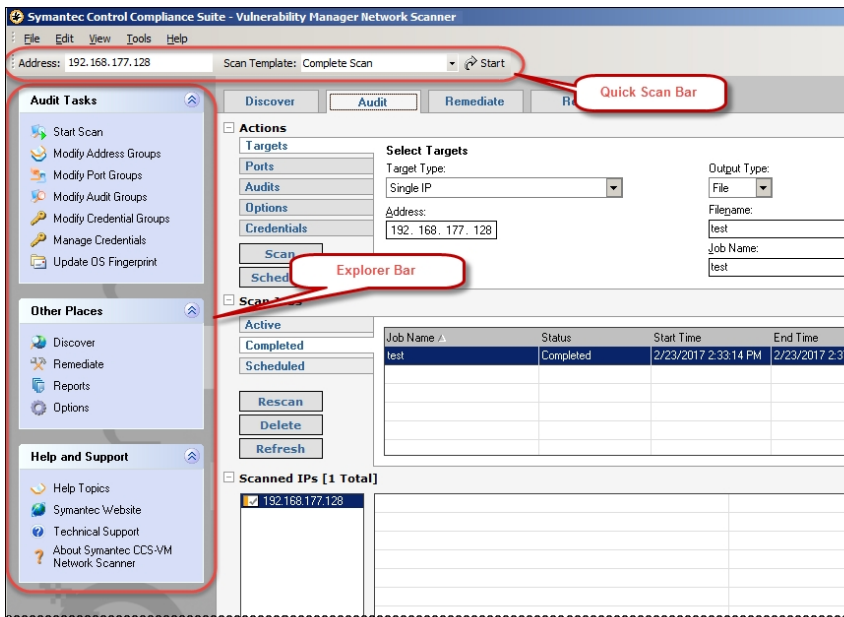
	Null Session	Authenticated
Audits	All Audits, Common Ports, Defaults	All Audits, Common Ports, Defaults, Local Scan Service
Traffic to Target	120 Kb	27.5 MB
Event Traffic to Centralized Console	15 Kb	165 Kb
Time To Complete	9 minutes	14 minutes
Results	High:0 Medium:0 Low:0 Information:12	High:135 Medium:38 Low:47 Information:52
Operating System	Windows XP, SP3	
Hardware	i7, 3GHz, 512MB RAM Virtual Machine	
Notes	Firewall Enabled	Remote Access Permitted

Changing the CCS-VM Network Scanner Home Page View

You can add an explorer view and quick scan bar to the CCS-VM Network Scanner home page.

To change the view:

1. Select **View > QuickScan** or **View > Explorer Bar**.



Getting Started

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

Note: You must have administrator rights to run scans on target assets.

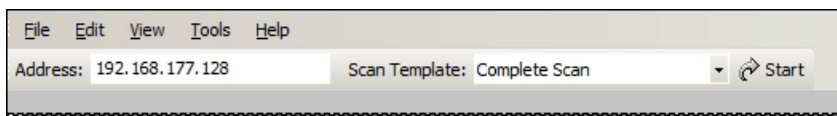
Quick Scanning

Using the templates, you can quickly scan based on an individual IP address or sequential range of IP addresses. You then generate a remediation report on the Remediate pane and generate and view the data online or offline using the Reports pane.

You can create a scan template, then use that template later rather than recreating the settings each time you want to run a scan. Go through the Scan Job Wizard on the Tools menu to create a template. For more information on the options available, see [Configuring Audit Scans](#).

To run a quick scan:

1. On the CCS-VM Network Scanner home page, verify the **Quick Scan** toolbar is displayed. If not, select **View > Quick Scan**.



2. Enter an IP address or sequential range of IP addresses in the Address box.
3. Select a template from the Scan Template list:
 - **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 progress displays in the Scanned Job area of the Audit tab. A summary of the vulnerabilities based on the scanned IPs is displayed in the Scanned IPs section.

The screenshot shows the 'Quick Scanning' application interface. The 'Audit' tab is selected, displaying the 'Scanned Job' area. The 'Scanned IPs' section shows a list of scanned IP addresses, with '192.168.177.128' selected. The 'Scan Results' section displays details for the selected IP, including the OS detected (Windows Server 2008, Service Pack 2) and the vendor (Microsoft).

Actions

- Targets
 - Ports
 - Audits
 - Options
 - Credentials
- Buttons: Scan, Schedule

Select Targets

Target Type: Single IP
 Address: 192.168.177.128
 Output Type: File
 Filename:
 Job Name:

Scan Jobs

Job Name	Status	Start Time	End Time	Data Source	Scan Engine
Complete Scan	Completed	3/2/2017 10:28:40 AM	3/2/2017 10:44:35 AM	C:\Program Files\Syma...	Vulnerability
test	Completed	3/2/2017 4:45:58 PM	3/2/2017 4:50:59 PM	C:\Program Files\Syma...	Vulnerability

Scanned IPs [1 Total]

192.168.177.128

Alerts

- NetBIOS Credentials: The selected credential has SYSTEM privileges

Machine

- Domain Name: WIN-B9E8UCFYE7.localdomain
- NetBIOS Credentials: SYSTEM account
- OS Detected: Windows Server 2008, Service Pack 2
- Remote Date: 03/03/2017 GMT
- Remote MAC: 00:0C:29:CD:FF:72
- Netbios Domain/Group: WORKGROUP
- Netbios Name: WIN-B9E8UCFYE7

OS Detected: Windows Server 2008, Service Pack 2

Vendor: Microsoft

OS Version: Windows Server 2008, Service Pack 2

Detection Method: Remote

Scan complete

The following details are included in the scan results. Note that results are only displayed when assets are detected during the scan.

General	Provides information on address, report date, ping response, time to live, trace route, and last logged on user.
Hardware	Lists disk drive, memory, network card, processor, video, and manufacturer information.
Audits	Lists the severity from critical to information and categorized as registry, Windows, IP services, web servers, remote access, anti-virus and miscellaneous.
Machine	Lists the machine by domain name, credentials, operating system, remote date, remote MAC, NetBIOS info, remote time, role, event auditing, number of open, closed, and filtered TCP and UDP ports. For a virtual machine, lists the virtual machine vendor, name, current snapshot, and UUID.
Ports	Describes the TCP and UDP ports.
Processes	Lists all the processes running on the target system and can include the following details: product name, file version, file description, file location, command line, memory usage, process ID, parent process, parent process ID, DLLs loaded, mutex, MD5/SHA1 hash, company name, verified signer, and user name.
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.
Software	Lists all software installed on the target system.
Users	Lists all the users found on the target system.
User Groups	Lists all the groups found on the target system.

5. To view the results in a report, select the **Report** tab.
6. Select the job name, then click **Generate**. The report is displayed. You can also view the report in Microsoft Word and web browsers.

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 CCS-VM Network Scanner, 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.

Credentials

Credential Management

Type: Microsoft SQL Server ▼

Description: db owner

Username: SQL DB

Password: [masked]

Confirm Password: []

Authentication Type: Any ▼

Any

Windows

SQL

Add

Description /	Username	Type

*The default credential, if any, appears in bold.

Delete

Close

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:

The image shows a sidebar on the left with a minus icon and the title 'Actions'. It contains several buttons: 'Targets', 'Ports', 'Audits', 'Options', 'Credentials', 'Scan', and 'Schedule'. The 'Credentials' button is highlighted. To the right of the sidebar is a 'Select Credentials' dialog. It has a 'Credential Type:' dropdown menu with 'Stored' selected. Below this is a list of three items: 'FLA admins', 'Mass admins', and 'New York admins', each with an unchecked checkbox. An 'Add' button is located to the right of the list.

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.

To create an SSH credential:

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

The image shows a dialog box for adding an SSH credential. It has a 'Type:' dropdown menu with 'SSH' selected. To the right is an 'Authentication Type:' dropdown menu with 'Password' selected. Below these are four text input fields: 'Description:', 'Username:', 'Password:', and 'Confirm Password:'. At the bottom left is an 'Elevation:' dropdown menu with 'None' selected. An 'Add' button is located at the bottom right.

3. Provide a description and user name.

4. Select an authentication type from the list: Plain Text or Public Key.
 - **Password** - 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 tsnames.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.

The screenshot shows a dialog box for creating an Oracle credential. It contains the following fields and values:

Type:	Oracle	Username:	DB_User
Description:	MyOracleCreds	Confirm Password:	XXXXXXXX
Password:	XXXXXXXX		
Access Level:	Standard		
Connect To:	Database SID	Database SID:	ORCL9
Protocol:	TCP		
Host:	10.100.5.12	Port Number:	1521

An **Add** button is located at the bottom right of the dialog box.

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**.

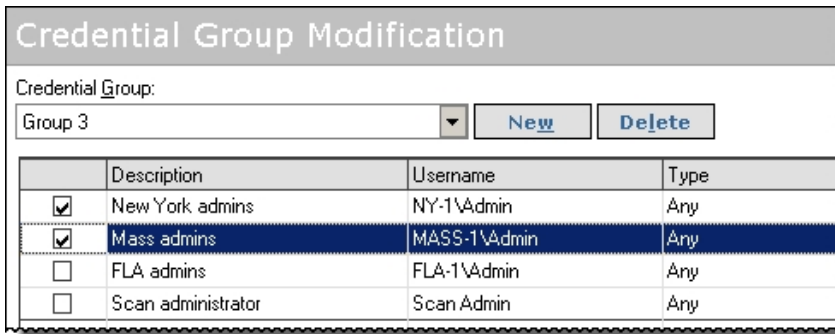
Creating a Credential Group

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

Note that credential groups cannot be used for XCCDF scans.

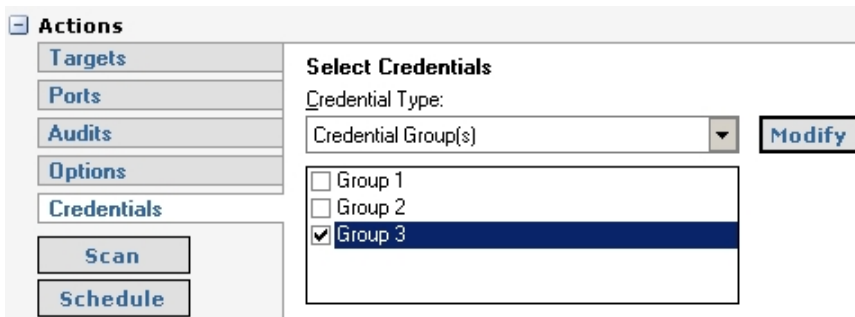
To create a credential group:

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.



	Description	Username	Type
<input checked="" type="checkbox"/>	New York admins	NY-1\Admin	Any
<input checked="" type="checkbox"/>	Mass admins	MASS-1\Admin	Any
<input type="checkbox"/>	FLA admins	FLA-1\Admin	Any
<input type="checkbox"/>	Scan administrator	Scan Admin	Any

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



Actions

Targets
Ports
Audits
Options
Credentials
Scan
Schedule

Select Credentials

Credential Type:
Credential Group(s) Modify

☐ Group 1
☐ Group 2
☒ Group 3

Defining Address Groups

To ensure repeatable scans CCS-VM Network Scanner 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.

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*. CCS-VM Network Scanner 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 created stored credentials, 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.

Address Groups

Address Group:

IP address range

New

Delete

☐ Single IP
 ☒ IP Range
 ☐ CIDR Notation
 ☐ Named Host

From: 192.168.177.5
 To: 192.168.177.10
☐ Omit this entry.

Credentials:

Address	Omit
192.168.177.5-192.168.177.10	No

Import

Add

Delete

Close

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

Managing Ports

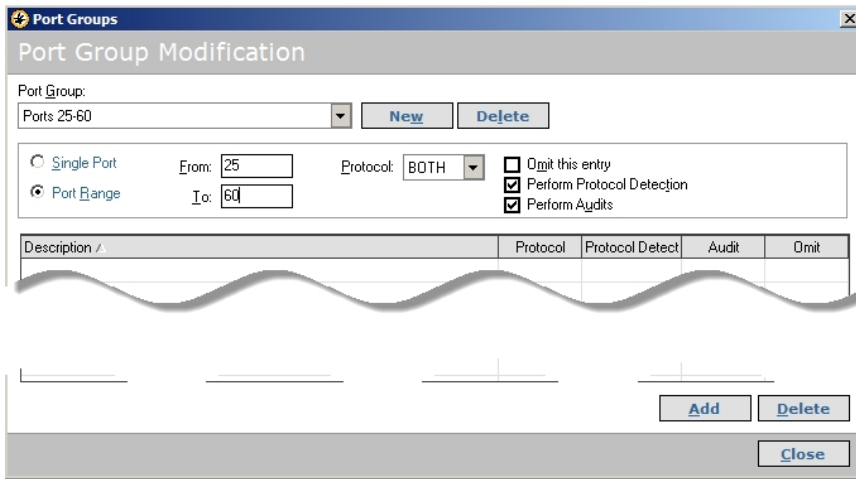
While there are preconfigured port groups available for scanning, you can create port groups that are specific to your scanning requirements.

You can create and change port and port group details.

