



# Comodo Forensic Analysis

Software Version 2.0

## Administrator Guide

Guide Version 2.0.120318

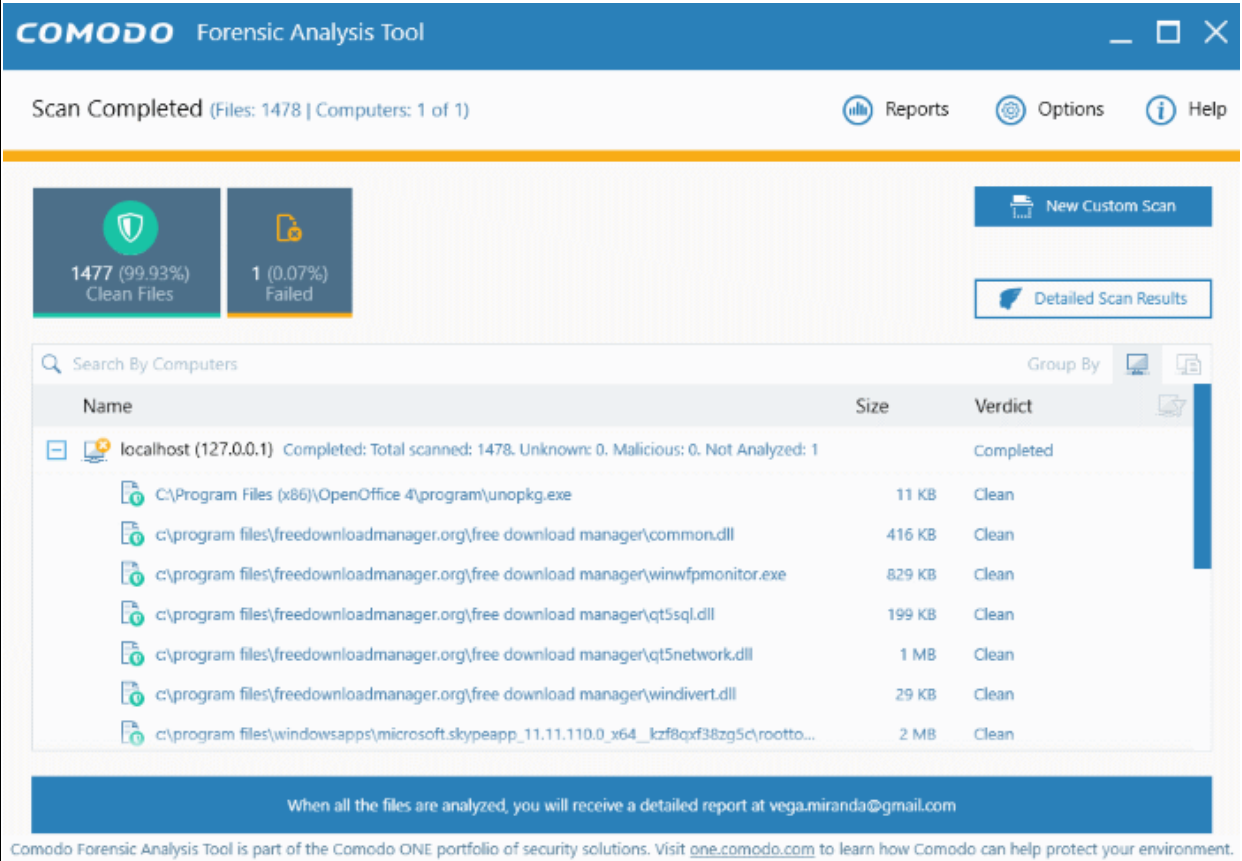
## Table of Contents

<b>1 Introduction to Comodo Forensic Analysis.....</b>	<b>3</b>
<b>2 Running Forensic Analysis .....</b>	<b>4</b>
2.1 The Main Interface.....	4
<b>3 Scanning Computers.....</b>	<b>6</b>
3.1 Scanning Computers using Active Directory.....	7
3.2 Scanning Computers using Workgroup.....	12
3.3 Scanning Computers by Network Addresses.....	17
3.4 Scanning Local Computer.....	21
<b>4 Scan Results.....</b>	<b>28</b>
<b>5 Reports.....</b>	<b>30</b>
5.1 Executive Valkyrie Report.....	31
5.2 Device Valkyrie Report.....	33
5.3 Program Valkyrie Report.....	33
<b>6 About Comodo Forensic Analysis.....</b>	<b>34</b>
<b>7 Agent Requirements.....</b>	<b>35</b>
<b>About Comodo Security Solutions.....</b>	<b>37</b>

# 1 Introduction to Comodo Forensic Analysis

It is estimated that traditional antivirus software can only catch 40% of all malware in the world today. The other 60% are 'unknown'. An advanced persistent threat (APT) is an 'Unknown' piece of malware that is so well disguised it can be months before a traditional anti-virus catches up to it. During this time, these malicious files continue to reside on the victim's computer, executing their payloads all the while.

Comodo Forensic Analysis (CFA) is a lightweight scanner which identifies unknown, and potentially malicious files, residing on your network. After scanning your systems, it will classify all audited files as 'Safe', 'Malicious' or 'Unknown'. While 'Safe' files are OK and 'Malicious' files should be deleted immediately, it is in the category of 'Unknown' that most zero-day threats are to be found. The CFA scanner automatically uploads these files to our Valkyrie servers where they will undergo a battery of run-time tests designed to reveal whether or not they are harmful. You can view a report of these tests in the CFA interface. You can also opt to have detailed scan reports sent to your email. The CFA interface displays results of both files analyzed by Forensic Analysis and Valkyrie analysis.



The screenshot displays the Comodo Forensic Analysis Tool interface. At the top, it shows 'Scan Completed (Files: 1478 | Computers: 1 of 1)'. Below this, there are two summary cards: '1477 (99.93%) Clean Files' and '1 (0.07%) Failed'. A 'New Custom Scan' button is visible in the top right. Below the summary cards, there is a search bar and a table of scan results. The table has columns for 'Name', 'Size', and 'Verdict'. The results show a list of files from 'localhost (127.0.0.1)' with various file names and sizes, all with a 'Clean' verdict. A footer message states: 'When all the files are analyzed, you will receive a detailed report at vega.miranda@gmail.com'. At the very bottom, a note says: 'Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment.'

Name	Size	Verdict
localhost (127.0.0.1) Completed: Total scanned: 1478. Unknown: 0. Malicious: 0. Not Analyzed: 1		
C:\Program Files (x86)\OpenOffice 4\program\unopkg.exe	11 KB	Clean
c:\program files\freedownloadmanager.org\free download manager\common.dll	416 KB	Clean
c:\program files\freedownloadmanager.org\free download manager\winwfpmoitor.exe	829 KB	Clean
c:\program files\freedownloadmanager.org\free download manager\qt5sql.dll	199 KB	Clean
c:\program files\freedownloadmanager.org\free download manager\qt5network.dll	1 MB	Clean
c:\program files\freedownloadmanager.org\free download manager\windivert.dll	29 KB	Clean
c:\program files\windowsapps\microsoft.skypeapp_11.11.110.0_x64_lkzf8qxf38zq5c\rootto...	2 MB	Clean

## Features

- No installation required, just run the portable application on any computer in the network
- Scan local machines or specify target endpoints by Active Directory, Work Group or network address
- Unknown files are automatically uploaded to Comodo Valkyrie and tested for malicious behavior
- Comprehensive reports provide granular details about the trust level of files on your endpoints

This guide is intended to take you through the use of Comodo FA and is broken down into the following main sections.

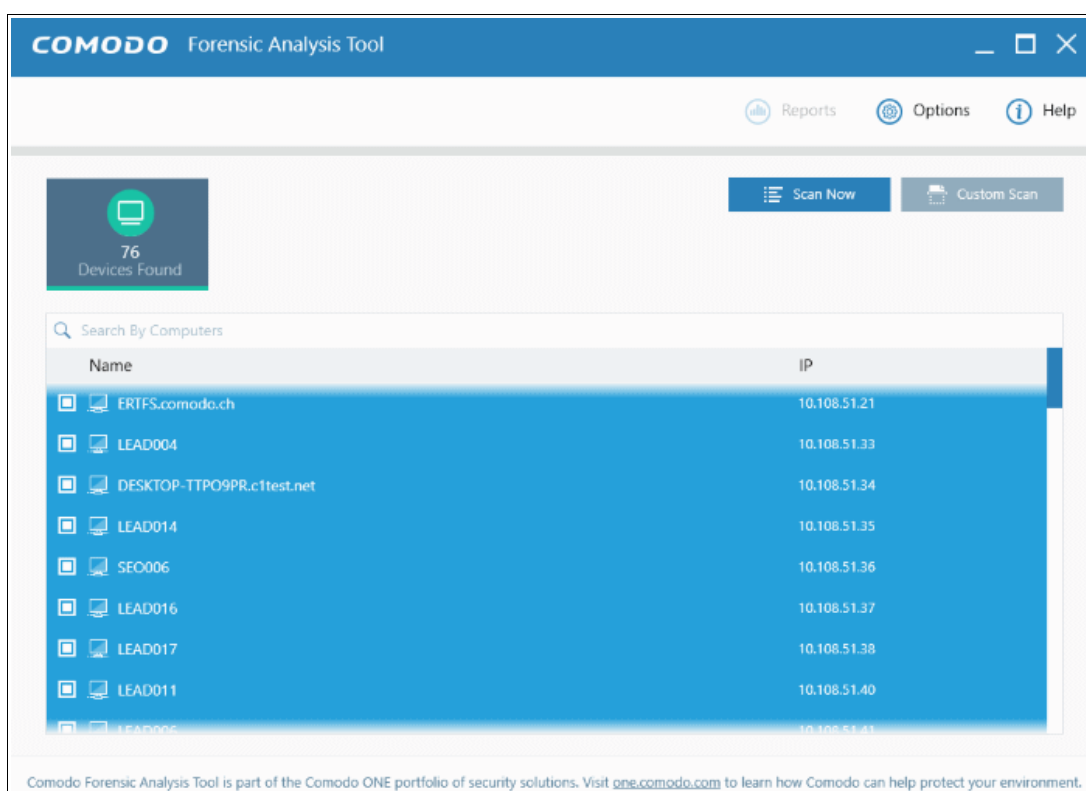
- **Introduction**
- **Running Forensic Analysis**
- **Scanning Computers**
  - **Scanning Computers using Active Directory**
  - **Scanning Computers using Workgroup**
  - **Scanning Computers by Network Addressees**
  - **Scanning Local Computer**
- **Scan Results**
- **Reports**
  - **Executive Report**
  - **Device Report**
  - **Program Report**