Creating a Port Group

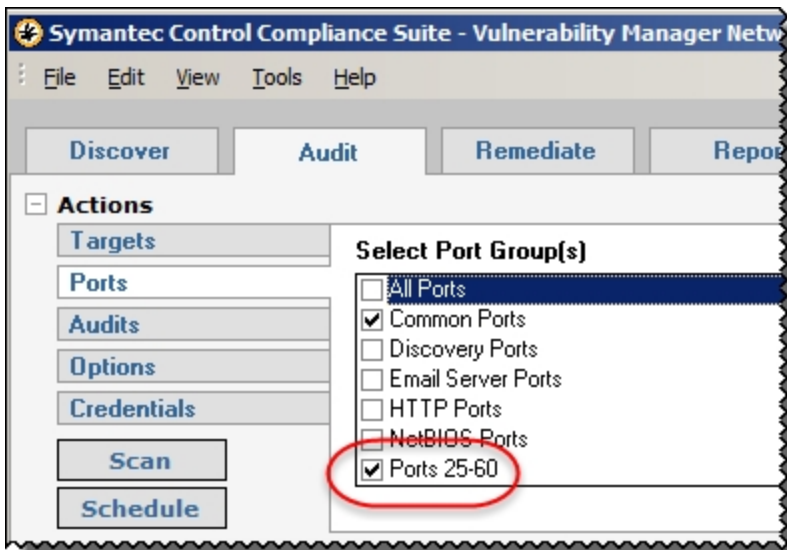
To create a port group:

1. From the Tools menu, select **Port Groups**.
2. Click **New**.
3. Enter a name for the group.
4. Select **Single Port** or **Port Range** and set the port numbers.
5. Select from the following options:
 - **Protocol** - Select the port protocol: Both, TCP, or UDP.
 - **Omit this entry** - Excludes the port from protocol detection and scanning.
 - **Perform Protocol Detection** - Excludes the ports from a scan. The ports are excluded even if during the dependence check one of the excluded ports is included. The check box is selected by default.
 - **Perform Audits** - When selected, run the audit on the port if the port is found during the port scan. The check box is selected by default.



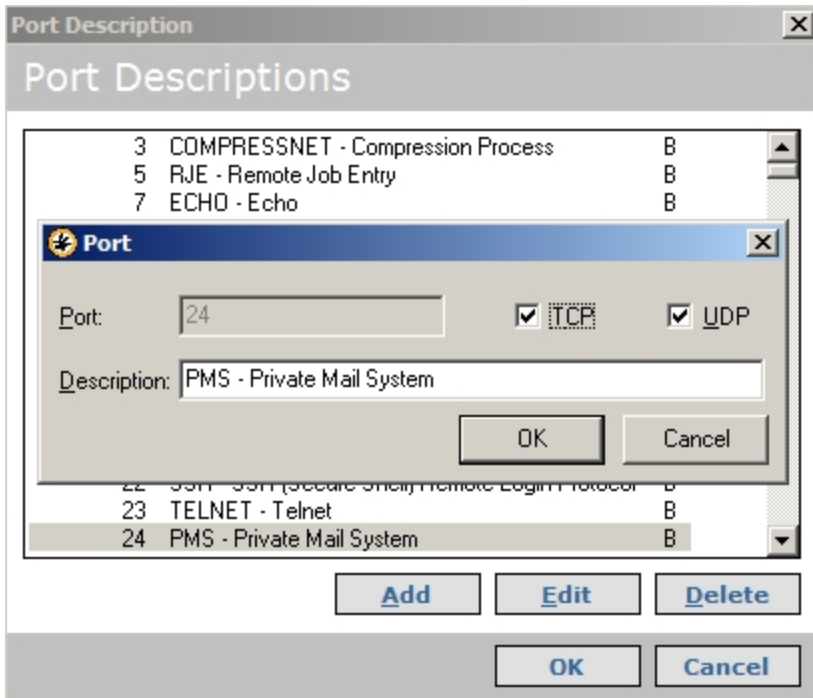
6. Click **Add**.
7. Click **Close**.

The port group is added to the list of port groups that can be selected for scanning.



Reviewing Port Number

1. To review a list of port numbers and associated processes, select **Tools > Port Descriptions**. You can add a port, change a port description, or delete ports to conform to your network.



Running Discovery Scans

The Discovery scan allows you to locate network devices, such as workstations, routers, laptops and printers, and determine if a single or multiple IP addresses are active. In addition, the scan results can provide data on an outside source attempting to exploit your network.

You can periodically repeat the discovery scans to verify the status of devices and programs and the delta between the current and previous scan.

Note: Administrator rights are required to run scans.

To access discovery scans:

1. On the CCS-VM Network Scanner home page, select the **Discover** tab. The Discovery page is displayed.

Configuring a Discovery Scan

To configure discovery scans:

1. On the Discovery pane, select the target type in the **Target Type** list box.
 - **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. 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 Group** - The group contains any combination of computer IP addresses, IP address ranges, subnets or other groups.

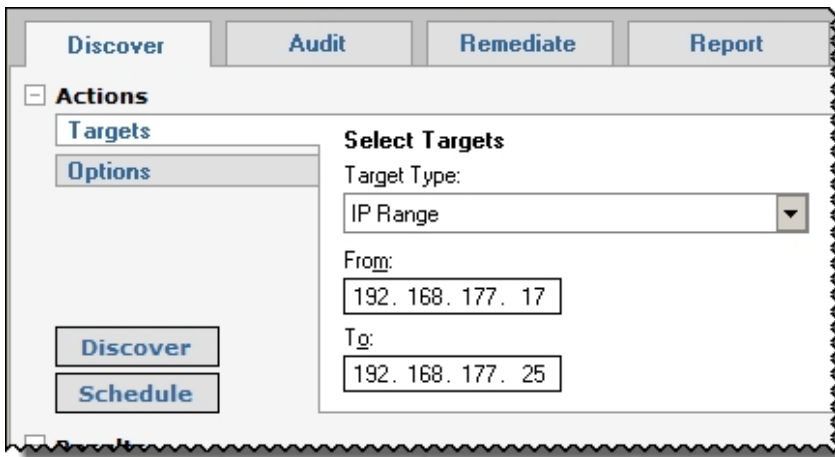
- **Advanced Addresses** - Scans using subnet IP address.
2. Click **Options**, then select the type of information to scan:
- **ICMP Discovery** - Determines the Internet Control Message Protocol.
 - **TCP Discovery on Ports** - Determines the Transmission Control Protocol message packets. You can enter multiple ports by using comma separators.

The default port list includes: 21,22,23,25,80,110,139,443,445,554,1433,3389
 - **UDP Discovery** - Determines the User Datagram Protocol.
 - **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** - Scans for a Network Basic Input/Output System.
 - **Get MAC Address** - Scans for the Media Access Control address or unique hardware number.

Running a Discovery Scan

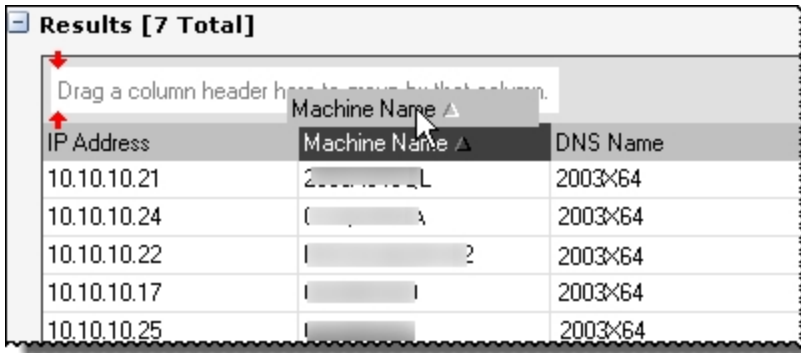
To run a discovery scan:

1. On the Discover pane, click **Discover**. The status bar displays the scan progress.



The discovered assets are displayed in the Results area.

2. To change the sort order, drag a column header to the top of the results.



Results [7 Total]

Drag a column header here to move to that column.

IP Address	Machine Name	DNS Name
10.10.10.21	2003X64	2003X64
10.10.10.24	2003X64	2003X64
10.10.10.22	2003X64	2003X64
10.10.10.17	2003X64	2003X64
10.10.10.25	2003X64	2003X64

3. To interrupt the scan and display the current results, click **Pause**. The results display in the Results area.
4. To generate a report, select **Report** or **Export** from the list, then click **Generate**. Select Export to generate XML format; select Report to generate HTML format.
5. To stop the scan, click **Abort**.
6. To clear the results, click **Clear Discovered Items**.

Scheduling a Discovery Scan

You can schedule Discovery scans. The scans are scheduled by Frequency, Time and Run Date.



The scan duration is calculated from the scheduled start time, not the time the job begins.

For example, if a job is delayed because the computer was rebooting, other jobs are running or the service was stopped, the 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.

To schedule scans:

1. Click the **Discover** tab, and click **Schedule**. The Scan Job Scheduler window is displayed.
2. Enter a name.
For Discover scan jobs, the default job name is Discovery Scan. This cannot be changed.
3. Select the start time and date.

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. To limit the schedule to a specific time duration, 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.
6. Click **OK**.

Clearing Discovery Scan Data

You can clear the discovery scan data from the database.

To clear the scan data:

1. From the Discovery Tasks list, select **Clear Discovered Items**.
Alternatively, right-click a discovered item in the Results pane and select **Clear Discovered Items**.
2. To clear all discovered assets from the list, click **Yes**.

Running Audit Scans

The scanner can scan any device with an IP address if the route between the scanner and the IP address can be established. Scans can be internal 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 CCS-VM Network Scanner 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. From the Output Type list, select one of the following:
- **File** - To store scan results in a file.
 - **DSN** - To store results to a system database. To restore results in a specific DSN, create the DSN using ODBC Data Source Administrator in Windows Administrative Tools.

If no file or DSN is defined, CCS-VM Network Scanner stores multiple results in a single file.

5. Enter a file name and job name.

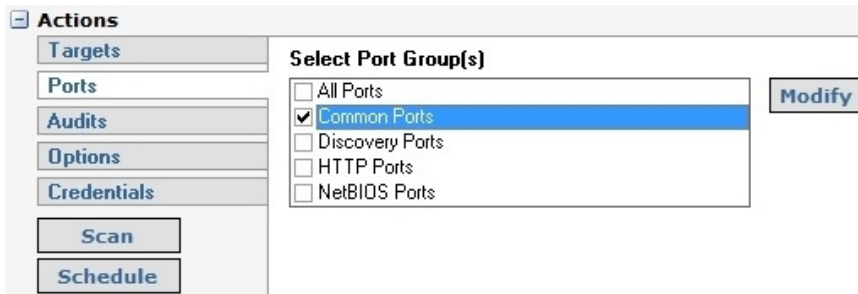
Selecting Ports

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

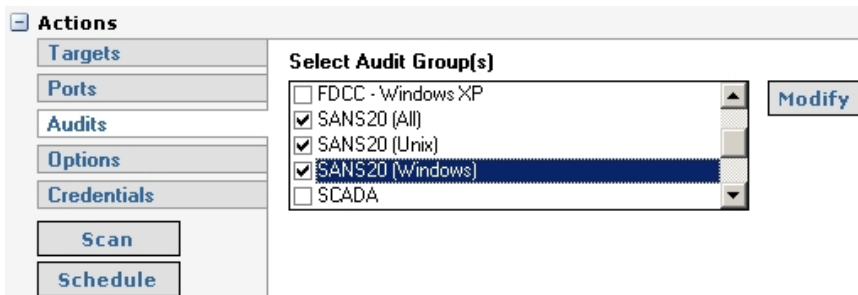
When you select audit group scan settings, you can:

- 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](#).

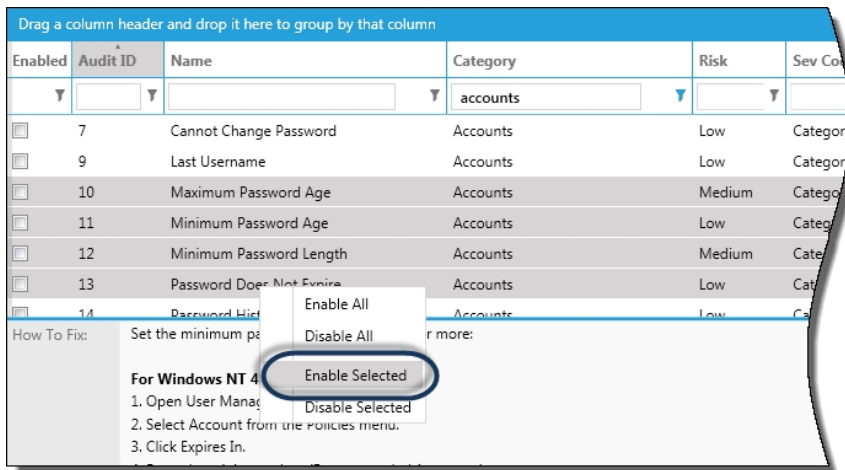
To select the audits for the scan:

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:

- 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.
- Select an audit group then select the check boxes for the audits that you want to add to the group.
- Right-click an audit and select **Enable All**; all audits in the audit group are selected.
- Shift+select audits to select more than one audit. Right-click and select **Enable Selected**.



- To change an existing audit group, select or clear audit check boxes.
- 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:

- Select the **Audit** tab.
- Select **Options**.
- 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 CCS-VM 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. CCS-VM is required for this option.
- **Perform IP Protocol Scanning** - Lists open and filtered IP protocols.
- **Enumerate Ports via Local Scan Service** - Installs the local CCS-VM Network Scanner 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 CCS-VM Network Scanner 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, CCS-VM Network Scanner 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 CCS-VM Network Scanner 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 CCS-VM Network Scanner 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 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, the scanner skips 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 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 or schedule the scan for a later date.

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

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

Scan Jobs						
Active						
Completed						
Scheduled						
Rescan						
Delete						
Refresh						
Job Name ▲	Status	Start Time	End Time	Data Source	Scan Engine	
All_Audits	Completed	6/16/2011 11:15...	6/16/201...	C:\Program File...	Retina	
First-time	Completed	6/15/2011 3:39:0...	6/15/201...	C:\Program File...	Retina	
scan-xccdf	Completed	6/15/2011 3:35:1...	6/15/201...	C:\Program File...	XCCDF	
Zero-Day	Completed	6/16/2011 1:27:4...	6/16/201...	C:\Program File...	Retina	

Scanning Immediately

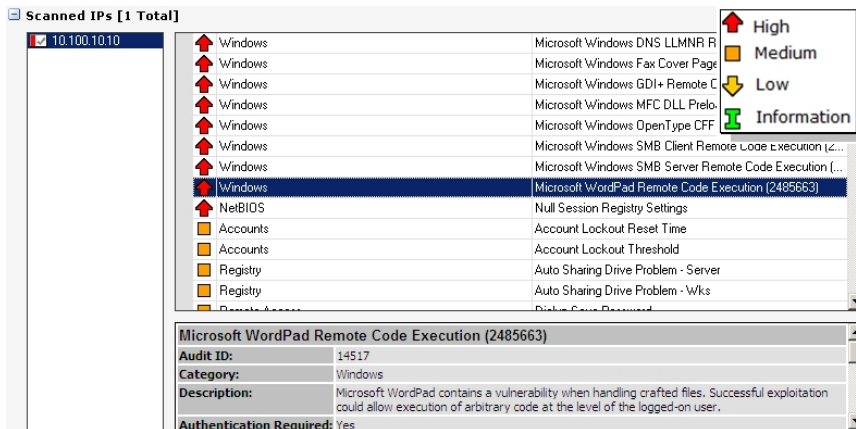
To scan the targets now:

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.



- 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](#).

Scheduling Scans

You can schedule scans. The scans are scheduled by frequency, start time and run date.

To schedule scans:

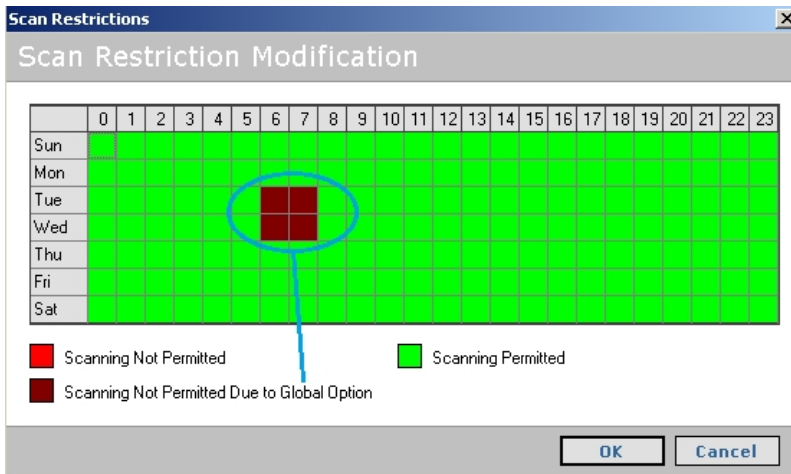
- Select the **Audit** tab, then click **Schedule**. The Scan Job Scheduler window displays.
- Enter a job name.
- Select the start time and date.



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. If there is a scan restriction set globally, the time frame is indicated on the Scan Restrictions dialog box. Click the **Override global scan restrictions** check box to clear the global settings.



9. Click the squares to set the restricted time frame, and then click **OK**.
10. If a scan is running when the scan restriction time starts, you can abort or pause the running scan. Select **Aborted** or **Paused**.
11. Click **OK**.

Scanning File Contents on Windows Targets

You can run scans on Windows remote targets to detect personally identifiable information, including:

Financial

- Actuality Report
- Credit card numbers, including the following card providers: AMEX cards, Diners Club, Discover Card, JCB, MasterCard, Maestro, Visa
- Credit card tracks. The audit includes all track types (1, 2, 3)
- Financial Report (English)
- IBAN Numbers (46 countries)

Note that actual credit card numbers are not reported in the scan information; only that the information is detected. For example, the scan might detect a file that contains an American Express credit card number; the scan output indicates the file name and the credit card type, but not the credit card number.

Personal

The following personal information can be detected: DNA sequence, Email address, Driver License (51 states/territories), Phone number, Social Security Number, ZIP Code (USA), ZIP Code+4 (USA)

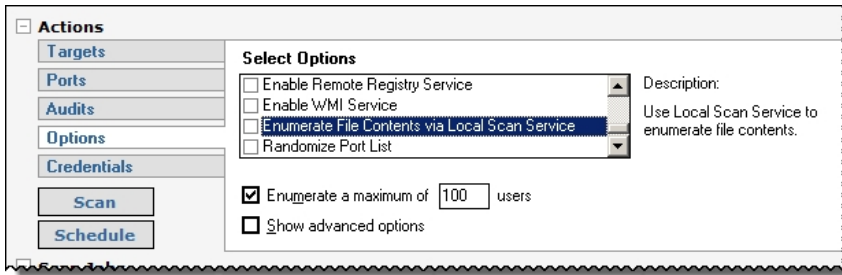
File types

The following list of file types can be scanned:

- Text Files (TXT)
- Log Files (LOG)
- XML Files (XML)
- Comma Separated Values (CSV)
- Microsoft Word 1997-2003 (DOC)
- Microsoft Word 2007+ (DOCX)
- Microsoft Excel 1997-2003 (XLS)
- Microsoft Excel 2007+ (XLSX)
- Microsoft PowerPoint 1997-2003 (PPT)
- Microsoft PowerPoint 2007+ (PPTX)
- Adobe Personal Document Format 1.2 – 1.7 (PDF)
- Rich Text Format (RTF)
- OpenOffice OpenDocument Text (ODT – as OpenXML)
- OpenOffice OpenDocument Spreadsheets (ODS – as OpenXML)
- OpenOffice OpenDocument Presentation (ODP – as OpenXML)

To configure the file contents scan:

1. Configure the scan settings as usual.
2. Select the **Options** tab, and then select the **Enumerate File Contents via Local Scan Service** check box.



3. Set credentials.
4. Click **Scan**.

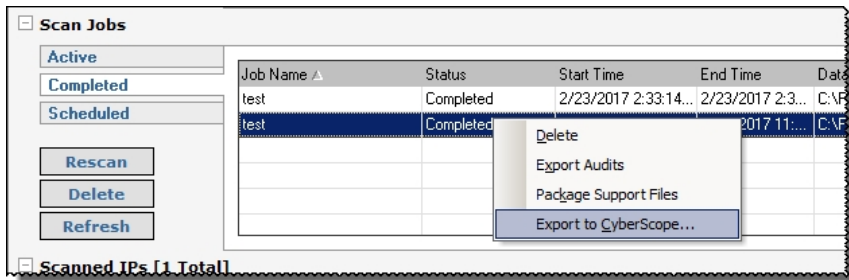
The output is similar to the following:

Financial Information - American	
Audit ID:	20001
Category:	Miscellaneous
Description:	American Express card numbers start with 34 or 37 and have 15 digits.
Authentication Required:	Yes
Risk Level:	High
Audit Confirmation Details	
Context:	C:\WINDOWS\...\USERS\ADMINISTRATOR\DOCUMENTS\PLP TEST DATA\FINANCIAL
Description:	Success
Tested Value:	%b?<[! = -\\ / + : ; ' \" \\ / @ ! #\$ & ' ^ & ' \" \\ / > ? . ' ~ w })3[47]d(2)<[!

Exporting Scan Results to CyberScope

You can export CCS-VM Network Scanner scans and SCAP scans to CyberScope format.

After a scan runs, right-click the scan and select **Export to CyberScope**.



Running a Wireless Scan

You can run wireless scans in one of the following ways:

- From the Tools menu
- Through the Options tab when running an audit scan. See [Selecting Audit Options](#).

To run a discovery scan to detect wireless devices:

1. Select **Tools > Wireless Scanner**.
2. To start the scan, click **Scan**.

Wireless Scanner

Scan

MAC Address	SSID	Vendor	Signal Strength	Authentication	Network Type	Channel	Last Detected
00-24-6C-B0-13-00	Guest	ARUBA NETWORKS, INC.	-68	Unknown	Infrastructure	11	10/14/2011 10:02:58 ...
00-24-6C-B0-13-01	TSNOfficeWLAN	ARUBA NETWORKS, INC.	-67	Unknown	Infrastructure	11	10/14/2011 10:02:58 ...
68-7F-74-35-9A-38	3393462	Cisco-Linksys, LLC	-69	Unknown	Infrastructure	11	10/14/2011 10:02:58 ...
00-24-6C-B5-E7-70	Guest	ARUBA NETWORKS, INC.	-73	Unknown	Infrastructure	11	10/14/2011 10:02:58 ...
00-24-6C-B5-E7-71	TSNOfficeWLAN	ARUBA NETWORKS, INC.	-72	Unknown	Infrastructure	11	10/14/2011 10:02:58 ...
00-24-6C-B5-F2-60	Guest	ARUBA NETWORKS, INC.	-75	Unknown	Infrastructure	1	10/14/2011 10:02:58 ...
00-24-6C-B5-F2-61	TSNOfficeWLAN	ARUBA NETWORKS, INC.	-74	Unknown	Infrastructure	1	10/14/2011 10:02:58 ...
00-24-6C-AA-2E-31	TSNOfficeWLAN	ARUBA NETWORKS, INC.	-87	Unknown	Infrastructure	1	10/14/2011 10:02:58 ...

Guest

MAC Address:	00-24-6C-B0-13-00	Vendor:	ARUBA NETWORKS, INC.
Security:	Unknown	Encryption:	None
Network Standard:	Unknown	Network Type:	Infrastructure
Channel:	11	Maximum Rate:	54 Mbit/s
Last Detected:	10/14/2011 10:02:58 AM	First Detected:	10/14/2011 10:00:03 AM
Signal Strength:	Current: -68 dBm	Min: -68 dBm	Max: -66 dBm Avg: -67 dBm

Reset **Report** **Close**

3. After the scan finishes, click **Report** to generate report details on the devices discovered.

The following screen shows sample output from a report.

Guest								
MAC Address:	00-24-6C-B5-F2-60		Vendor:	ARUBA NETWORKS, INC.				
Security	Open		Encryption:	None				
Network Standard:	802.11g		Network Type:	Infrastructure				
Channel:	1		Maximum Rate:	54 Mbit/s				
Last Detected:	10/14/2011 11:55:07 AM		First Detected:	10/14/2011 11:55:07 AM				
Signal Strength:	Current	-76 dBm	Min	-76 dBm	Max	-76 dBm	Avg	-76 dBm
TSNOfficeWLAN								
MAC Address:	00-24-6C-B5-F2-61		Vendor:	ARUBA NETWORKS, INC.				
Security	WPA2-Enterprise		Encryption:	AES				
Network Standard:	802.11g		Network Type:	Infrastructure				
Channel:	1		Maximum Rate:	54 Mbit/s				
Last Detected:	10/14/2011 11:55:07 AM		First Detected:	10/14/2011 11:55:07 AM				
Signal Strength:	Current	-75 dBm	Min	-75 dBm	Max	-75 dBm	Avg	-75 dBm
eduroam								
MAC Address:	00-1A-30-30-37-32		Vendor:	Cisco Systems				
Security	WPA2-Enterprise		Encryption:	AES				
Network Standard:	802.11g		Network Type:	Infrastructure				
Channel:	1		Maximum Rate:	54 Mbit/s				
Last Detected:	10/14/2011 11:55:07 AM		First Detected:	10/14/2011 11:55:07 AM				
Signal Strength:	Current	-86 dBm	Min	-86 dBm	Max	-86 dBm	Avg	-86 dBm

Note the following when running wireless scans.

- Windows 2000, Windows XP SP1/SP2, Windows 2003

The Security, Encryption, and Network Standard fields in the details will display either Unknown or None.

This data is not available on these platforms.

- Windows XP SP3

If the WZC service is not running, Windows XP SP3 behaves as above. When the service is running, the Security and Encryption fields reflect the correct values.

In the Network Standard field, the value 802.11g is displayed for 802.11n devices since the drivers are unaware of the 802.11n standard.

- Windows Vista, Windows 7

If the WLAN AutoConfig service is not running, wireless scanning fails.

When the service is running, all values are returned correctly.

- Windows 2008, Windows 2008 R2

For Windows 2008 and 2008 R2, add the Wireless LAN Service feature in the Server Manager for WLAN support to be enabled.