## 2 Running Forensic Analysis

Comodo Forensic Analysis can be downloaded from

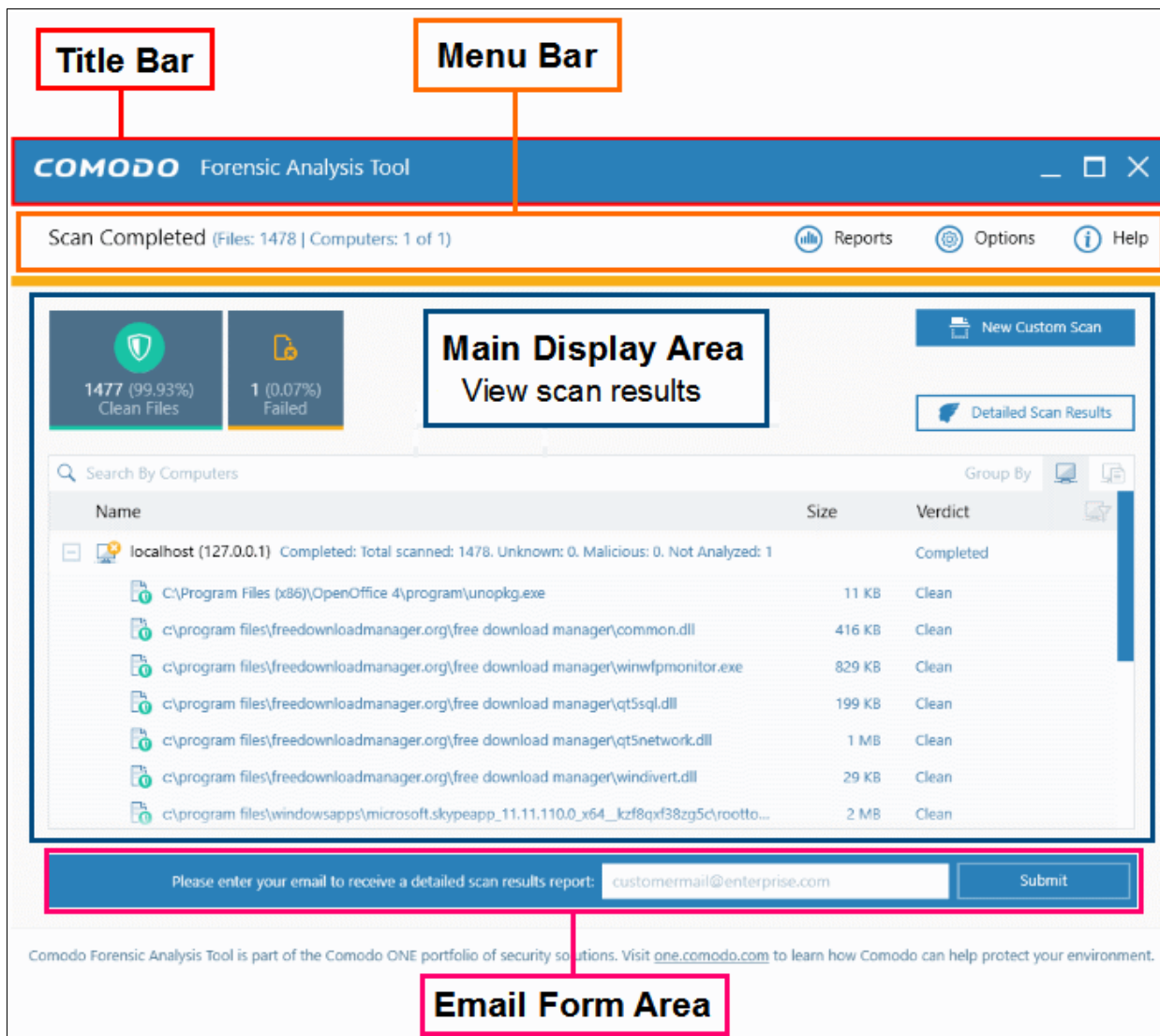
[http://bddvjenserv.brad.dc.comodo.net/CESM\\_copy/FAT/2.0.30223.26/sfx/ForensicAnalysisTool.exe](http://bddvjenserv.brad.dc.comodo.net/CESM_copy/FAT/2.0.30223.26/sfx/ForensicAnalysisTool.exe)

After saving, you can launch the tool by double-clicking on the setup file. No installation is required.



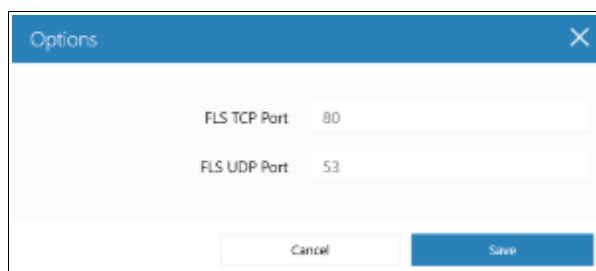
### 2.1 The Main Interface

The main interface of the tool allows you to configure and run scans, view results and generate risk reports.



## Main Functional Areas

- **Title Bar** - Displays the scanning progress. You can also minimize, maximize and close the application by using the controls at the far right.
- **Menu Bar** - Contains the controls for using the application.
  - **Options** - Displays the port numbers that CFA uses to communicate with our file lookup service (FLS). The FLS is used to deliver real-time verdicts on the trust status of unknown files. Admins should leave these ports at the default.



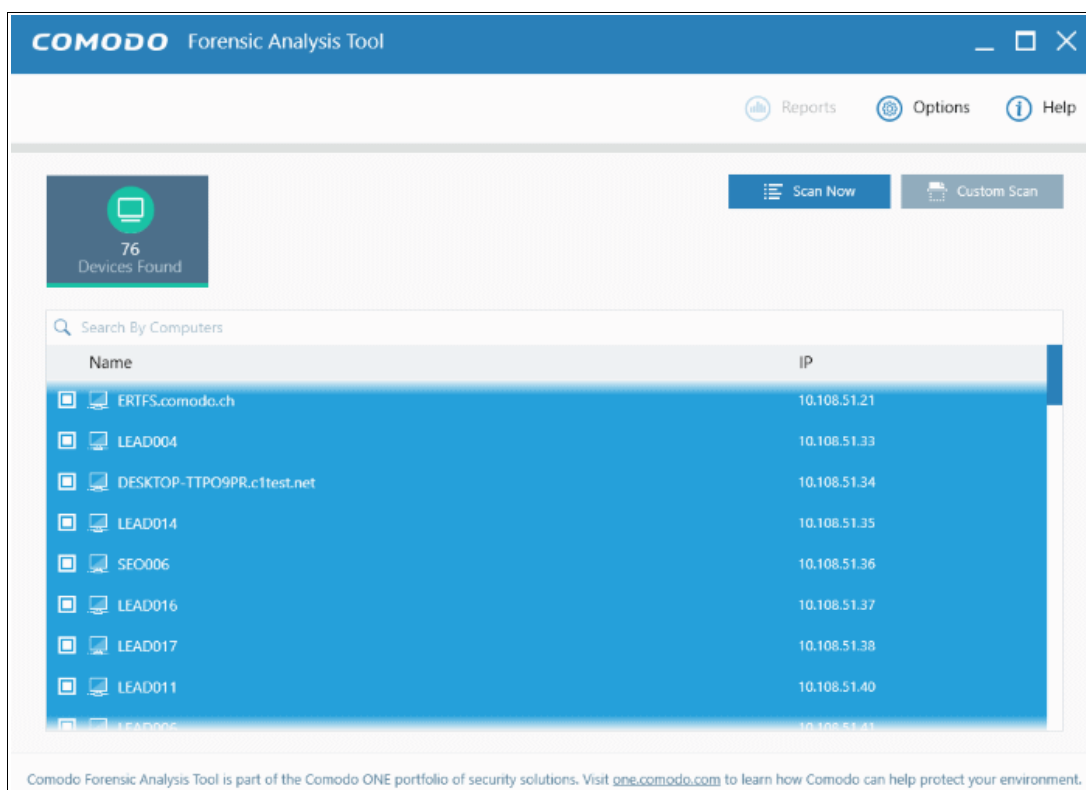
- **Reports** - Allows administrators to view reports generated by Valkyrie. Refer to the section '**Reports**' for more details.
- **Help** - The 'About' menu entry shows product and version information. Refer to **About Comodo Forensic Analysis** for more details. The 'Agent Requirements' menu entry contains troubleshooting

- advice if you experience problems connecting to your target computer.
- **Search** - Allows administrators to search for listed endpoints by name.
- **Main Display Area** - Displays details of scanned endpoints and the results from Valkyrie. Refer to the sections '**Scanning Computers**' and '**Scan Results**' for more details. Also contains controls for launching local and custom scans:
  - **Scan Now** - Scan endpoints on your local network to identify unknown files. Refer to section '**Scanning Computers**' for more details.
  - **Custom Scan** - Allows you to scan endpoints in a Workgroup, Active Directory, or Network Addresses. You can also scan your local computer. Refer to the section '**Scanning Computers**' for more details.
- **Email Form Area** - Enter your email address after the Valkyrie analysis is complete to receive a detailed scan report.

## 3 Scanning Computers

The Comodo Forensic Analysis tool allows administrators to add computers for scanning in multiple ways. Scans results will be shown in the CFA interface. Unknown files are automatically submitted to Comodo Valkyrie for further analysis. The CFA interface displays results of both files analyzed by Forensic Analysis and Valkyrie analysis.

- **Active Directory** - Suitable for a corporate environment where a large number of endpoints need to be scanned within a network.
- **Workgroup** - Allows you to add computers that belong to a work group
- **Network Address** - Specify target endpoints by host name, IP address or IP range
- **This Computer** - Allows you to run a scan on your local device.



Refer to the following sections for more details:

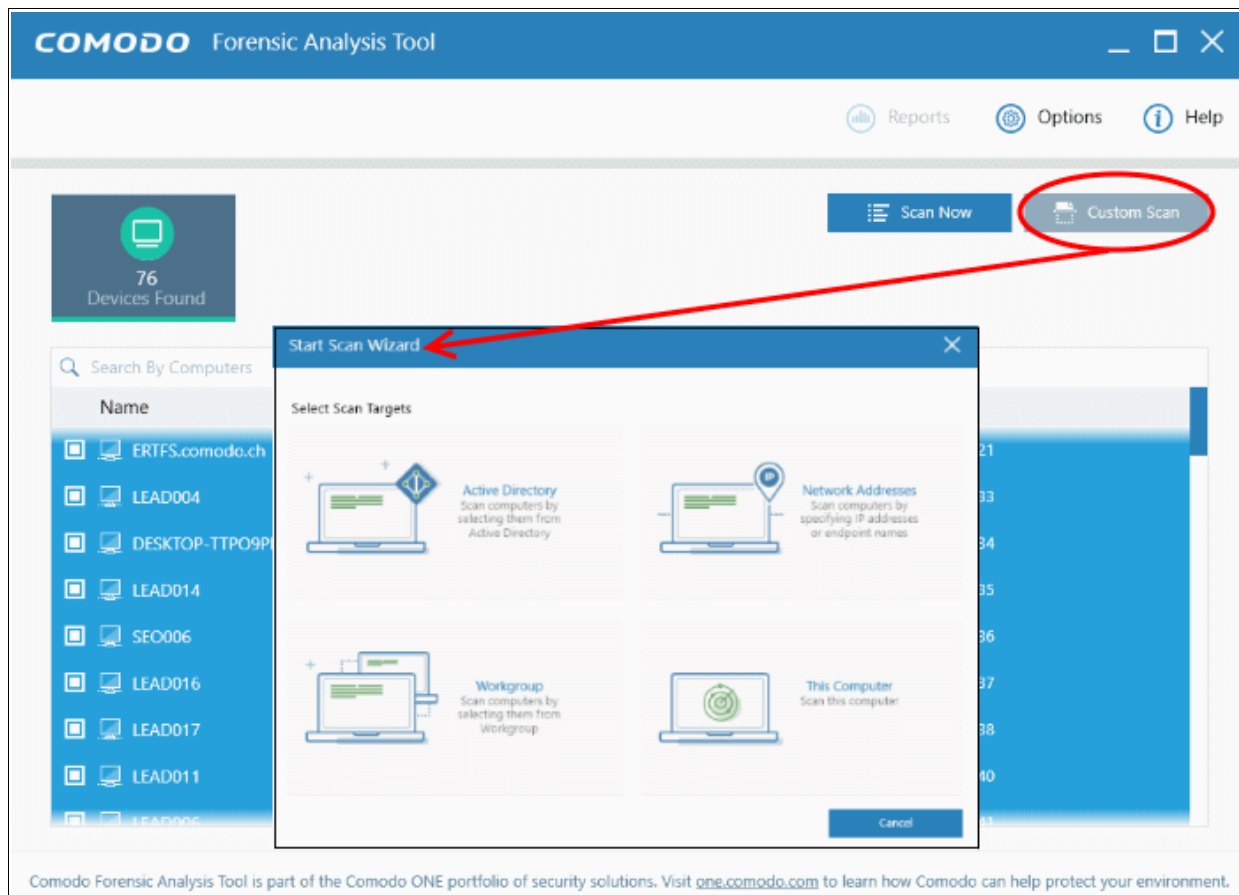
- **Scanning Computers using Active Directory**
- **Scanning Computers using Workgroup**