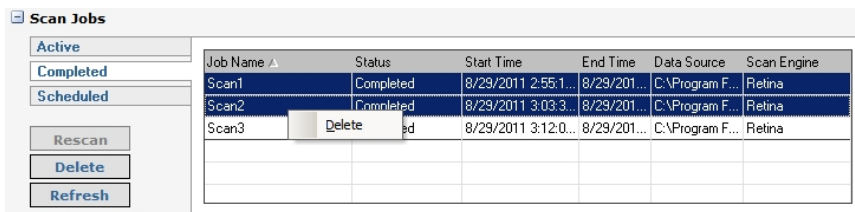
Once this feature is added, scans will run as described in the Windows Vista, Windows 7 section.

Deleting Scan Jobs

Scan jobs can be deleted.

To delete scan jobs:

1. Select the **Audit** tab, and then click the **Completed** tab.
2. Right-click a job, and then select **Delete**.
Press Shift + select jobs to select more than one job in the list.



3. Click **Yes**.

Aborting Large Scans

You can cleanly restart CCS-VM Network Scanner during large connect and force scans. However, aborting large scans requires additional time to clear out of the target.

For example, an audit scan on a Class C network using a force scan and connect scan typically requires 20 minutes, but, depending on the situation, could require 60 minutes. If the scan is requiring additional time, the user times out and aborts the job after approximately an hour.

In a connect scan with multiple ports using the OS stack, the abort requires additional time. The actual scanning stops quickly, but the multiple connections require an extended period to timeout and the queue also requires deleting.

If you restart or stop the service, this only stops the scanning until the CCS-VM Network Scanner Engine service restarts. The abort does not clear the queue entries. As the scanner accesses the queue and restarts scanning for the devices still listed, the job immediately starts again.

To preclude this, the best solution is abort the scan job and wait for the abort process to complete. If the job is causing another problem on the network, then aborting the job and unplugging the network is the next best solution. Though without the network connection, the abort could take even longer.

To abort the job and place the scan in a known state:

1. Click **Abort**.
2. Stop the CCS-VM Network Scanner service (net stop retinaengine).
3. If the scan will be continued in the future, rename or move queue.xml. If not, delete it.
4. Open the associated .RTD file, locate the job name in the eeey_groups and set the status to aborted or Completed. This allows the retention of data. If not, delete the RTD file.
5. Restart the RetinaEngine.

6. Delete the following files to place the scanner in a clean state for troubleshooting:

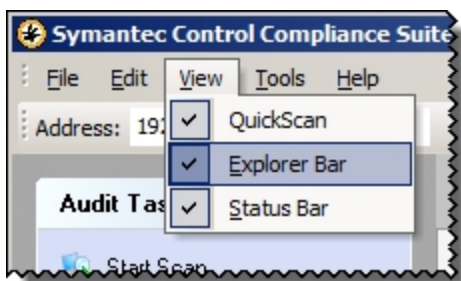
- CCS-VM Network Scanner\queue*.
- CCS-VM Network Scanner\targetlog.*
- CCS-VM Network Scanner\schedule.xml
- CCS-VM Network Scanner\jobs*.*
- CCS-VM Network Scanner\scans*.rtd
- CCS-VM Network Scanner\scans*.ldb
- CCS-VM Network Scanner\scans\scanrequests*.xml
- CCS-VM Network Scanner\scans\jobs*.xml
- CCS-VM Network Scanner\temp*.*
- CCS-VM Network Scanner\logs*.*

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

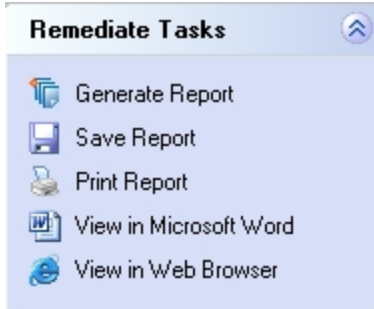
– **Sort Vulnerabilities By list** - Risk, Name

3. Select the specific vulnerabilities or machines.
4. Select the **Options** tab. The Options pane displays the section headings and creation details.

The screenshot shows the 'Options' tab within a configuration pane. The pane has a 'Filter' section with 'Options' selected. Below this is a 'Generate' button. The main area is divided into three sections: 'Include', 'Creation Details', and 'Include by Risk'. The 'Include' section has five checkboxes: 'Page breaks' (checked), 'Confidentiality page' (checked), 'Expand URLs (for printing)' (checked), 'Notes area after each section' (checked), and 'Detailed Audit Status' (unchecked). The 'Job Metrics' checkbox is also checked. The 'Creation Details' section has an 'Include creation details page' checkbox (unchecked), a 'Report created by:' text box, and a 'Report created for:' text box. The 'Include by Risk' section has three checkboxes: 'Information' (checked), 'Low' (checked), and 'Medium' (checked). The 'High' checkbox is unchecked.

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:

NAME: .NET Security Feature Bypass (3141780) - 3135988 .NET 3.5.1					
AUDITID: 57467	RISK: High	SEV CODE: Category-II	CVSS SCORE (V2): 10.0	EXPLOIT: No	PCI STATUS: Fail
CATEGORY:	Windows				
DESCRIPTION:	This security update resolves a vulnerability in Microsoft .NET Framework. The security feature bypass exists in a .NET component that does not properly validate certain elements of a signed XML document.				
FIX:	Update the affected packages to the versions specified in Microsoft .NET Framework Security Feature Bypass (3141780)				
SEV CODE:	Category II				
PCI COMPLIANCE:	SEVERITY LEVEL	COMPLIANCE STATUS		REASON	
	High	Fail		CVSS Score	
CVSS SCORE:	VERSION	ID	SCORE	VECTORS	
	CVSS 2	CVE-2016-0132	10.0	[AV:N/AC:L/Au:N/C:C/I:C/	
RELATED LINKS:	Microsoft Security Bulletin MS16-035 3141780				
CVE: CVSS SCORE (V2/V3)	CVE-2016-0132 (10.0)				

Using CVSS Scores

The scanner 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.
- Non-compliant report details assets that are vulnerable to any IAVA alert.
- Regulatory compliance report ensures assets meet compliance.
- Access report lists assets that are inaccessible.
- PCI Compliance report details the vulnerability results of PCI security scans.
- Dashboard report provides a high-level overview of a scan.

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.

Configuration				
Type				
Options				
Include				
<input checked="" type="checkbox"/> NetBIOS Name	<input checked="" type="checkbox"/> Operating System	<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> CVE	<input checked="" type="checkbox"/> Finding Date
<input checked="" type="checkbox"/> DNS Name	<input checked="" type="checkbox"/> CPE	<input checked="" type="checkbox"/> Risk Level	<input checked="" type="checkbox"/> CCE	<input checked="" type="checkbox"/> IAV
<input checked="" type="checkbox"/> NetBIOS Domain	<input checked="" type="checkbox"/> Job Metrics	<input checked="" type="checkbox"/> PCI Level	<input checked="" type="checkbox"/> CWE	
<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> Audit ID	<input checked="" type="checkbox"/> CVSS Score	<input checked="" type="checkbox"/> Exploit	<input checked="" type="checkbox"/> Sev Code
<input checked="" type="checkbox"/> MAC Address	<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Fix Information	<input checked="" type="checkbox"/> Context	

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 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 PCI Compliance Reports

Payment Card Industry Data Security Standard (PCI DSS) specifies security requirements for merchants and service providers that store, process, or transmit cardholder data. PCI Security Scans are run over the Internet by an Approved Scanning Vendor (ASV). The PCI requires all Internet-facing IP addresses to be scanned for vulnerabilities.

CCS-VM Network Scanner supports PCI DSS 1.1, 1.2 and 2.0 scoring. In version 1.2 severity levels are High, Medium, and Low. Each severity level corresponds to a range of CVSS scores. The scan passes or fails based on the CVSS score.

Severity Level Description

Severity	CVSS Score	Scan Status
High	7 - 10	Fail
Medium	4 - 6.9	Fail
Low	0 - 3.9	Pass

The PCI Compliance report contains the following information:

- A summary section that displays the vulnerability, sorted by severity then maximum CVSS score. CVE-IDs are also included.
- A status of Fail or Pass.

- A vulnerability reference section that includes CVE-IDS, CVSS scores, PCI severity, and PCI status.

To generate a report:

1. Select the **Report** tab.
2. From the Report Type list, select **PCI Compliance**.
3. Select **Options**. The Options pane is displayed.
4. In the Service Provider area, enter the company name and certificate number. Click **Modify** to add more information for the company.
5. In the Customer area, type the name of the company being scanned. Click **Modify** to add more information for the customer.
6. In the Include area, select the following:
 - **Attestation of Scan Compliance** - Select the check box to include an introduction that is required when submitting a report to the PCI Council.
 - **Special Notes per Target** - Select the check box to add a blank table to the report. Add special findings to the table that need to be addressed. Clear the check box to omit the table.
 - **PCI Self-Assessment Questionnaire** - Select the check box to include the self-assessment questionnaire.

The questionnaire allows you or your customer to analyze the security based on the requirements included in the PCI Data Security Standard. The applicable questionnaire (A, B, C, C-VT or D) depends on how the organization handles sales transactions.

Click the **More Info** link to visit the PCI Security Standards web site.

The screenshot shows a web interface titled "Configuration". On the left, there is a sidebar with "Type" and "Options" tabs, and a "Generate" button at the bottom. The main area is divided into three sections: "Service Provider", "Customer", and "Include". The "Service Provider" section has input fields for "Company Name" and "Certificate Number", each with a "Modify" button. The "Customer" section has a "Company Name" input field with a "Modify" button. The "Include" section contains three checkboxes: "Attestation of Scan Compliance" (checked), "Special Notes per Target" (checked), and "PCI Self-Assessment Questionnaire" (unchecked). To the right of the "PCI Self-Assessment Questionnaire" checkbox is a "More Info" link. Below the checkboxes is a dropdown menu.

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.

Adding Your Logo to PCI Compliance Reports

You can replace the logo on the title page of the PCI Compliance report with your company logo. The image must be in a .jpg format. The image size can vary; however, as a guideline, the default logo is 400 x 260 pixels.

To print your logo on the report:

1. Access the following directory:
%CCS-VM%\Database\Reports\Templates\PCISCompliance\assets
2. Replace the provider_logo.jpg file with your image file.
The new logo is displayed the next time you run the PCI report.

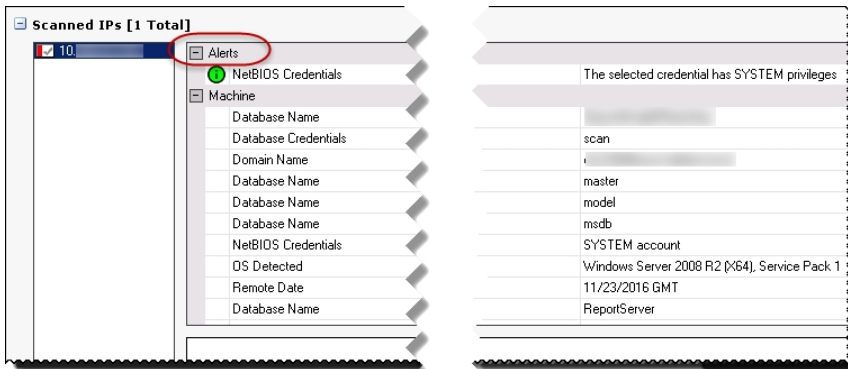
Running a Dashboard Report

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.

Running an Alert Report

Displays alerts detected on an asset. Alerts are organized in the report by asset.

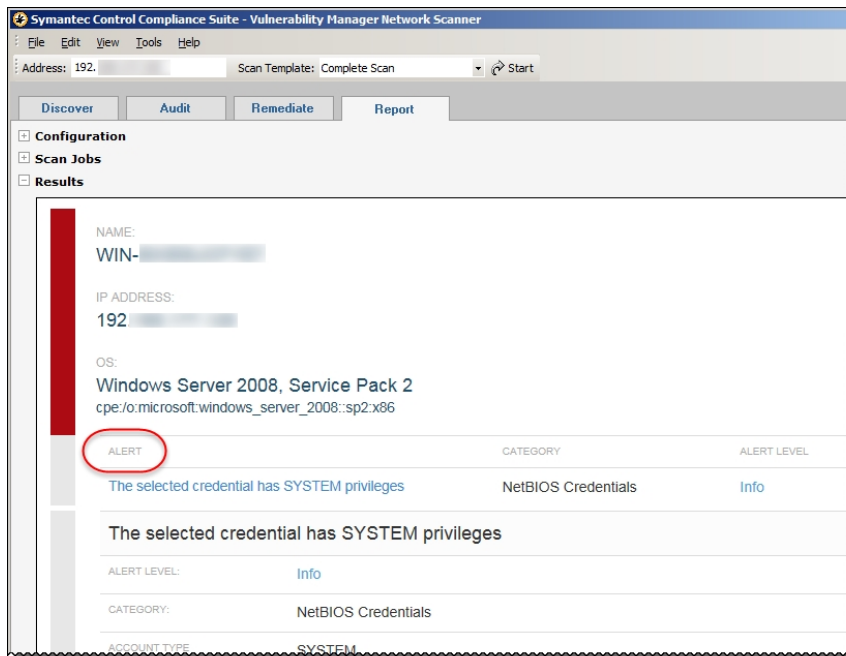
The scan results indicate if alerts are detected on an asset:



To generate an alert report:

1. Select the **Report** tab.
2. From the Report Type list, select **Alert**.
3. Click **Generate**.

The following screen capture shows an example of an alert.