- **Scanning Computers by Network Addresses**
- **Scanning Computers by Custom Scan**

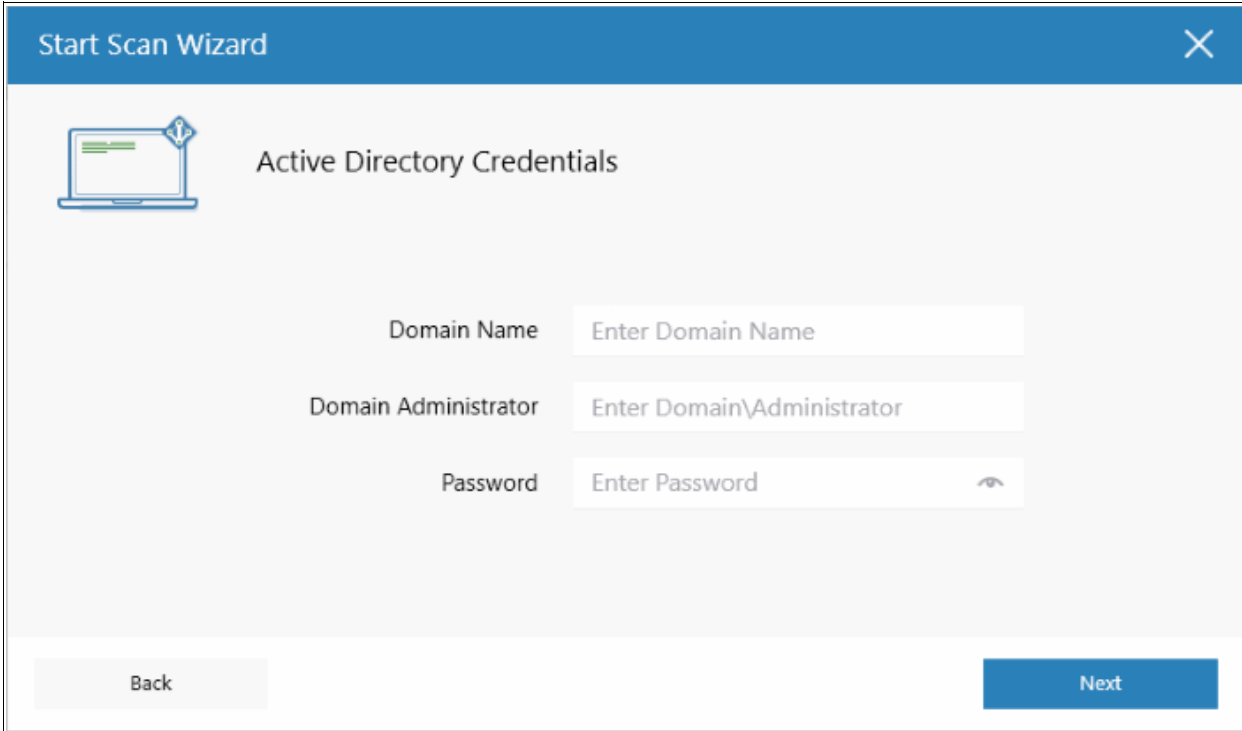
## 3.1 Scanning Computers using Active Directory

The Active Directory method allows administrators to import and scan all endpoints in a domain.

- Click 'Custom Scan' on the home screen to open the scan wizard:

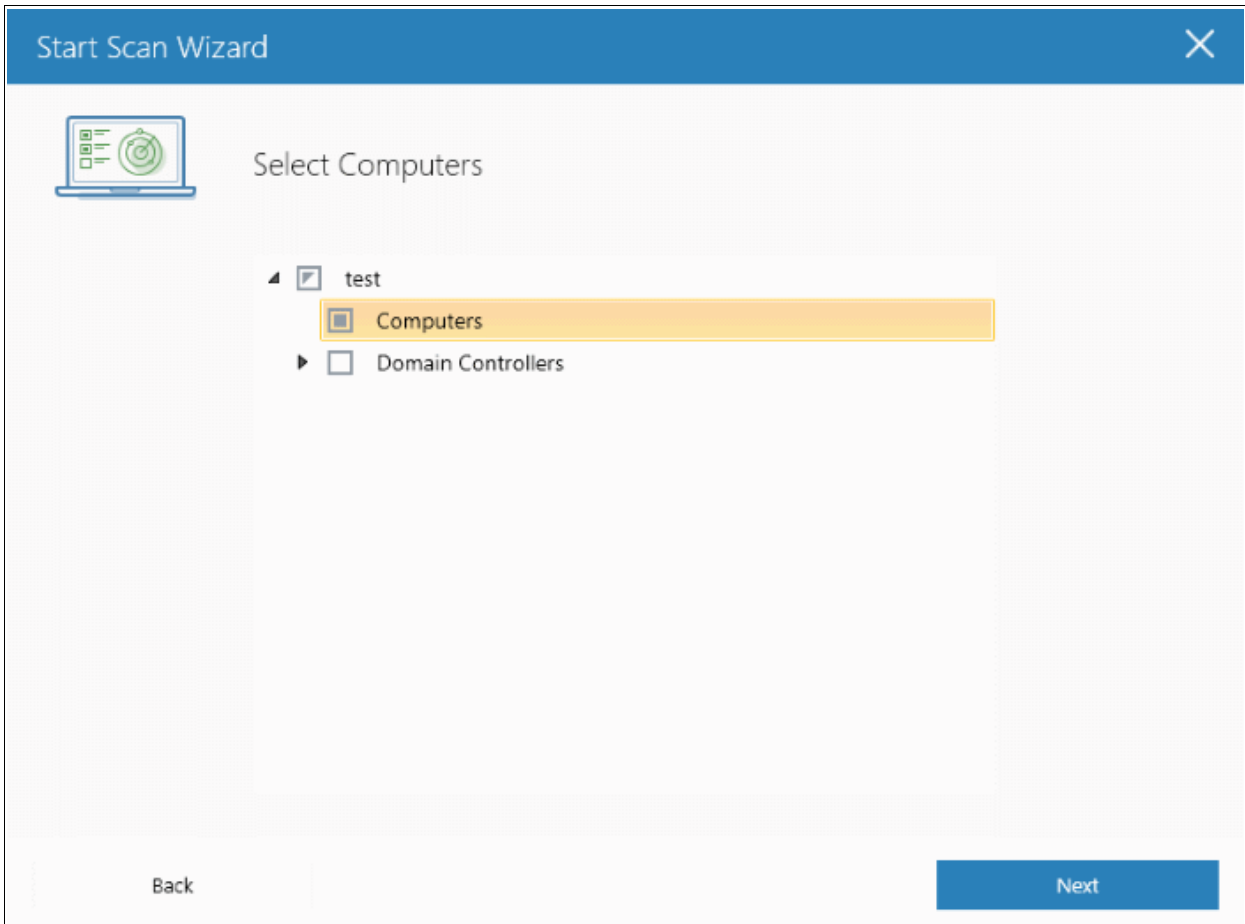


- Select 'Active Directory' to open the AD configuration screen.
- Enter the domain name and login details of your Active Directory domain:



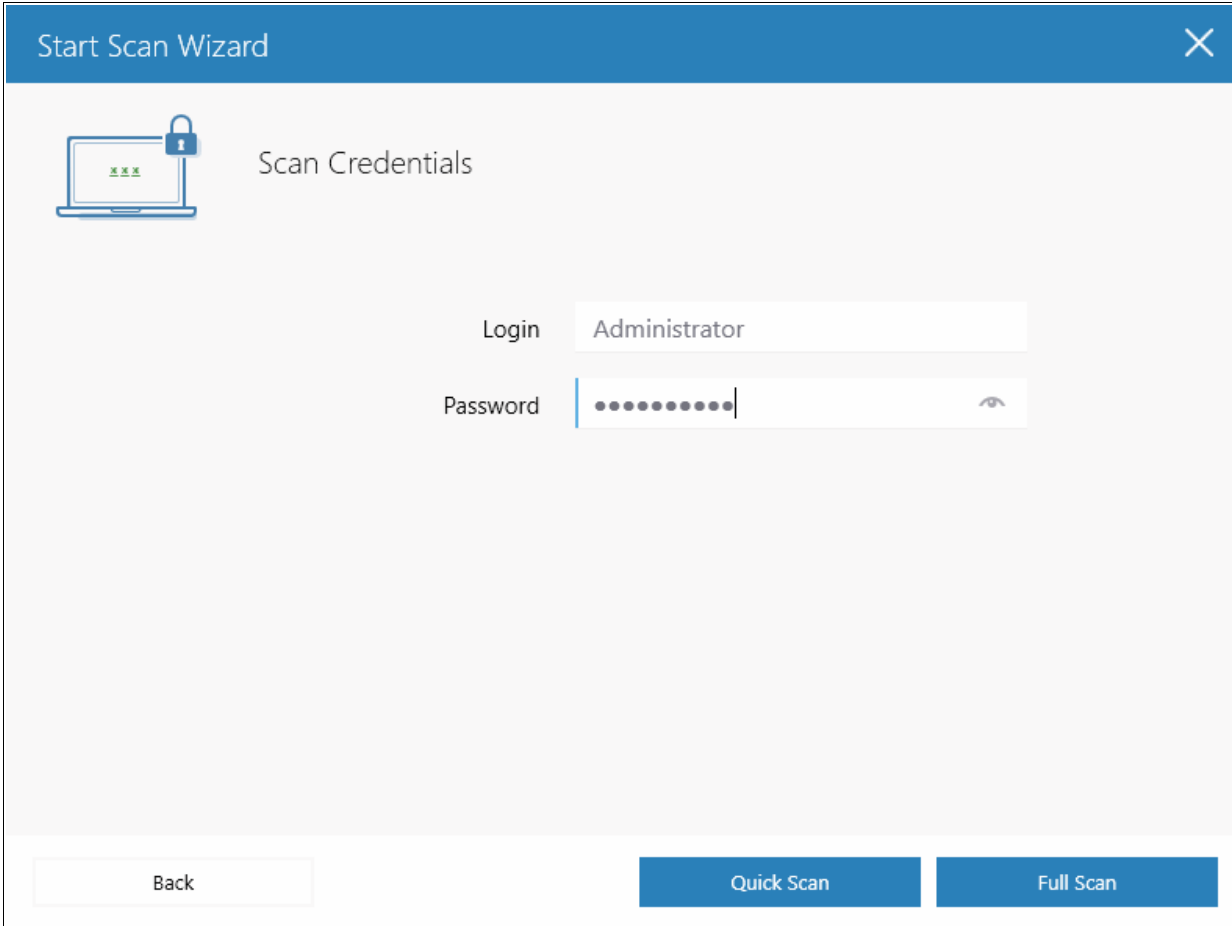
The screenshot shows the 'Start Scan Wizard' window with the title bar 'Start Scan Wizard' and a close button. The main content area is titled 'Active Directory Credentials' and features a laptop icon with a lock symbol. Below the title, there are three input fields: 'Domain Name' with the placeholder text 'Enter Domain Name', 'Domain Administrator' with the placeholder text 'Enter Domain\Administrator', and 'Password' with the placeholder text 'Enter Password' and a toggle eye icon. At the bottom, there are two buttons: 'Back' on the left and 'Next' on the right.