Customizing Reports

You can change the presentation of reports. You can customize the product title, logo, colors, and PCI logo.

A logo image must be in a .jpg format.

To change the report presentation:

1. Select **Tools > Customize Reports**.
2. Change the default values to your preferences, and then click **OK**.
Click **Reset** to change customizations to the default settings.

Customizing Audits

You can customize existing audits, create new audits or write custom audit modules to meet the needs of your network security.

Customized audits will be overwritten by customized audits created from the centralized console.

Audit types are:

- **Customizable Audits** – Displays audits that can be modified.
- **Modified Audits** – Displays audits that you modified.
- **User Created Audits** – Displays audits defined using the Audit wizard.

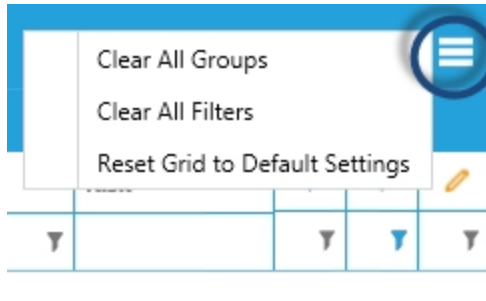


Before modifying the audit parameters, research the details associated with a vulnerability. Modifying audit parameters could impact the accuracy of the scans.

To customize audit settings:

1. In the main toolbar, select **Tools > Customize Audits**. The Audit Customization window is displayed.
2. You can filter the audit type.

Note: You can refresh the Audit Customization window at any time. Select Clear All Groups, Clear All Filters, or Reset Grid to Default Settings.



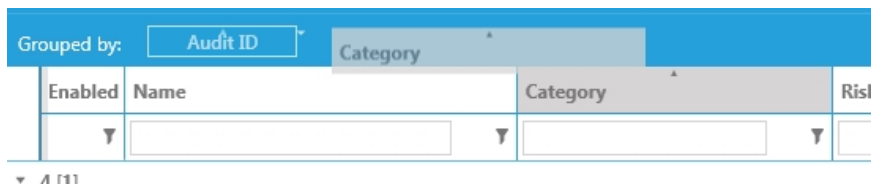
Searching the Audit Database

You can search the audit database for specific risk levels, categories or audit groups.

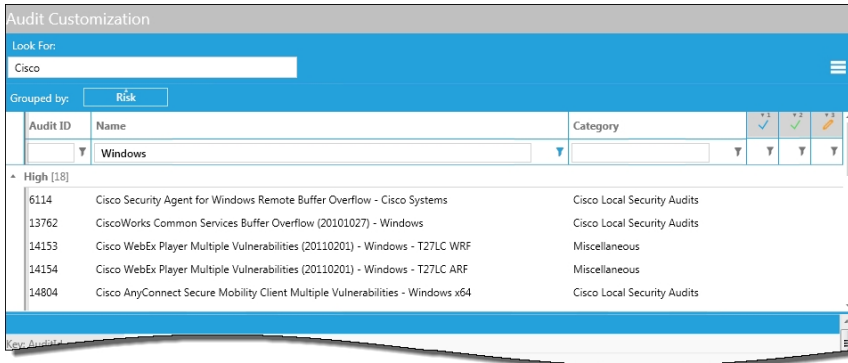
To search the audit database:

1. Enter search text in the **Look For** box.
The results display audits containing any portion of the search criteria.
2. Depending on your search, enter filtering parameters for the following columns: Audit ID, Name, Category, Risk, and Modified.
3. To group the search parameters, move the header columns to the area above the columns.

Click the heading name to change the sort order.



The following example shows Cisco audits grouped by Risk that include Windows in the name.



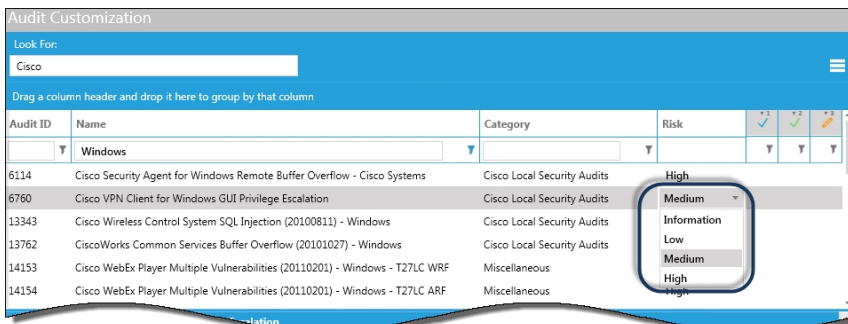
Changing Risk Levels

The risk levels correspond to the severity of the vulnerability detected. These risk levels are:

- **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.

To change the risk level:

1. On the Audit Customization window, select the audit, then select the **Risk** column.



2. Select the new risk level.
3. To save the settings, click **Close**.

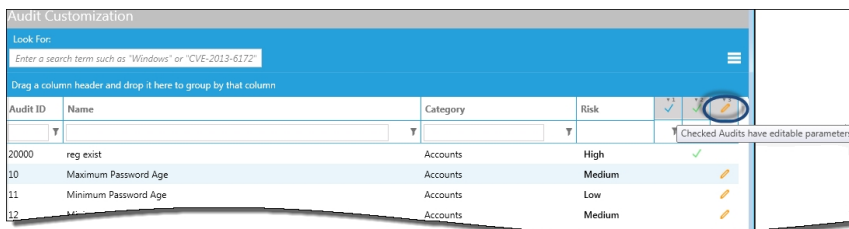
Modifying Customizable Settings

You can modify the audit parameters, such as risk level, password length and paths, of specific CCS-VM Network Scanner audits. You can generate a Customized Audits Report that describes audits that were changed from the default value. The report lists the current modified value and default value for audit parameters, such as risk level, password length and paths.

Note: Before modifying the audit parameters, research the details associated with the vulnerability. Modifying audit parameters could impact the accuracy of the scans.

To customize an audit:

1. On the Audit Customization window, click the edit button. The audits that can be customized are displayed.



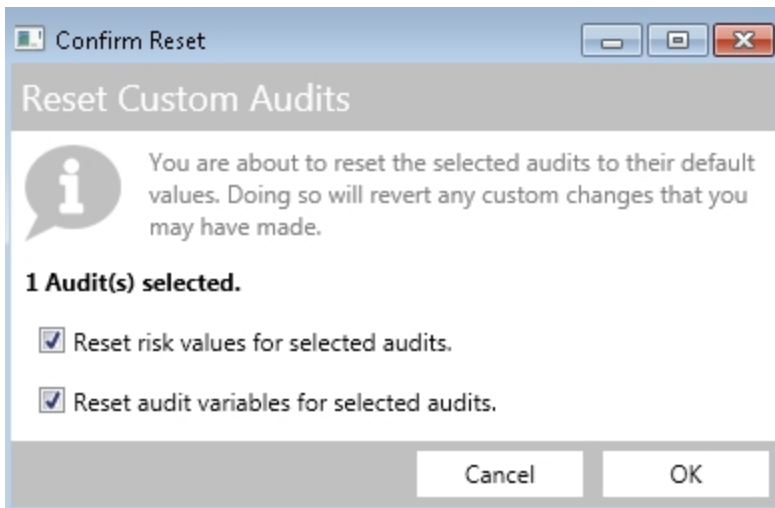
2. Select the audit, then click **Edit**.
You can also double-click the audit. You cannot change the description and default value properties.
3. Enter a new value.
4. Click **OK**. The Audit Customization window is displayed. The Audit Details section will not change.
5. To verify the audit customization, click **Report**. The Customized Audits Report is displayed. All audit changes are displayed in the Customized Values section. The Audit Details section will not change.
6. To save changes, click **Close**.

Resetting Audits to Default Values

If you change values on the Audit Customization window for a particular audit, you can reset the value later to the default value.

To change audits to the default settings:

1. On the Audit Customization window, select an audit.
2. Click **Reset**. The Reset Audits message indicates the number of audits that you selected.



3. The check boxes are selected by default. To retain the current settings for risk levels or audit variables, clear the respective check box.
4. Click **OK**. The audits are reset to the default values.

Running Audit Customization Reports

The Customized Audit report describes audits that were changed from the default values.

The report details the current modified value and default value for the audit parameters, including risk level.

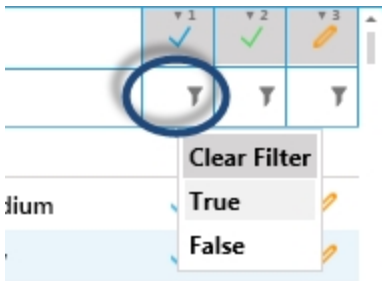
To view a report:

1. On the Audit Customization window, click **Report**. The report displays in a web browser window.

Viewing Modified Audits

To view modified audits:

1. Select **Tools > Customize Audits**.
2. On the Audit Customization window, select the **True** filter in the Modified column.



All audits changed are displayed.

Audit ID	Name	Category	Risk	✓ 1	✓ 2	✎ 3
10	Maximum Password Age	Accounts	Medium	✓	✎	
11	Minimum Password Age	Accounts	Low	✓	✎	

To display all audits again, select **Clear Filter**.

If needed, select audits and click **Reset**. Default values are restored.

Creating Custom Audits

You can create audits by selecting criteria from multiple categories, such as protocols, servers and services, then including the audits in the scan process and running against specified targets.

You can run the audits against specific software versions, CGI scripts, patches and registry entries.

You can only add one audit at a time. Audits are updated automatically after a custom audit is added.

To create an audit:

1. In the toolbar, select **Tools > Audits Wizard**.
2. Click **Next**.
3. Type the audit name. An audit name is required. This name displays in the Audit Groups after the database is updated.
4. From the Category list, select an audit category, such as Database, Mail Servers, Miscellaneous or Windows.
5. From the Risk Level list, select the severity level that corresponds to the severity of the vulnerability:
 - **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.
6. In the Vulnerability Description box, describe the vulnerability.
7. In the Vulnerability Fix box, describe how to remediate, investigate or mitigate the vulnerability.
8. Click **Next**. The Audit Type page displays.
9. Select the type of audit, and then click **Next**:
 - **Banner** - Determines vulnerabilities by scanning the banner information, such as firewall name, IP addresses and server name.
 - **CGI Script** - Determines vulnerabilities by scanning the common gateway interface that passes a Web user's request to an application program and to receive data back to forward to the user.
 - **Registry** - Detects vulnerabilities by scanning registry entries and values.
 - **Service Pack - Hotfix** – Determines vulnerabilities by scanning service packs, hotfixes and patches.
 - **File Version** - Verifies the software version.
 - **File Checksum** - Determines vulnerabilities based on file checksum comparisons. Supported values include: MD5, SHA1, SHA256. Network performance issues might occur if you use this feature. Use this feature with caution.
 - **Remote Check** - Verifies if a specific Unix program or patch is installed on an operating system.

The Audit Details page displays parameters based on the audit type that you select in step 9.

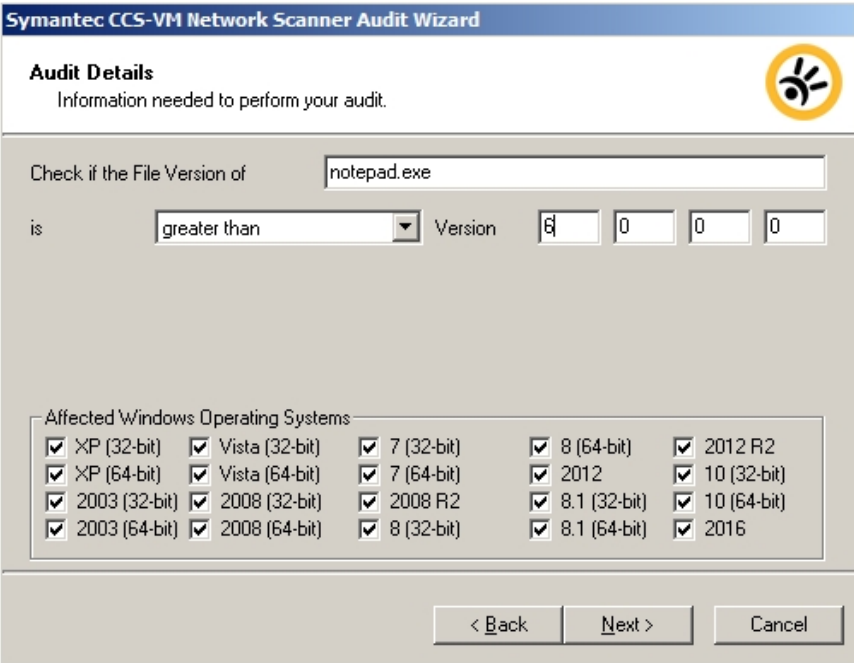
10. Enter the information for the audit type, and then click **Next**.
 - **Banner Audit Details** - Select the Banner protocol, and then type the banner name.
 - **CGI Script audit details** - Type the URL path to the script name. Select the Path, Key, or Value from the menu.
 - **Registry** - Select the OS that the vulnerability affects. Note that the registry path cannot contain the selected Hive value.