- After successful authentication, the 'Select Computers' screen will be displayed. Choose the endpoints you want to scan then click next:



The screenshot shows the 'Start Scan Wizard' window with the title bar 'Start Scan Wizard' and a close button. The main content area is titled 'Select Computers' and features a laptop icon with a target symbol. Below the title, there is a tree view structure. The root node is 'test', which is expanded and has a checked checkbox. Under 'test', there are two sub-nodes: 'Computers' and 'Domain Controllers'. The 'Computers' node is highlighted with a yellow background and has a checked checkbox. The 'Domain Controllers' node has an unchecked checkbox. At the bottom, there are two buttons: 'Back' on the left and 'Next' on the right.





The screenshot shows a window titled "Start Scan Wizard" with a close button (X) in the top right corner. The main content area is titled "Scan Credentials" and features an icon of a laptop with a lock and three green 'x' marks on the screen. Below the icon, there are two input fields: "Login" with the text "Administrator" and "Password" with a masked password of ten dots and a toggle eye icon. At the bottom of the window, there are three buttons: "Back" (disabled), "Quick Scan" (active), and "Full Scan" (active).

- Next, choose one of the following scan types:
  - **Quick Scan:** Scans critical and commonly infected areas of target endpoints
  - **Full Scan:** Scans all files and folders on target endpoints.

The screenshot displays the Comodo Forensic Analysis Tool interface. At the top, the title bar reads "COMODO Forensic Analysis Tool". Below the title bar, the status bar shows "37.20% Scan In Progress... (Files: 6840 | Computers: 0 of 7)". To the right of the status bar are icons for "Reports", "Options", and "Help".

Below the status bar, there are three summary cards:

- Clean Files:** 6642 (97.11%)
- Malicious Files:** 2 (0.03%)
- In Analysis:** 196 (2.87%)

A "Stop Scan" button is located to the right of these cards.

Below the summary cards is a table with the following columns: "Name", "Size", and "Verdict". The table is titled "Search By Computers".

Name	Size	Verdict
DESKTOP-TTPO9PR (10.108.51.100)	3120 scanned (4.57%), Unknown: 0, Malicious: 2, In Analysis 21.	In Progress
TONYSTARK-PC (10.108.51.245)	Login problem: invalid username or bad password.	Failed
WIN-CU2OXBJDY3D (10.108.51.129)	3721 scanned (7.04%), Unknown: 0, Malicious: 0, In Analysis 175.	In Progress
DESKTOP-1AMD5C1 (10.108.51.104)	This computer is not accessible.	Offline
SKYHIGH-PC (10.108.51.192)	This computer is not accessible.	Offline
TOM (10.108.51.175)	This computer is not accessible.	Offline
WIN-8719G19C0H7 (10.108.51.117)	This computer is not accessible.	Offline

At the bottom of the interface, there is a form to request a detailed scan results report. The text reads: "Please enter your email to receive a detailed scan results report:". The email address entered is "customermail@enterprise.com". A "Submit" button is located to the right of the input field.

At the very bottom of the screenshot, a footer note states: "Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment."

Scan progress will be displayed for each computer and the total scan progress shown on the title bar.

- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.
- After the scan is complete, the results will be displayed in the CFA interface. All unknown files will be uploaded to Valkyrie for further testing:

**COMODO Forensic Analysis Tool**

Scan Completed (Files: 58864 | Computers: 2 of 7) Reports Options Help

58703 (99.73%) Clean Files | 5 (0.01%) Malicious Files | 94 (0.16%) Unknown Files | 11 (0.02%) Failed | 51 (0.09%) In Analysis

[New Custom Scan](#) [Detailed Scan Results](#)

Search By Computers Group By

Name	Size	Verdict
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total scanned: 33350. Unknown: 10. Malicious: 4. In A...		Completed
TONYSTARK-PC (10.108.51.245) Login problem: invalid username or bad password.		Failed
WIN-CU2OX8JDY3D (10.108.51.129) Completed: Total scanned: 25521. Unknown: 84. Malicious: 1. In A...		Completed
DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible.		Offline
SKYHIGH-PC (10.108.51.192) This computer is not accessible.		Offline
TOM (10.108.51.175) This computer is not accessible.		Offline
WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible.		Offline

Please enter your email to receive a detailed scan results report:  [Submit](#)

Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment.

- The results interface contains details of each scan you have run along with verdicts for each file discovered
- The results of an 'in-progress' scan will be displayed after the scan finishes.
- Results can be displayed in two ways:
  - **Group by Computer:** Scan results will display total number of computers scanned and the number of unknown files found on those computers.
  - **Group by File:** Scan results will show the name and number of instances of scanned files.
- Unknown files will be uploaded to Valkyrie for analysis. Valkyrie is an online file verdict service which analyzes the behavior of unknown files with a range of static and dynamic tests. You need not have login details for Valkyrie to view the Valkyrie results via CFA tool.

You can view Valkyrie results by clicking the 'Detailed Scan Results' button.

- Enter your email address in the field at the bottom to receive a report on the Valkyrie analysis on unknown files.

APT Tool Scan Results

MY APT TOOL SCAN SESSION DETAILS

Show 25 entries Search:

File Name	Path	SHA1	Last Activity	Final Verdict	Hu
Solitaire.dll	C:\Program Files\Win...	283de0fb691f0e57d7...	2017-03-01 00:24:49		
Ghost.exe	C:\Users\Administrat...	df3328f9944867c3c5e...	2017-03-01 00:24:39	Malware	
ProcX.exe	C:\Users\Administrat...	2f0b217263bcd4d7d89...	2017-03-01 00:24:38	Clean	Cle
It-coat.exe	C:\Users\Vega\Deskt...	f7c419660229b865af1...	2017-03-01 00:24:30	Malware	
apt.exe	C:\Users\Vega\Deskt...	df18d63364187287ab4...	2017-03-01 00:24:29	Malware	
wrar521[1].exe	\\10.108.51.129\VC\...	cf1ebaf2ed0e3d537a5...	2017-03-01 00:22:36	Malware	Not

Showing 126 to 150 of 154 entries

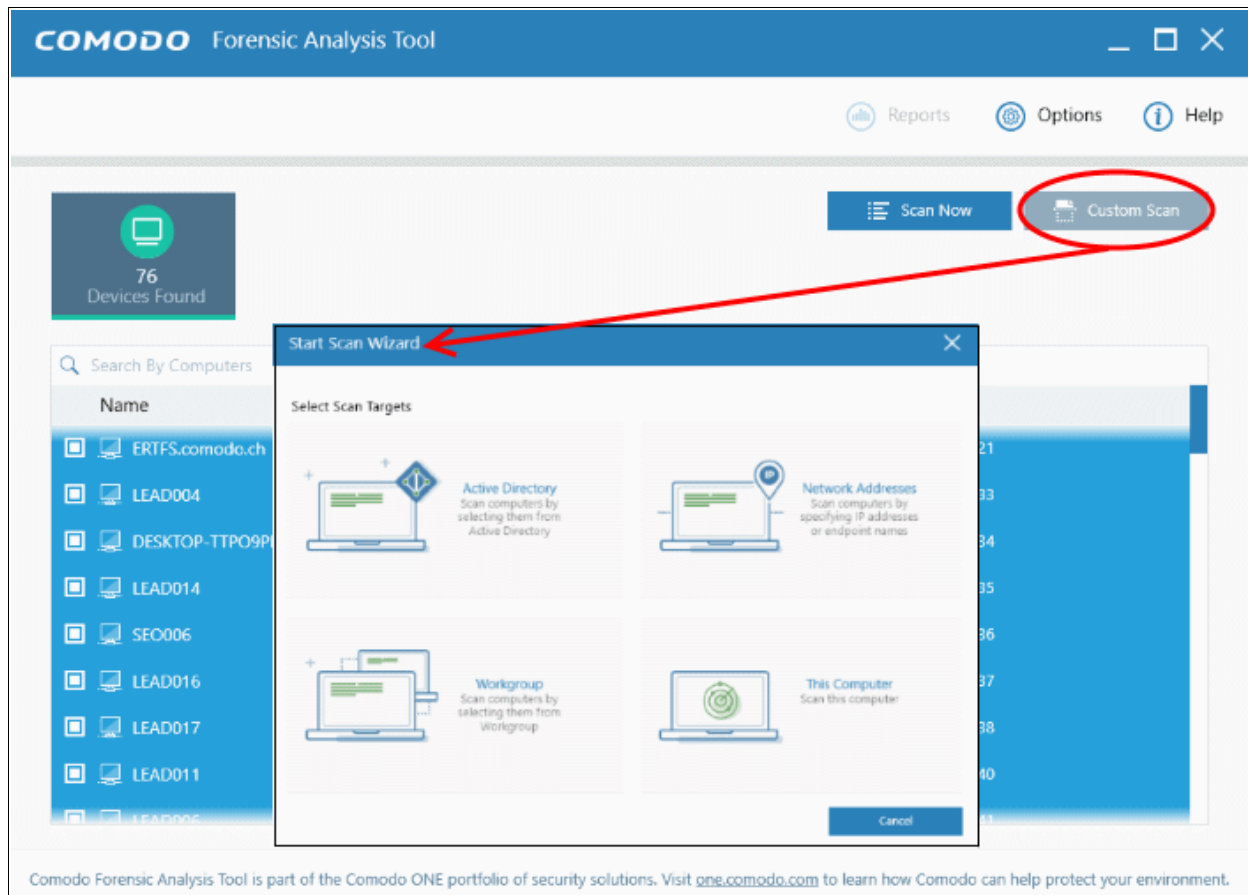
Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

Refer to the section '[Scan Results](#)' for more details.

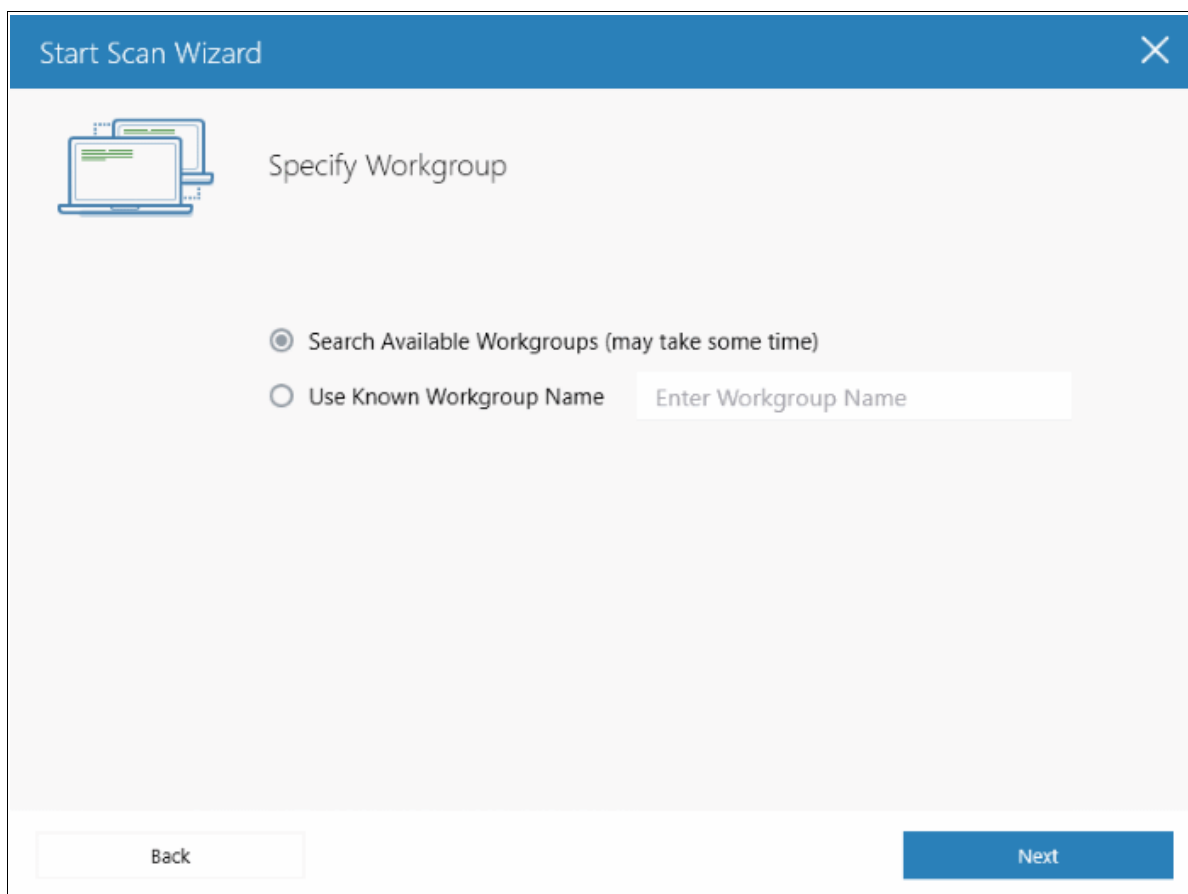
## 3.2 Scanning Computers using Workgroup

The Workgroup method allows administrators to import and scan all endpoints in a group.

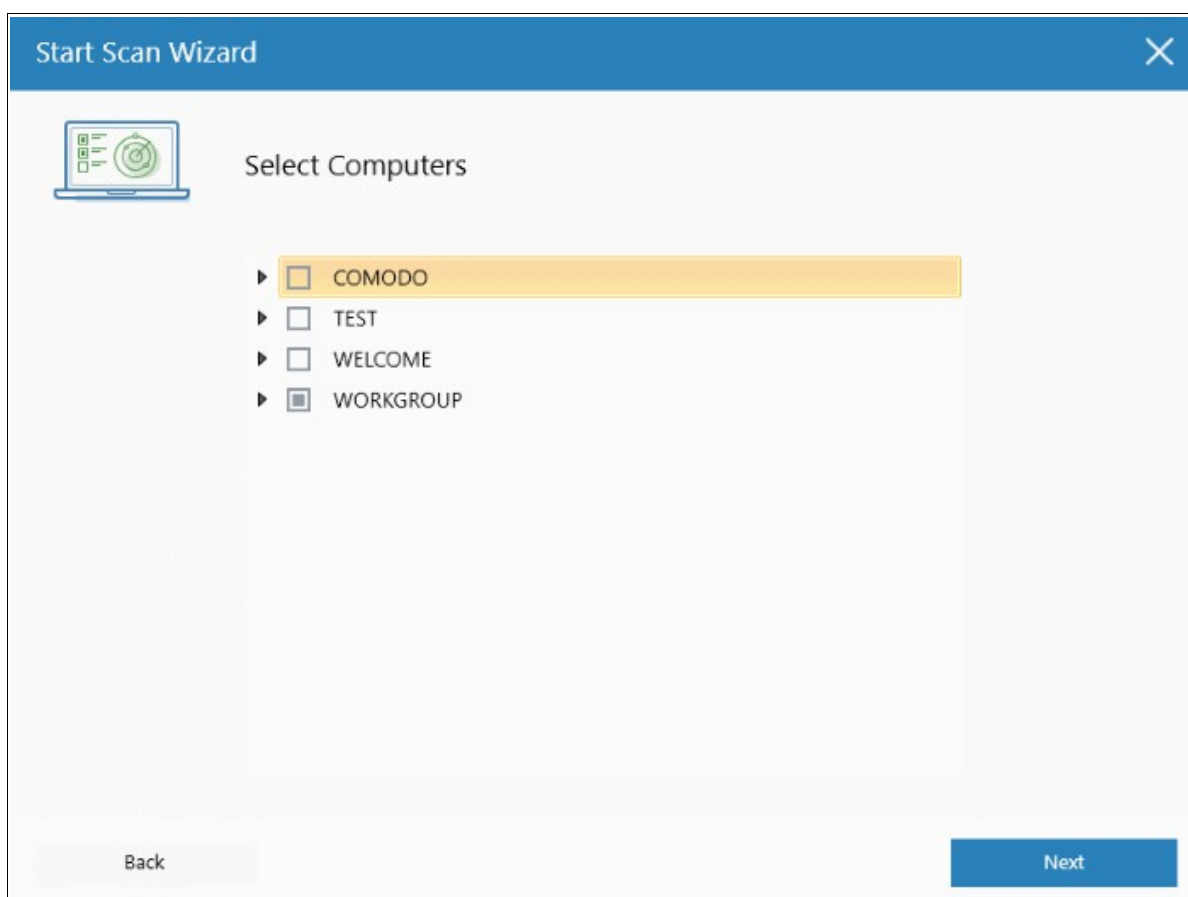
- Click 'Custom Scan' on the home screen to open the scan wizard:



- Click 'Workgroup' and select the available workgroups or enter the domain name of your existing Workgroup



- Select the Workgroup you want to scan.



- Next, enter the system's unique administrator username/password and choose one of the following scan types:
  - **Quick Scan:** Scans critical and commonly infected areas of target endpoints
  - **Full Scan:** Scans all files and folders on target endpoints.

Start Scan Wizard

Scan Credentials

Login

Password

After successful authentication, the scanning of endpoints in the Workgroup will start.

15.71% Scan In Progress... (Files: 480 | Computers: 0 of 1)

477 (99.38%) Clean Files | 3 (0.63%) In Analysis

Stop Scan

Search By Computers

Name	Size	Verdict
localhost (127.0.0.1) 480 scanned (15.71%). Unknown: 0. Malicious: 0. In Analysis 3.		In Progress

Please enter your email to receive a detailed scan results report:  Submit

Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment.

Scan progress will be displayed for each computer and the total scan progress shown on the title bar.

- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.
- After the scan is complete, the results will be displayed in the CFA interface. All unknown files will be uploaded to Valkyrie for further testing:

COMODO Forensic Analysis Tool

Scan Completed (Files: 1491 | Computers: 1 of 1)

1490 (99.93%) Clean Files | 1 (0.07%) Failed

New Custom Scan

Detailed Scan Results

Search By Computers

Name	Size	Verdict
localhost (127.0.0.1) Completed: Total scanned: 1491. Unknown: 0. Malicious: 0. Not Analyzed: 1		Completed

Please enter your email to receive a detailed scan results report:  Submit

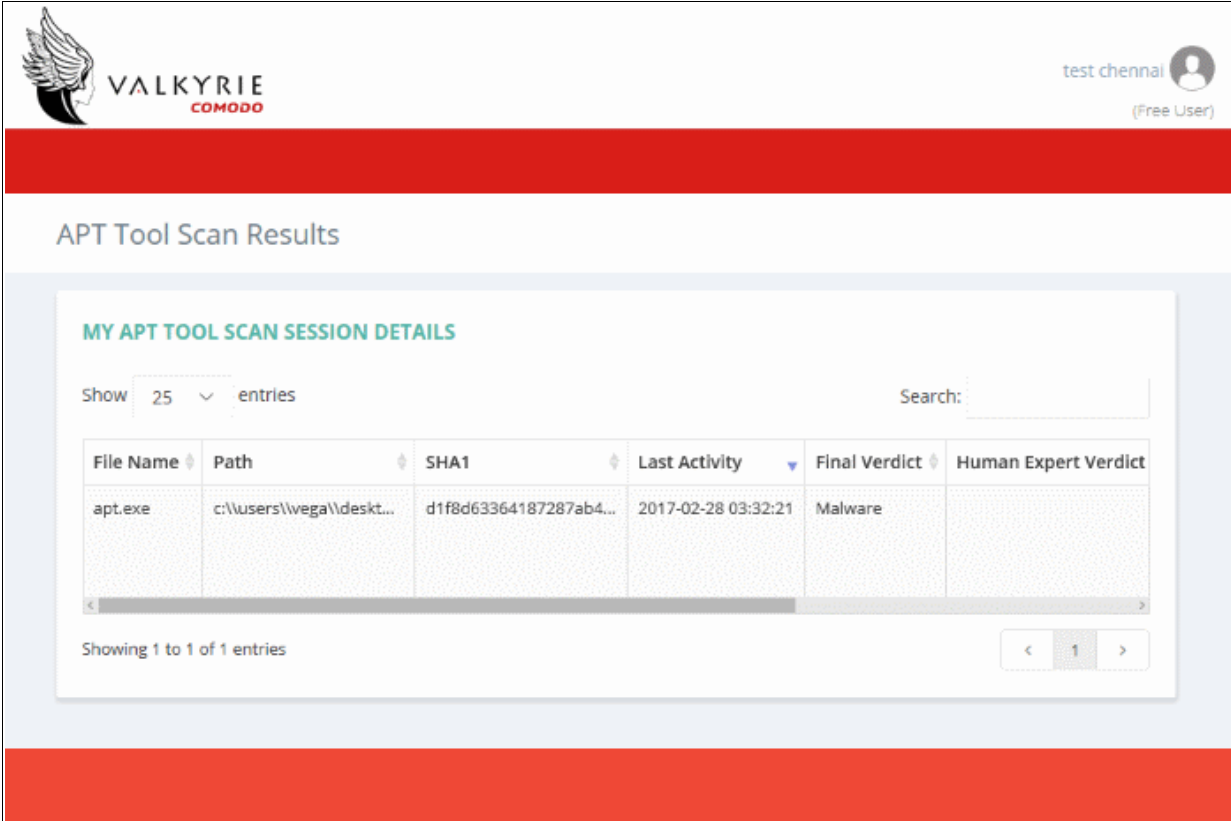
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment.