The screenshot shows the 'Audit Details' window of the Symantec CCS-VM Network Scanner Audit Wizard. The title bar reads 'Symantec CCS-VM Network Scanner Audit Wizard'. The main heading is 'Audit Details' with the subtitle 'Information needed to perform your audit.' and a yellow icon with a hand. The form contains the following fields and options:

- A text field: 'The system is considered vulnerable if the following registry' followed by a dropdown menu set to 'Path' and another dropdown set to 'does not exist'.
- A label 'Hive:' followed by a dropdown menu set to 'HKEY_CLASSES_ROOT'.
- A label 'Registry Path:' followed by a text input field.
- A label 'Registry Key:' followed by a text input field.
- A label 'Registry Value:' followed by a text input field.
- A section titled 'Affected Windows Operating Systems' containing a grid of checkboxes for various OS versions and architectures. All checkboxes are checked.
- At the bottom, three buttons: '< Back', 'Next >', and 'Cancel'.

<input checked="" type="checkbox"/> XP (32-bit)	<input checked="" type="checkbox"/> Vista (32-bit)	<input checked="" type="checkbox"/> 7 (32-bit)	<input checked="" type="checkbox"/> 8 (64-bit)	<input checked="" type="checkbox"/> 2012 R2
<input checked="" type="checkbox"/> XP (64-bit)	<input checked="" type="checkbox"/> Vista (64-bit)	<input checked="" type="checkbox"/> 7 (64-bit)	<input checked="" type="checkbox"/> 2012	<input checked="" type="checkbox"/> 10 (32-bit)
<input checked="" type="checkbox"/> 2003 (32-bit)	<input checked="" type="checkbox"/> 2008 (32-bit)	<input checked="" type="checkbox"/> 2008 R2	<input checked="" type="checkbox"/> 8.1 (32-bit)	<input checked="" type="checkbox"/> 10 (64-bit)
<input checked="" type="checkbox"/> 2003 (64-bit)	<input checked="" type="checkbox"/> 2008 (64-bit)	<input checked="" type="checkbox"/> 8 (32-bit)	<input checked="" type="checkbox"/> 8.1 (64-bit)	<input checked="" type="checkbox"/> 2016

- **Service Pack - Hotfix** - Determines vulnerabilities by scanning service packs, hotfixes, and patches.
- **File version** - Verifies the software version.



Symantec CCS-VM Network Scanner Audit Wizard

Audit Details
Information needed to perform your audit.

Check if the File Version of is Version

Affected Windows Operating Systems

<input checked="" type="checkbox"/> XP (32-bit)	<input checked="" type="checkbox"/> Vista (32-bit)	<input checked="" type="checkbox"/> 7 (32-bit)	<input checked="" type="checkbox"/> 8 (64-bit)	<input checked="" type="checkbox"/> 2012 R2
<input checked="" type="checkbox"/> XP (64-bit)	<input checked="" type="checkbox"/> Vista (64-bit)	<input checked="" type="checkbox"/> 7 (64-bit)	<input checked="" type="checkbox"/> 2012	<input checked="" type="checkbox"/> 10 (32-bit)
<input checked="" type="checkbox"/> 2003 (32-bit)	<input checked="" type="checkbox"/> 2008 (32-bit)	<input checked="" type="checkbox"/> 2008 R2	<input checked="" type="checkbox"/> 8.1 (32-bit)	<input checked="" type="checkbox"/> 10 (64-bit)
<input checked="" type="checkbox"/> 2003 (64-bit)	<input checked="" type="checkbox"/> 2008 (64-bit)	<input checked="" type="checkbox"/> 8 (32-bit)	<input checked="" type="checkbox"/> 8.1 (64-bit)	<input checked="" type="checkbox"/> 2016

< Back Next > Cancel

- **File Checksum** - Select the file checksum from the list.
Enter a file name, checksum value, and file version. Use an asterisk (*) to compare all file versions.
 - **Remote Check** - Verifies if a specific Unix program or patch is installed on an operating system.
11. On the Vulnerabilities page, enter the BugTraq ID, CVE ID, or CCE ID.
Enter the web site that provides solutions and more information for the vulnerability.
Entering information on this page is optional.
Some audits include BugTraq, CVE, and CCE information. Access the information later on the Audit Groups window.

Audit Group Modification

Audit Group: All Audits New Delete ☒ Auto

AUDIT CVE BID IAVA

Look For:

Drag a column header and drop it here to group by that column

Enabled	Audit ID	Name	Category
<input checked="" type="checkbox"/>	15276	FortiMail Multiple Vulnerabilities (20110913) (Zero-Day)	Web Application
<input checked="" type="checkbox"/>	1149	IMail arbitrary file deletion vulnerability	Mail Servers
<input checked="" type="checkbox"/>	1159	IMail arbitrary mailbox access	Mail Servers

Related Links: [Download patches or the latest version of IMail](#)

CVE: CVE-2000-0780

Exploits: CVE-ID: CVE-2000-0780 Exploit Database: Yes Core Imp: No

Bugtraq ID: 1617

Dependencies: Ports: Options:

Reset

12. Click **Next**.

13. Click **Finish**.

The audits database is updated with the new audit information.

Your custom audit is enabled in all CCS-VM Network Scanner Audit Groups with the **Automatically enable new audits in this group** option checked. You can verify the audits in the Audit Groups window.

For more information, see [Modifying Audit Groups](#).

Updating the Scanner Database

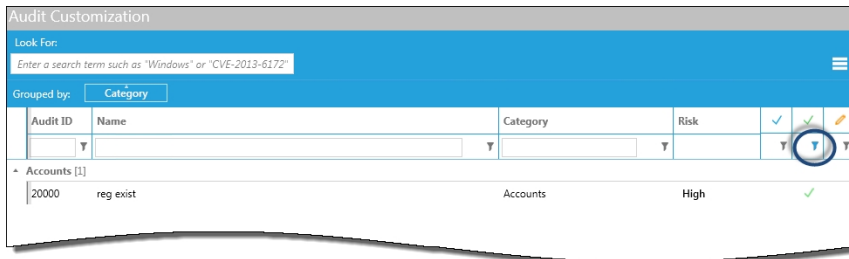
To update the database:

1. On the CCS-VM Network Scanner home page, select **Tools > Updates**. If enabled, a message displays stating Auto Update will close CCS-VM Network Scanner.
2. Click **Yes**. Auto Update displays.
3. Click **Next**. The Downloading window displays and the updates begin. The Update Summary window displays.
4. Click **Finish**. CCS-VM Network Scanner launches. You can verify your audit customizations using the Audit Group tool.

Viewing Custom User Created Audits

To view the audits that you created:

1. On the CCS-VM Network Scanner home page, select **Tools > Customize Audits**.
2. Select the **True** filter in the custom audit column. The audits that you created display.



3. To delete the audit, select the audit, then click **Delete**.
4. To run a report, click **Report**.
The report provides details on any audits that have been changed from the original. User created audits are also included.
5. To save any changes, click **Close**.
6. To exit without saving changes, click **Reset**. Reset only applies to the selected row.
Note that Reset is not available for user created audits.

To display all audits again, select **Clear Filter** in the custom audit column.

Modifying Audit Groups

You can view the audit groups and verify the audit details, such as description, risk level and dependencies. In addition, you can view audit groups by type.

To access audit groups:

1. In the toolbar, select **Tools > Audit Groups**. The Audit Group Modification window is displayed.
2. Select a tab to view the audit type: **Audit**, **CVE**, **BID**.
3. Click **New** to add a group and enter the audit group name.
4. Click **OK**. The name is displayed in the Audit Group list.
5. To update this group automatically, select **Automatically enable new audits in this group**.

6. Select one of the following tabs to select the audits to include in the audit group: Audit, CVE, BID.

Select the Audit tab to display all audits.

7. Set or change the audit parameters.
8. Click **Close** to save the settings.

Click **Reset**. All audits associated with the selected audit group are reset. Settings are reverted to the version provided by Symantec (either the default version or auto-update version). This feature is only available for audit groups provided by Symantec.

Exporting Audits

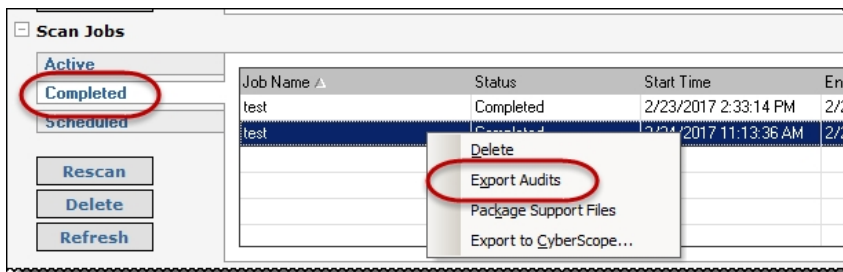
You can export audits associated with a selected scan to a CSV file. The export file provides information about the audits included in the scan (for example, audit ID, audit name, risk level).

You cannot export audit results from an XCCDF scan or Discovery scan.

To export audits:

1. Select the **Audits** tab, and then select the **Completed** tab.
2. Select a scan. The scan status must be Completed or Aborted.
3. Select **Tools > Export Audits**.

Alternatively, right-click the job name and select **Export Audits**.



4. Select a file location, and then enter a file name.
5. Click **Save**.

Creating Custom Audit Modules

You can write, add, modify and delete custom audit modules written using the CCS-VM Network ScannerAPI.

Note: For more information on the API, refer to the CCS-VM Network Scanner API documentation. The default location is %CCS-VM Network Scanner%\Help\Api.

To add a custom audit module:

1. On the CCS-VM Network Scanner home page, select **Tools > Plugins Wizard**. The Module plugin wizard starts.
2. Click **Next**. The Action Select page displays.
3. Select **Add Module**, then click **Next**. The Module Details page displays.
4. In the Module Name box, click **Browse** to select a file.
5. In the Description box, describe the module.
6. Select or clear the **Enabled** check box.
7. Select or clear the **Run module only if specified protocol or port is detected** check box, then select the protocol and enter the ports.
8. If the module always runs during every scan on the local system, select the **Always Run** check box.
9. Click **Next**. The Summary page displays.
10. Click **Finish**.
11. To restart the scanner engine now, click **Yes**.

Editing Custom Audit Modules

You can change the properties for your custom audit modules. You can also delete a custom audit module when it is no longer required.

To edit or delete custom audit modules:

1. On the CCS-VM Network Scanner home page, select **Tools > Plug-in Wizard**. The CCS-VM Network Scanner Module Plugin wizard displays.
2. Click **Next**. The Action Select window displays.
3. Select **Edit Module**, and then click **Next**.
 - a. Select the module, then click **Next**. The Module Details window displays.
 - b. Change the audit properties, and then click **Next**.
 - c. Review the settings, and then go to step 5.
4. Select **Remove Module**, and then click **Next**.

- a. Select the module to remove, and then click **Next**.
 - b. Review the settings, and then go to step 5.
5. Click **Finish**.
6. To restart the scanner engine now, click **Yes**.

Exploiting Vulnerabilities

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.

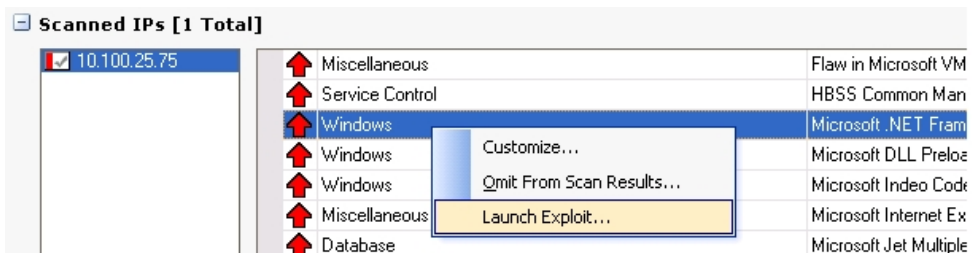
CVE-ID	Exploit Database	Core Impact	CANVAS	Metasploit	Microsoft Exploitability Index
CVE-2010-0249	Yes	Yes	No	Yes	1 - Consistent exploit code likely

Exploiting a Vulnerability

Integrating Metasploit with CCS-VM Network Scanner, 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.

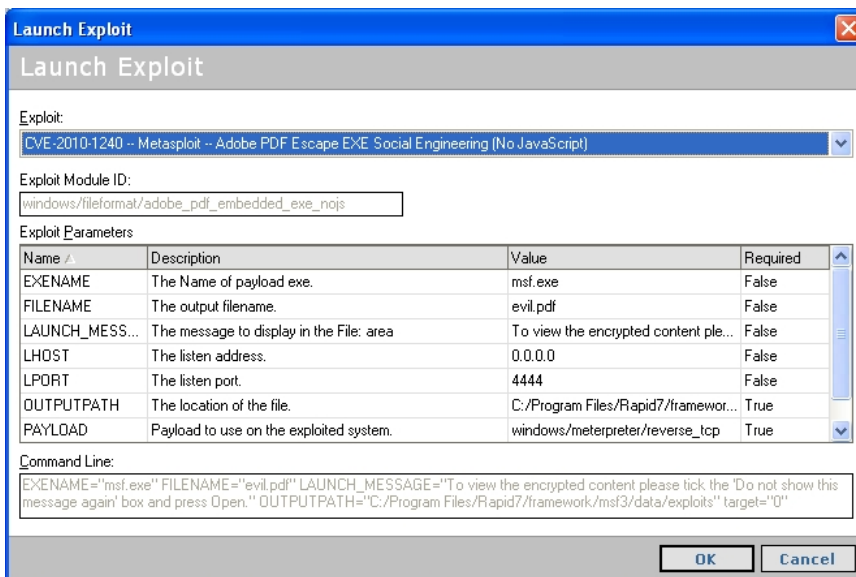
To exploit a vulnerability:

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 CCS-VM Network Scanner. This saves time when loading exploits.