- The results interface contains details of each scan you have run along with verdicts for each file discovered
- The results of an 'in-progress' scan will be displayed after the scan finishes.
- Results can be displayed in two ways:
  - **Group by Computer:** Scan results will display total number of computers scanned and the number of unknown files found on those computers.
  - **Group by File:** Scan results will show the name and number of instances of scanned files.
- Unknown files will be uploaded to Valkyrie for analysis. Valkyrie is an online file verdict service which analyzes the behavior of unknown files with a range of static and dynamic tests. You need not have login details for Valkyrie to view the Valkyrie results via CFA tool.

You can view Valkyrie results by clicking the 'Detailed Scan Results' button.

- Enter your email address in the field at the bottom to receive a report on the Valkyrie analysis on unknown files.



The screenshot displays the Valkyrie portal interface. At the top left is the Valkyrie logo with the text 'VALKYRIE COMODO'. At the top right, the user is identified as 'test chennai' with a profile icon and '(Free User)' below it. The main heading is 'APT Tool Scan Results'. Below this is a section titled 'MY APT TOOL SCAN SESSION DETAILS'. It features a 'Show 25 entries' dropdown and a search field. A table lists scan results with columns: File Name, Path, SHA1, Last Activity, Final Verdict, and Human Expert Verdict. One entry is visible: 'apt.exe' at path 'c:\users\vega\desk...' with SHA1 'd1f8d63364187287ab4...' and 'Last Activity' '2017-02-28 03:32:21'. The 'Final Verdict' is 'Malware'. The table is followed by a pagination bar showing 'Showing 1 to 1 of 1 entries' and navigation arrows.

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict
apt.exe	c:\users\vega\desk...	d1f8d63364187287ab4...	2017-02-28 03:32:21	Malware	

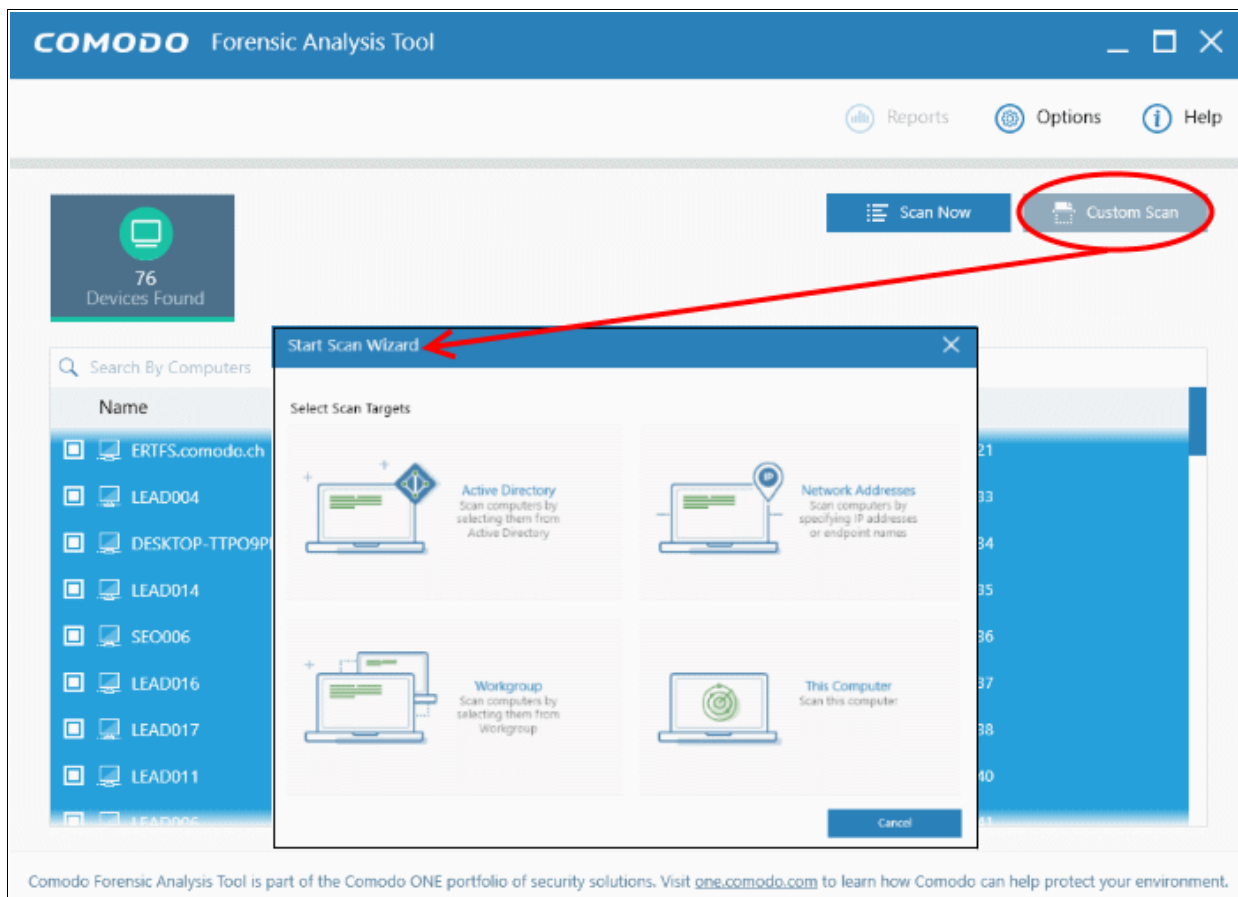
Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

Refer to the section '[Scan Results](#)' for more details.

## 3.3 Scanning Computers by Network Addresses

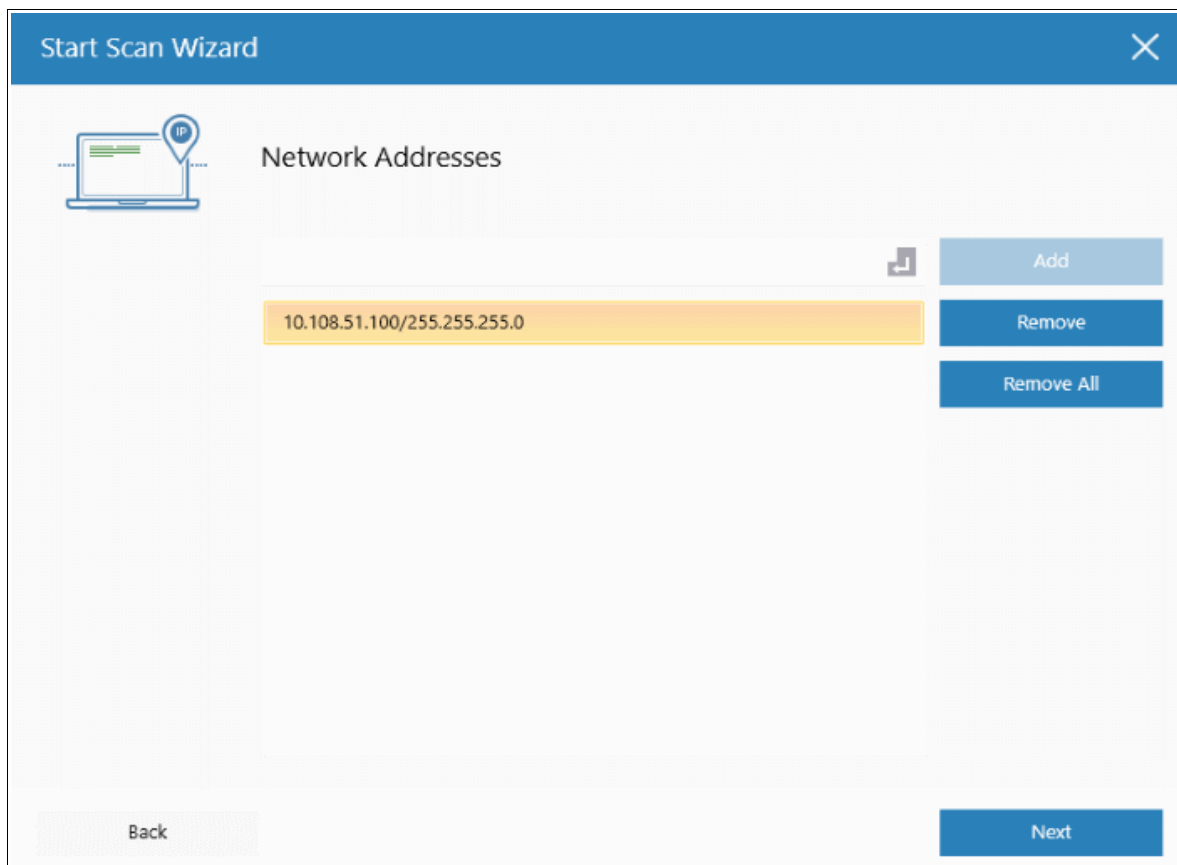
The Network Address method allows administrators to import and scan all endpoints in a specific network.

- Click 'Custom Scan' on the home screen to open the scan wizard:



To open the 'Start Scan Wizard', click the 'Custom Scan' button at the top-right of the main display area.

- Select 'Network Addresses' to open the AD configuration screen.



- Network Address: Enter the IP address, IP range or host name as shown below:
  - IP - 10.0.0.1
  - IP Range - 10.0.0.1-10.0.0.5
  - IP Subnet - 10.0.0.0/24 or 10.0.0.0/255.255.255.0
  - Computer Name - Home Computer
- Click the 'Add' button

The specified item will be added and displayed. Repeat the process to add more endpoints. To delete an item from the list, click the 'Remove' button beside it.

- Click 'Next' to continue.
- Login to the target device using either use the existing administrator credentials, or custom credentials.
- Next, choose one of the following scan types:
  - **Quick Scan:** Scans critical and commonly infected areas of target endpoints
  - **Full Scan:** Scans all files and folders on target endpoints.

By default, the IP subnet details are added in the network address field. The CFA tool will start discovering computers within the specified network, if the subnet details are given and then start the scanning process.

The screenshot displays the Comodo Forensic Analysis Tool interface. At the top, the title bar reads "COMODO Forensic Analysis Tool". Below the title bar, the status bar shows "99.27% Scan In Progress... (Files: 960 | Computers: 0 of 115)". There are three main sections: "Clean Files" (957, 99.69%), "Malicious Files" (1, 0.10%), and "In Analysis" (2, 0.21%). A "Stop Scan" button is visible in the top right. Below these sections is a table with columns for "Name", "Size", and "Verdict". The table lists several computers and their scan status. At the bottom, there is a form to enter an email address for detailed scan results, with the example "customermail@enterprise.com" and a "Submit" button.

Name	Size	Verdict
DESKTOP-TTPO9PR (10.108.51.100) 960 scanned (31.29%). Unknown: 0. Malicious: 1. In Anal...		In Progress
10.108.51.139 (10.108.51.139) Unknown error		Failed
ADPHP001 (10.108.51.119) Unknown error		Failed
ADPHP001-GANESH (10.108.51.244) Unknown error		Failed
ADPHP003 (10.108.51.178) Unknown error		Failed
ANAMICA (10.108.51.150) Unknown error		Failed
C4002 (10.108.51.208) Login problem: invalid username or bad password.		Failed

Scan progress will be displayed for each computer and the total scan progress shown on the title bar.

- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.
- After the scan is complete, the results will be displayed in the CFA interface. All unknown files will be uploaded to Valkyrie for further testing:

**COMODO Forensic Analysis Tool**

Scan Completed (Files: 1497 | Computers: 1 of 115)

Reports Options Help

1495 (99.87%) Clean Files | 1 (0.07%) Malicious Files | 1 (0.07%) In Analysis

New Custom Scan

Detailed Scan Results

Search By Computers

Name	Size	Verdict
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total scanned: 1497. Unknown: 0. Malicious: 1. In Analysis:...		
c:\users\vega\desktop\testing\apt4\apt.exe	45 KB	Malware
c:\program files\freedownloadmanager.org\free download manager\qt5widgets.dll	5 MB	Clean
C:\Program Files (x86)\OpenOffice 4\program\soffice.exe	9 MB	Clean
c:\program files\windowsapps\microsoft.skypeapp_11.11.110.0_x64_kzf8qxf38zg5c\skywrap.dll	40 MB	In Analysis
c:\program files\freedownloadmanager.org\free download manager\qt5gui.dll	5 MB	Clean
c:\program files\windowsapps\microsoft.skypeapp_11.11.110.0_x64_kzf8qxf38zg5c\skypebackgroundta...	175 KB	Clean
C:\Program Files\7-Zip\7-zip32.dll	48 KB	Clean

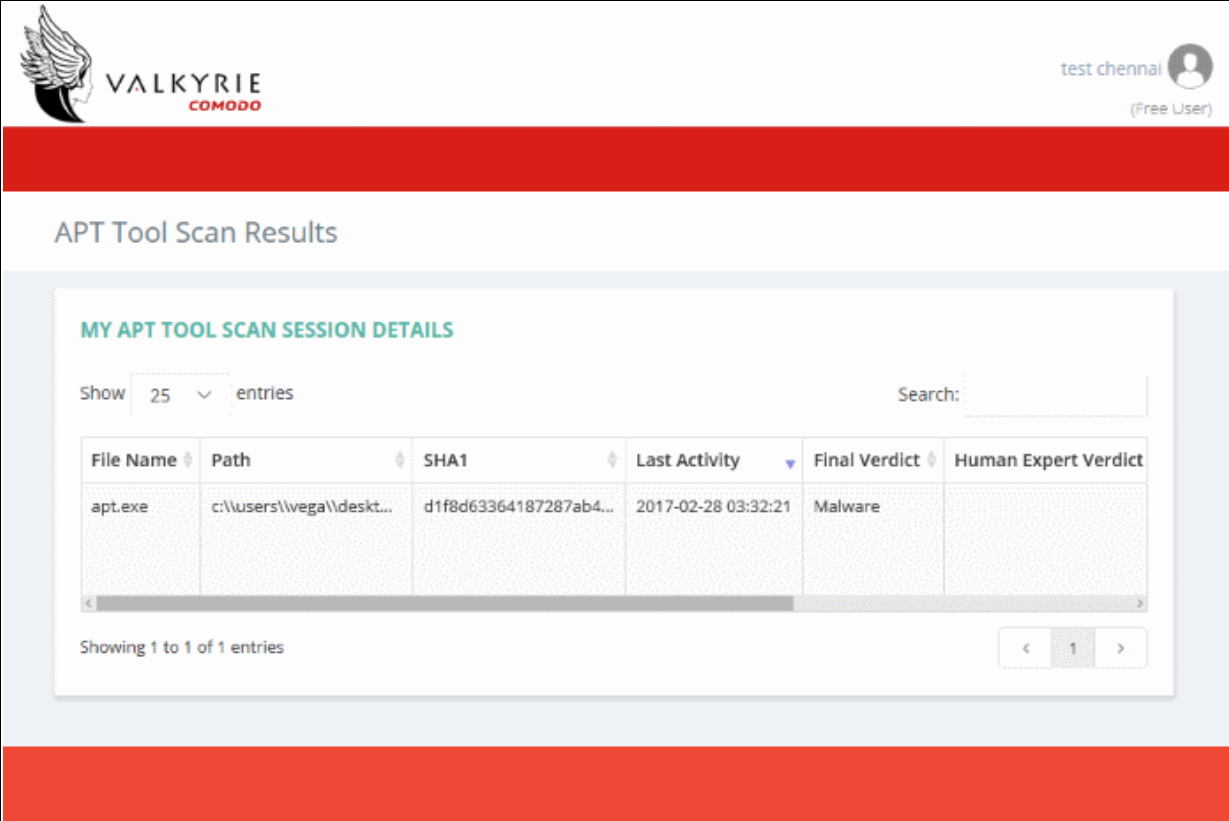
Please enter your email to receive a detailed scan results report:

Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment.

- The results interface contains details of each scan you have run along with verdicts for each file discovered
- The results of an 'in-progress' scan will be displayed after the scan finishes.
- Results can be displayed in two ways:
  - **Group by Computer:** Scan results will display total number of computers scanned and the number of unknown files found on those computers.
  - **Group by File:** Scan results will show the name and number of instances of scanned files.
- Unknown files will be uploaded to Valkyrie for analysis. Valkyrie is an online file verdict service which analyzes the behavior of unknown files with a range of static and dynamic tests. You need not have login details for Valkyrie to view the Valkyrie results via CFA tool.

You can view Valkyrie results by clicking the 'Detailed Scan Results' button.

- Enter your email address in the field at the bottom to receive a report on the Valkyrie analysis on unknown files.



The screenshot displays the Valkyrie portal interface. At the top left is the Valkyrie logo. At the top right, the user is identified as 'test chennai (Free User)'. The main heading is 'APT Tool Scan Results'. Below this is a section titled 'MY APT TOOL SCAN SESSION DETAILS'. It features a 'Show 25 entries' dropdown and a search box. A table lists scan results with columns for File Name, Path, SHA1, Last Activity, Final Verdict, and Human Expert Verdict. One entry is shown for 'apt.exe' with a 'Malware' verdict. A pagination bar at the bottom indicates 'Showing 1 to 1 of 1 entries'.

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict
apt.exe	c:\users\vega\deskt...	d1f8d63364187287ab4...	2017-02-28 03:32:21	Malware	

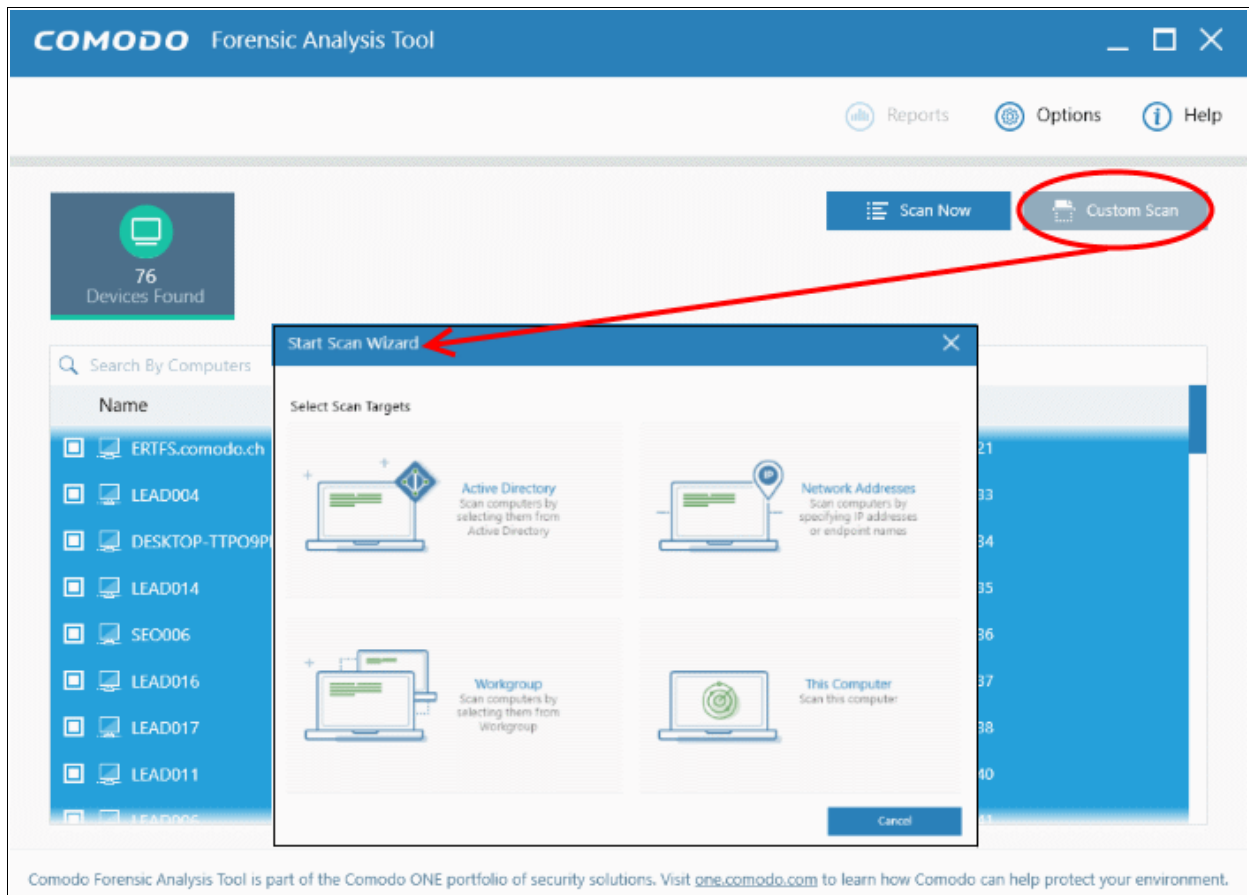
Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

Refer to the section '[Scan Results](#)' for more details.