To integrate Metasploit with CCS-VM Network Scanner:

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**.

OS Fingerprinting

You can run a wizard to capture the TCP fingerprint for a selected IP address.

Updating TCP OS Fingerprints

You can change TCP OS fingerprints.

To modify TCP OS fingerprints:

1. On the Audit page, right-click a completed IP address to display the submenu, then select **Update OS Fingerprint**.

Or

Select **Update OS Fingerprints** on the Tasks pane.

The CCS-VM Network Scanner OS Fingerprint Wizard displays.

2. Click **Next**. The Operating System Selection window displays.
3. To select an existing fingerprint, select the **One of the detected operating systems is correct** check box, then select the operating system and click **Next**.
4. To enter a new fingerprint, select the **None of the detected operating systems are correct** check box, then click **Next**. The Operating System Details window displays.
5. Enter the operating system identification, such as description, vendor, application name, version and revision.
6. To email the fingerprint to **Symantec**, select the **Email Fingerprint to Symantec** check box. Your email client launches and mails the fingerprint to ret-os-fingerprint@Symantec.com.

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**.

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 CCS-VM Network Scanner 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 CCS-VM Network Scanner, copy its SCAP Data Stream Content (such as FDCC checklists) to the CCS-VM Network Scanner benchmarks directory.

The default directory is:

C:\Program Files\Symantec\CCS-VM Network Scanner\Database\XCCDF\benchmarks

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 CCS-VM Network Scanner 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 CCS-VM Network Scanner 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.com 10.202.6.0/24”.
 - **Single IP (IPv6)** - Enter a single IPv6 address.
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 %CCS-VM Network Scanner%\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**.

Setting 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.
 - **Event Routing** - enable event logging and specify the audits to log.
 - **Scanner** - modify the scan engine performance and set ping and data timeout values.
 - **Management** - enable Central Policy and set policy parameters.

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

Generating Log Files

CCS-VM Network Scanner generates log files, including:

- RetinaStatus.log
- RetinaUI.log

The log files are saved to %CCS-VM Network Scanner%\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 CCS-VM Network Scanneroperations** 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**- Set the number of seconds to wait before starting the updater.
4. Click **OK**.

Enabling Event Routing

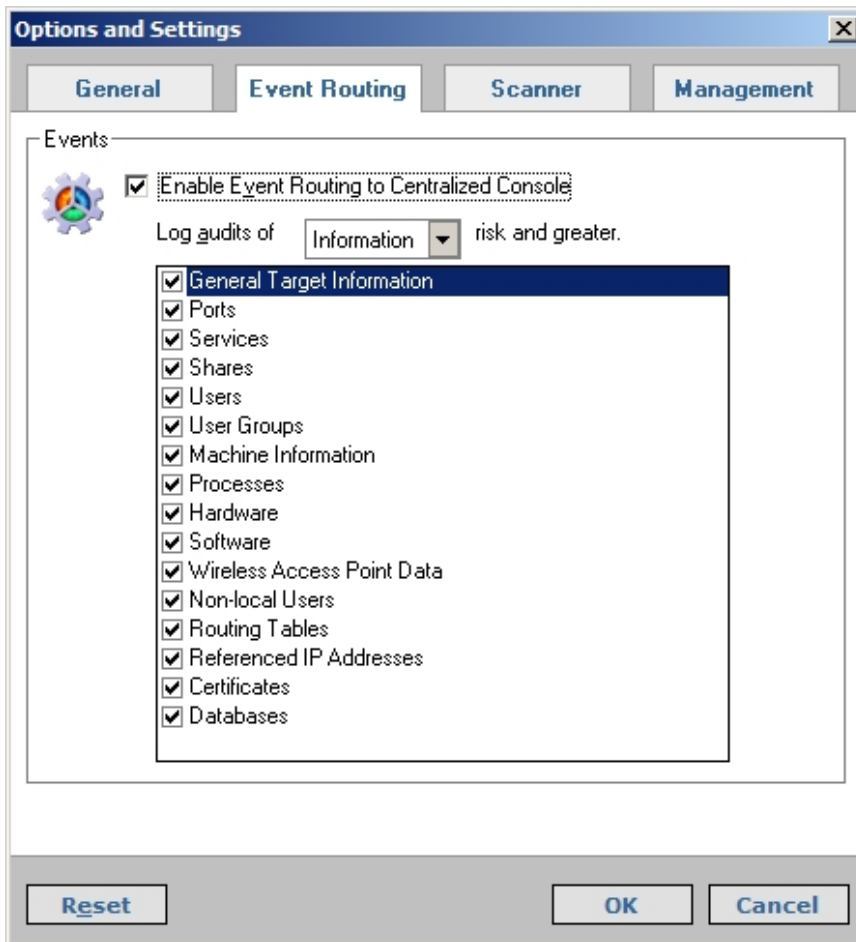
Event routing enables CCS-VM Network Scanner to send the scan data, such as port, services and general scan information, to a centralized console. You can view the information on the centralized console.

Note: If you are managing scans using a centralized console, you must enable event routing.

To enable event routing:

1. Select **Tools > Options**.
2. Select the **Event Routing** tab.
3. Select the **Enable Event Routing to Centralized Console** check box.

4. From the **Log Audits of [information] Risk and Greater** list, select the risk level. Audits contain a risk level that corresponds to the severity of the vulnerability detected. Selecting Information causes all risk levels to be logged. These risk levels are:
 - **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.
5. Select the check boxes for the log categories to include.



6. 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 the scanner 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 the scanner to compensate for network latency.

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

If the scanner 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**.

Setting Scan Restrictions

You can configure time based scan restrictions. Set scan restrictions on a global level or job level.

Configure scan restrictions at the job level on the Schedule tab. For more information, see [Scheduling Scans](#).

To set a scan restriction on all scans:

1. Select **Tools > Options**.
2. Click the **Scanner** tab.
3. Select the **Enable global scan restrictions** check box, and then click **Configure**.
4. Click the squares to set the restricted time frame.
5. Select the check box to allow job level scan restrictions.
6. If a scan is running when a scan restriction time starts, you can abort or pause the running scan. Select **Aborted** or **Paused**.
If you choose **Paused**, the scan resumes after the scan restriction ends.
7. Click **OK**.

Enabling Central Policy

Specifying a Central Policy allows a centralized console to manage CCS-VM Network Scanner remotely. You must enter the location of the centralized console server.

To specify a Central Policy:

1. Select **Tools > Options**.
2. Select the **Management** tab.
3. Select the **Enable Central Policy** check box.
Note that changes to customized audits are lost if you subscribe to Central Policy.
4. From the Central Policy Type list, select either **Version 1** or **Version 2**.
If you select **Version 1**, the minutes that pass before CCS-VM Network Scanner checks for policy updates is set at 15 minutes. The time cannot be changed.
Note: If the centralized console is on the same system, you can type localhost in the Central Policy Server box. The Password and Confirm Password boxes remain blank.
5. Enter the server name in the Central Policy Server box.
6. Type the password in the Password and Confirm password boxes.
7. Enter the agent name.

8. To test the connection, click **Test**.
9. Click **OK**.

Run Database Application Scans

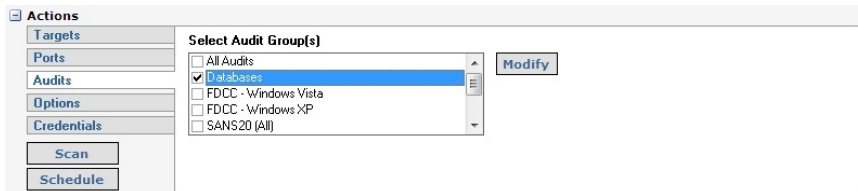
Database application scanning gives you the ability to scan Microsoft SQL Server, MySQL and Oracle databases for vulnerabilities.

Database application scanning is disabled by default. A complete scan of a remote database server may significantly increase the time required to audit a remote target.

Running Database Application Scans

To add database application auditing to your scan:














1. Select the **Audit** tab, and select **Options**.
2. Scroll through the list and select the **Perform Database Application Scanning** check box.
3. Select **Audits**.
4. Select the **Databases** check box.



5. On the Audit pane, click **Scan** to run the scan now.

Review Database Application Vulnerabilities

Database application vulnerabilities are treated as a standard vulnerability type. The vulnerabilities are displayed in the scan and report results in the same way as other vulnerabilities.

Audits		
	Database	SQL Insecure sp_createorphan Procedures and Permissio...
	Database	SQL Insecure sp_replcmds Procedures and Permissions D...
	Database	SQL Insecure sp_replsetsynstatus Procedures and Permiss...
	Database	SQL Insecure sp_replwritetovarbin Procedures and Permis...
	Database	SQL Insecure sp_resyncexecute Procedures and Permissi...
	Database	SQL Insecure sp_unprepare Procedures and Permissions ...
	Database	SQL xp_cmdshell Arbitrary Command Execution Vulnerability
	Database	SQL Accounts With Null Password Detected
	Database	SQL Database Mail XP Detected
	Database	SQL Database OLE Store Procedures Enabled Detected
	Database	SQL Does Not Enforce C2 Auditing Detected
	Database	SQL Insecure Cross DB Ownership Chaining Detected
	Database	SQL Insecure Password Policy Enforcement Detected

Preparing Database Applications for Scans

You can set your database applications as targets for scanning.

To ensure that your database can be successfully scanned by CCS-VM Network Scanner, review the following section on MySQL to prepare your database.

Preparing Your MySQL Database for Scans

Review your MySQL settings and ensure the following is in place:

- Verify the latest GA release of MySQL ODBC driver is installed on the scanner system.
 - Go to **Administrator tools**.
 - Run **Data Sources (ODBC)**.
 - Select the **Drivers** tab.
 - Search for the MySQL driver.

If no driver is found, then download and install the newest GA released MySQL driver from the MySQL website.
- Ensure a remote connection can be established to the target database using the 'mysql' tool provided in a MySQL database installation.

Running Retina from the Command Line

CCS-VM Network Scanner has two command line interfaces (CLI):

- Retina.exe
- Retina RPC client

In the following sections, %CCS-VM Network Scanner% is the Install Directory.

Retina.exe CLI Switches

Using the Retina.exe CLI, you can:

- Run a scan.
- Run a report.

The Retina.exe syntax is:

Retina.exe /<Option Name>

You do not need to specify the full path or file extension for an Addressgroup or Scantemplate.

Example:

C:\Program Files\Symantec\CCS-VM Network Scanner\ScanTemplates\CompleteScan.xml

This scan template only needs to be specified as /scantemplate="CompleteScan"

Addressgroups and Scantemplates referenced in the command line need to be valid XML files located in %CCS-VM Network Scanner%\Groups\Addresses and %CCS-VM Network Scanner%\ScanTemplates, respectively.

Parameter	Description
?	Display command line options.
lprange	Nmap-style IP range. Addressgroup overrides this value.

Parameter	Description
Addressgroup	Name of the address group file used in the scan. This value overrides iprange.
Scantemplate	Name of the scan template file used for the scan.
Outputfile	Name of output RTD file being generated. Use "*" to have the scanner auto-assign a name based on the current timestamp. DSN overrides this value.
DSN	Name of the DSN used for data storage. This value overrides outputfile.
Noupdate	Suppresses the launch of Sync-It.exe.
Quietmode	Suppresses all dialog boxes.
Minimize	Launches the scanner minimized to the system tray.
Policy	Name of the scan template file used for the scan. Identical to scantemplate.
Status	Name of the scanner scan status file.

Not Supported — report, hostoutputfile and activityid

Run Reports from the CLI

You can run reports from the CLI. The output types include HTML and XML.

Parameters

Run Retina.exe from the installation directory with the following parameters:

Retina /rpttype target rtd [jobname]

Parameter	Description
"rpttype"	rptdisc = Discovery rptexec = Executive rptrem = Remediation rptsum = Summary rptvuln = Vulnerability Report (HTML) rptacc = Access

Parameter	Description
	rptpci = PCI Compliance rptvulnxml = Vulnerability Export (XML) rptvulncsv = Vulnerability Export (CSV) rptreg = Regulatory Compliance
"target"	HTML output full path and filename, including extension. If spaces exist in the path, the target should display in quotes.
"rtd"	Full path and filename to the source RTD. If spaces exist in the path, the target should display in quotes. The rtd is not required for Discovery reports.
"jobname"	Name of the job in the RTD that generates a report. This is optional. If this is omitted or more than one job with that name exists within the RTD, then the latest job will be used as the source. If spaces exist in the path, the target should display in quotes. The jobname is not required for Discovery reports.

Examples

- Generating a summary report for the latest job in an RTD
 Retina /rptsum "c:\reports\summary\latest_job.html" "c:\program files\Symantec\CCS-VM Network Scanner\scans\latest.rtd"
- Generating a Discovery report
 Retina /rptdisc "c:\reports\discovery\latest_disc.html"
- Generating an Executive report for latest job named "WAN":
 Retina /rptexec "c:\reports\executive\WAN_exec.html" "c:\program files\Symantec\CCS-VM Network Scanner\scans\network.rtd" "WAN"

Retina.Report.Console.exe CLI

Retina.Report.Console.exe can be used to run Dashboard, PCI Compliance, Regulatory Compliance, Remediation, Vulnerability Export, XML Assessment, and Alert reports.

Note: The XML Assessment report is not available from within the user interface. It can only be created via the Retina.Report.Console.exe CLI.

Parameters

Parameter	Description
<ReportType>	Report type to be generated. Valid values include Compliance, Dashboard, PCI, Remediation, VulnerabilityExport, XmlAssessment, Alert, Executive, Discovery, Consolidated
-f --filename	Output file name prefix (no extension).
-j --jobid	OPTIONAL. JobId of scan.
-g --groupid	OPTIONAL. GroupId of scan.
-r --rtddfile	OPTIONAL. Name of results database (RTD) file.
-s --scanname	OPTIONAL. Name of scan job.
-x --xmloptions	OPTIONAL. Full path to options XML file.
-d --details	OPTIONAL. Include detailed audit status.
-d --related descriptions	OPTIONAL. Include related descriptions.
-d --console	OPTIONAL. Output the details of the report to the console.
-p --pdf	OPTIONAL. Output the report to a PDF file.

Note: For examples of XML options file, refer to the sample files which are located by default in C:\Program Files\Symantec\CCS-VM Network Scanner\Reports\Options\Samples\

Examples

Generate a Remediation report from the “DailyScan” RTD file.

```
Retina.Report.Console.exe Remediation -r "DailyScan.rtd" -f  
"C:\Reports\RemediationReport.html"
```

Generate an XML assessment report via Job ID:

```
Retina.Report.Console.Exe XmlAssessment -j  
"1732F56FA0D94EB3BACEE662AE3CD93B"  
-f "c:\Reports\Xml\XmlAssessment.xml"
```

RetRPC_client.exe CLI

Using the RetRPC_client.exe CLI, you can:

- Run scans
- Monitor scan jobs
- Start, stop, and restart the Retina service
- Clean the job queue

The Retrpc_client.exe syntax is:

```
retrpc_client <command> <args>
```

Retrpc_client.exe returns no debug or other data to the command line; all errors and data are sent to the Retina logs.

Parameter	Description
StartScan <scan name>	Starts <scan name>, where <scan name> is the name of a scan request file in %CCS-VM Network Scanner%\Scans\ScanRequests. Scan requests have xml extensions.If <scan name> was previously scheduled, no action is taken. If <scan name> is an immediate job, the job is queued.The return text is in the format: Started scan <jobinstance>:<jobid> Started scan B7BBAEB8B8E34BDC9034AE88FE8ECEB3:4FF2FAA7D95B4034B03DA10E11AEF82B

Parameter	Description
StopScan <jobid>	Stops <jobid> where <jobid> is the name of a scan request file in %CCS-VM Network Scanner%\Scans\ScanRequests. Scan requests have xml extensions. If <jobid> is not running, no action is performed.
PauseScan <jobid>	Pauses <jobid> where <jobid> is the name of a scan request file in %CCS-VM Network Scanner%\Scans\ScanRequests. Scan requests have xml extensions. If <jobid> is not running, or paused, no action is performed.
UnpauseScan <jobid>	Continues <jobid> where <jobid> is the name of a scan request file in %CCS-VM Network Scanner%\Scans\ScanRequests. Scan requests have xml extensions. If <jobid> is not running, or not paused, no action is performed.
ModifySchedule <scan name>	Forces a change in the time of a scheduled job <scan name> where <scan name> is the name of a scan request file in %CCS-VM Network Scanner%\Scans\ScanRequests. Scan requests have xml extensions.
StopSchedule <jobid>	Deletes <scan name> where <scan name> is the name of a scan request file in %CCS-VM Network Scanner%\Scans\ScanRequests. Scan requests have xml extensions. Deletes all occurrences of <scan name> because it removes the scanrequest.
DelCredentials <description>	Deletes the credentials for <description>.

Parameter	Description
SetCredentials <user name><password> <description>	Creates a credential <user name> with password <password>. If <user name> exists, it is overwritten. If a credential is used here, it will be available in the CCS-VM Network Scanner UI.
GetEngineStatus [/num]	
GetJobStatus <[jobinstance]:jobid> [/num]	Returns the status of the specified job. jobid - The job to check the status of. /num - Optional parameter to return the numeric representation of the result: 1 Queued 2 Active 3 Complete 4 Pausing 5 Paused 6 Aborting 7 Aborted 8 Error The exit code of the program is set to the corresponding value of the status.
Config	Reinitializes the configuration values from %CCS-VM Network Scanner%\retinaconfig.xml.
WriteConfig <file name>	
TestREM <server> <password> <agent name> [WCF REM3]	
FixIt <audit id> <host ip> <credential name>	Performs a Fixit operation identified by <audit id> against host <host ip>. It can optionally use <credential name> to authenticate.
Stop	Stops the Retina service.

Parameter	Description
Start	Starts the Retina service.
Restart	Restarts the Retina service.
PipeClient	Acts as a simple pipe client by seeing all the xml output that the interface would see.
Dump [path]	Creates a dump snapshot of the engine in it's current state. path - Optional path for dump file. The default directory is CCS-VM Network Scannerlogs\Exceptions
Clean <Queue Schedule Logs Scans All>	Removes the following files: Queue file and stops all jobs Schedule files All RTD files All scan requests All scan jobs All temp files All log files

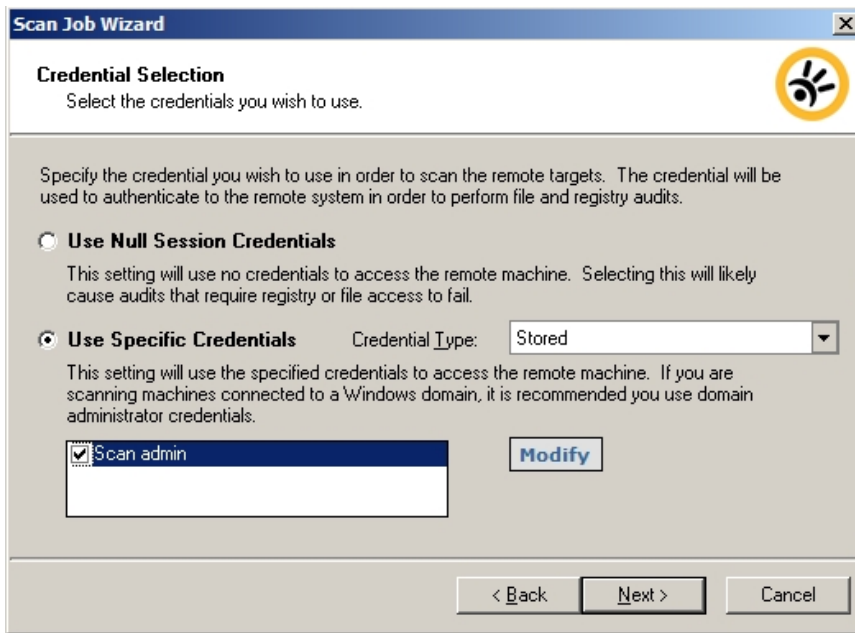
Starting a Scan from the CLI

Before you can run a scan from the RetRPC_client CLI, you must first create a scan. This scan generates a jobID that you need to run a scan from the CLI.

Use the following procedure to create a scan job.

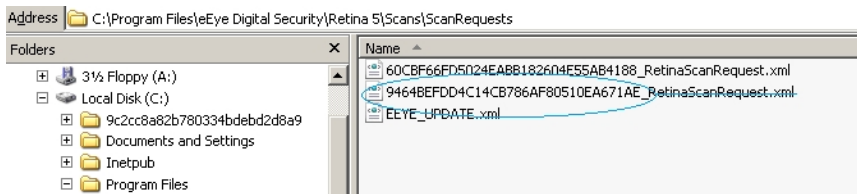
To create a scan:

1. Select **Tools > Scan Job Wizard**.
2. On the Target Selection page, select the target assets, and then click **Next**.
3. On the Credential Selection page, select **Use Specific Credentials**.
4. On the Credential Type list, select **Stored**.
5. Select the credentials to use for the scan, and then click **Next**.



6. Select port settings, and then click **Next**.
7. On the Audit Selection page, select **Custom Audit Settings**, select the audits to use for the scan, and then click **Next**.
8. On the Audit Selection page, select the audits, and then click **Next**.
9. On the Option Selection page, select scan settings. For more information, see [Selecting Audit Options](#).
10. On the Output Selection page, select **Database**, select the output DSN, and then click **Next**.
11. On the Details Selection page, enter a name for the scan job and select the check box **Save as a scan template**. Click **Next**.
12. On the Schedule Selection page, click **Next**. By default, Run Now is selected.
13. On the last page, click **Finish**. The job will run now.
14. To see the job ID, go to:
%CCS-VM Network Scanner%\Scans\ScanRequests\

A job ID, similar to the following, will be used in the command line for future scans. Do not include `_RetinaScanRequest` in the command line.



Name	Date modified
BD7A39364F8F478F9E3674859382B712_RetinaScanRequest	3/3/2017 3:08
B018F76F404E4BA1979BE965EE6413E3_RetinaScanRequest	3/3/2017 10:08
2449BB1C24C34D6EB21D540786A4C6CC_RetinaScanRequest	3/2/2017 4:08

Command Line Sample:

```
retrpc_client startscan "C:\Program Files\Symantec\CCS-VM Network  
Scanner\Scans\ScanRequests\<job_id>.xml"
```


Database and XML Schema

This appendix provides information about the database and XML schema.

RTD Schema

Table 1. eeeye_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 CCS-VM Network Scanner. Extensions will be added as modules are added to CCS-VM Network Scanner.
IP	String [255]	IP address of target being scanned.
RequesterIP	String [255]	Reserved for future use

Identifier	Field Type	Description
RequesterMac	String [255]	Reserved for future use

Table 2. eeeye_Alerts

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier for each scanned IP address.
ActivityID	String [32]	Link to eeeye_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. eeeye_AuditExtend

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier
ActivityID	String [32]	Link to eeeye_Activity:ID_
Audit_ID	String [32]	Link to eeeye_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.

Identifier	Field Type	Description
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 eeeye_activity:ID_
path1	String [255]	<p>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.</p> <p>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.</p>
path2	String [255]	Audit ID as referenced in audits.xml.
path3	String [255]	<p>Reference to RTH file. Contains Audits\<category>\<rth name>.rth. Integrators should not need this file.</p>
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. eeeye_Devices

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Links to eeeye_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. eeeye_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. eeeye_Hardware

Identifier	FieldType	Description
ID_	String [32]	Unique record identifier
ActivityID	String [32]	Link to eeeye_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”
ValueField	String [255]	Captured data, such as “CD-ROM Disc” or “CPU0”
Risk	Integer	Not Used

Table 8. eeeye_Machine

Identifier	Field Type	Description
ID_	String [32]	Unique record identifier
ActivityID	String [32]	Link to eeeye_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. eeeye_NoAudits

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

Table 10. eeeye_Ports

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeeye_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
path2	String [255]	<p>If blank, DisplayField and ValueField contain the port number and protocol.</p> <p>If State, ValueField expresses the port state as Open, Closed, or Filtered.</p> <p>If Version, ValueField contains the port banner.</p> <p>The meaning of the banner varies based on protocol.</p> <p>If HTTP services, the banner is the Server HTTP response header field.</p> <p>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.</p> <p>If FTP, SMTP, Telnet or miscellaneous, the banner is the greeting string sent back when CCS-VM Network Scanner connects to the service.</p>
path3	String	Not Used

Identifier	Field Type	Description
	[255]	
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. eeeye_Processes

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeeye_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. eeeye_Protocols

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeeye_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-response 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. eeeye_ReportNvp

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

Table 14. eeeye_Services

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

Identifer	Field Type	Description
ActivityID	String [32]	Link to eeeye_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.
Risk	Integer	Not Used

Table 15. eeeye_Shares

Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeeye_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. eeeye_Software

Identifier	Field Type	Description
Identifier	Field Type	Description
ID_	String [32]	Unique Record Identifier
ActivityID	String [32]	Link to eeeye_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 “Symantec CCS-VM”
Risk	Integer	Not Used

Table 17. eeeye_Users

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

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

Identifier	Field Type	Description
ActivityID	String [32]	Link to eeeye_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 eeeye_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 eeeye_Machine Entries

path1	path2	DisplayField	ValueField
zOpen		Open Ports	Displays the number of open TCP ports detected on the target device
OSDETECT		OS Detected	Scanner description of the machine's operating system

path1	path2	DisplayField	ValueField
			<p>Entries depend on how the OS was detected.</p> <ul style="list-style-type: none"> - Discovered using Windows registry, the registry information is entered. - 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 <CCS-VM Network ScannerInstallation>\Database\Reference\ICMPOSD_FP directory is entered. - Discovered using TCP fingerprinting, the string from the retfp file located in the <CCS-VM Network ScannerInstallation>\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

path1	path2	DisplayField	ValueField
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
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

path1	path2	DisplayField	ValueField
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

path2	ValueField
f1Homedrive	User's home drive
g1Logonserver	Name of server where logon requests are sent
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.