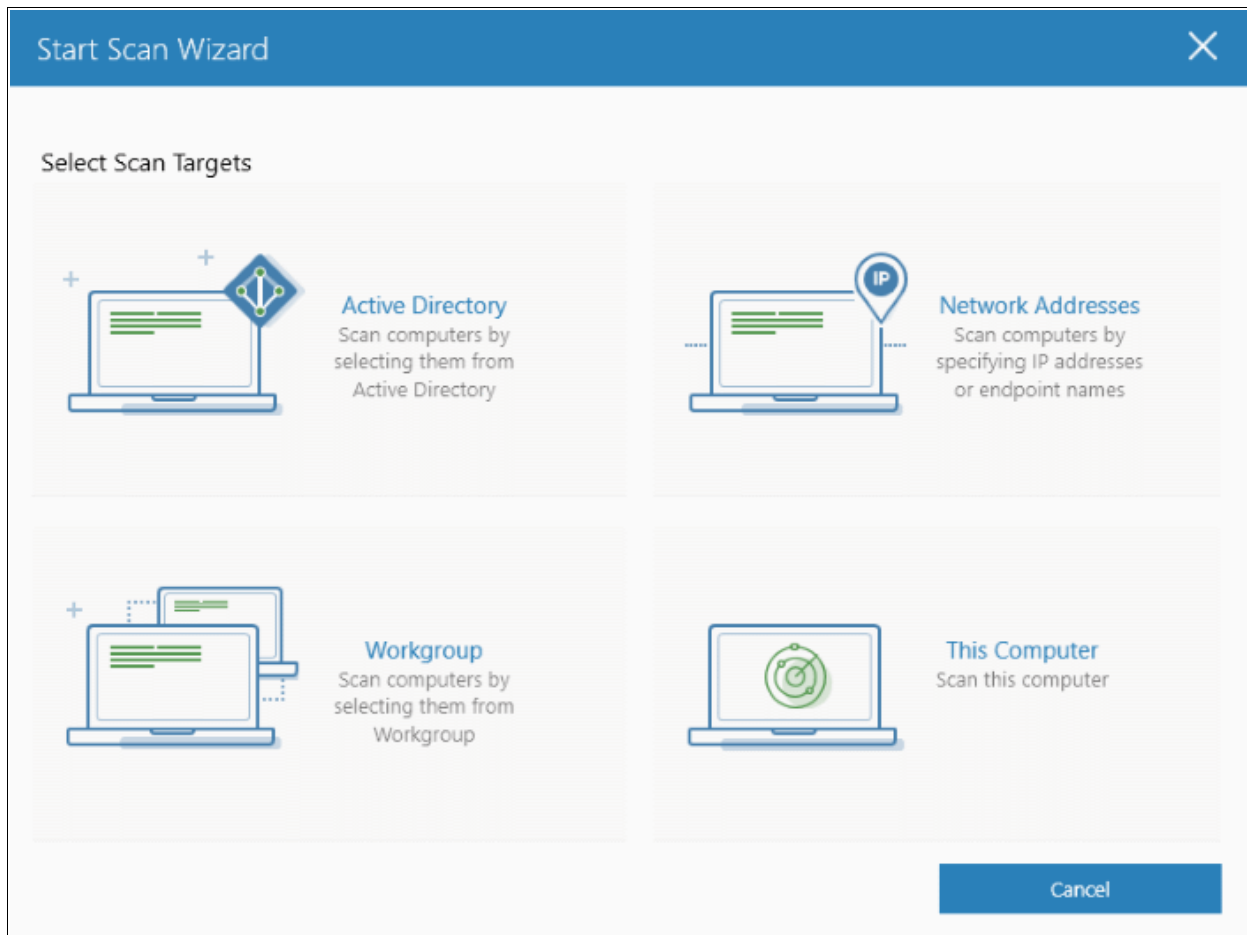
## 3.4 Scanning Local Computer

The Local Computer method allows administrators to import and scan all endpoints in your computer.

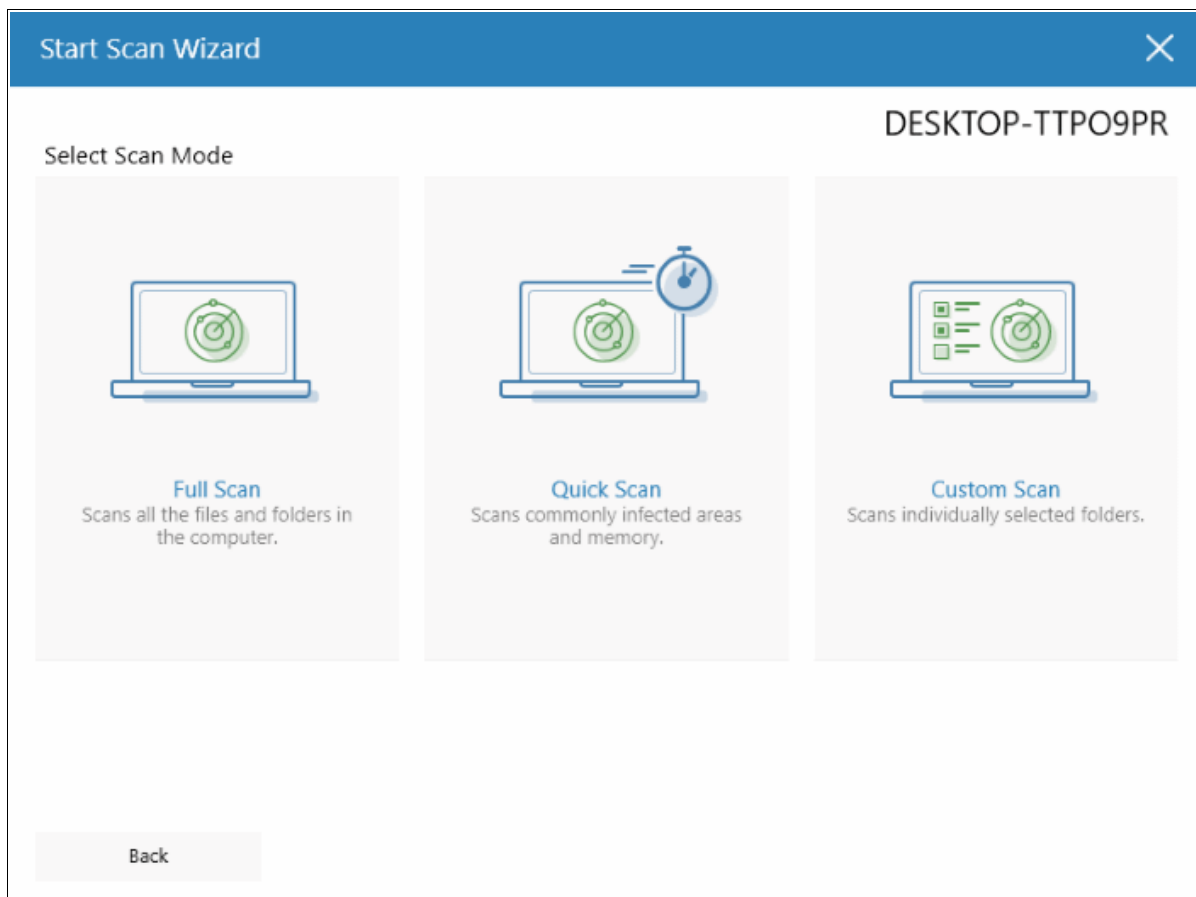
- Click 'Custom Scan' on the home screen to open the scan wizard:



- Click 'This Computer'

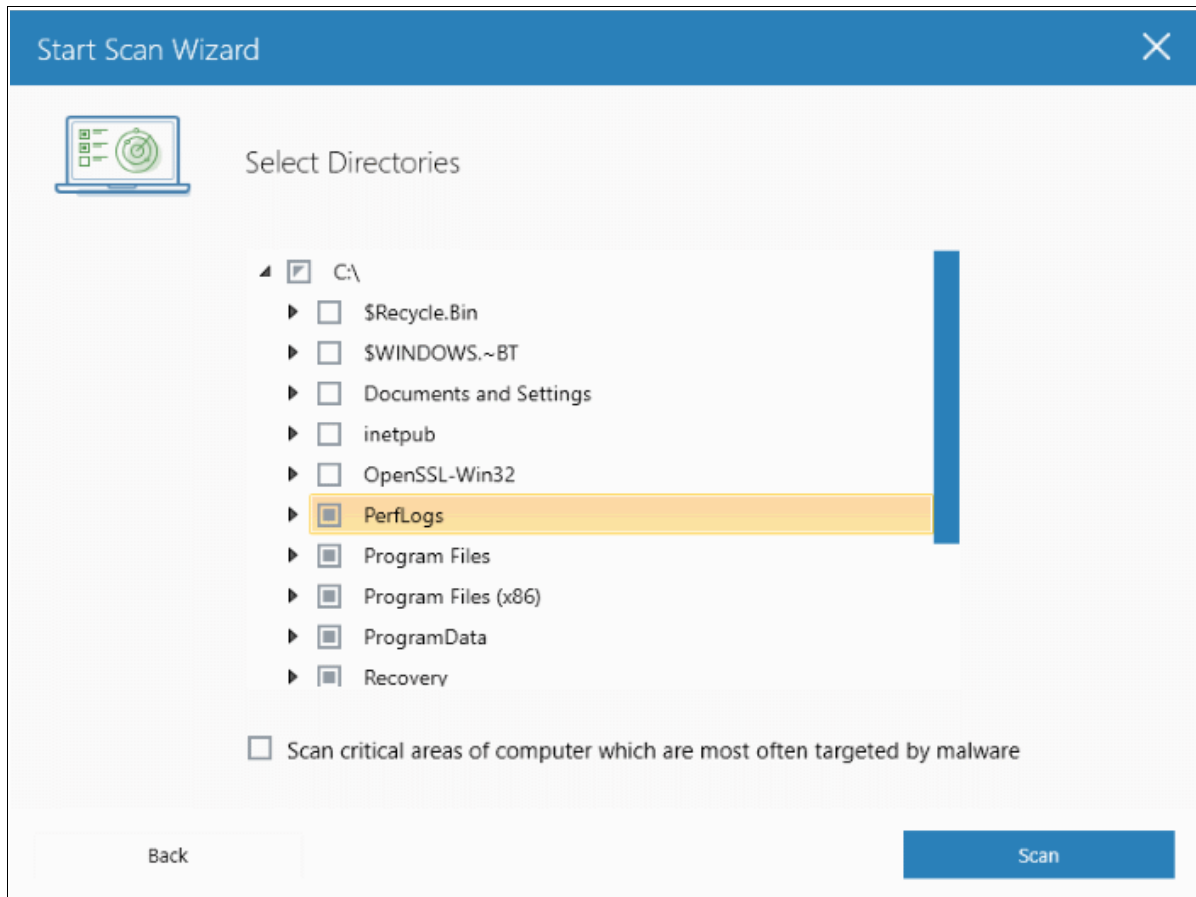


The three scan types will open.



- Select the endpoints that you want to scan and choose one of the following scan types:
  - **Quick Scan:** Scans critical and commonly infected areas of target endpoints
  - **Full Scan:** Scans all files and folders on target endpoints.
  - **Custom Scan:** Scans selected files or folders.

If you choose the 'Quick' or 'Full Scan' options then the scan will begin immediately. If you select 'Custom Scan', then you should next choose the directories and files you wish to scan in the 'Select Directories' screen:



- Select 'Scan critical areas...' to scan frequently targeted areas of your computer in addition to the items in your custom scan.
- Click 'Scan' to begin the scan.

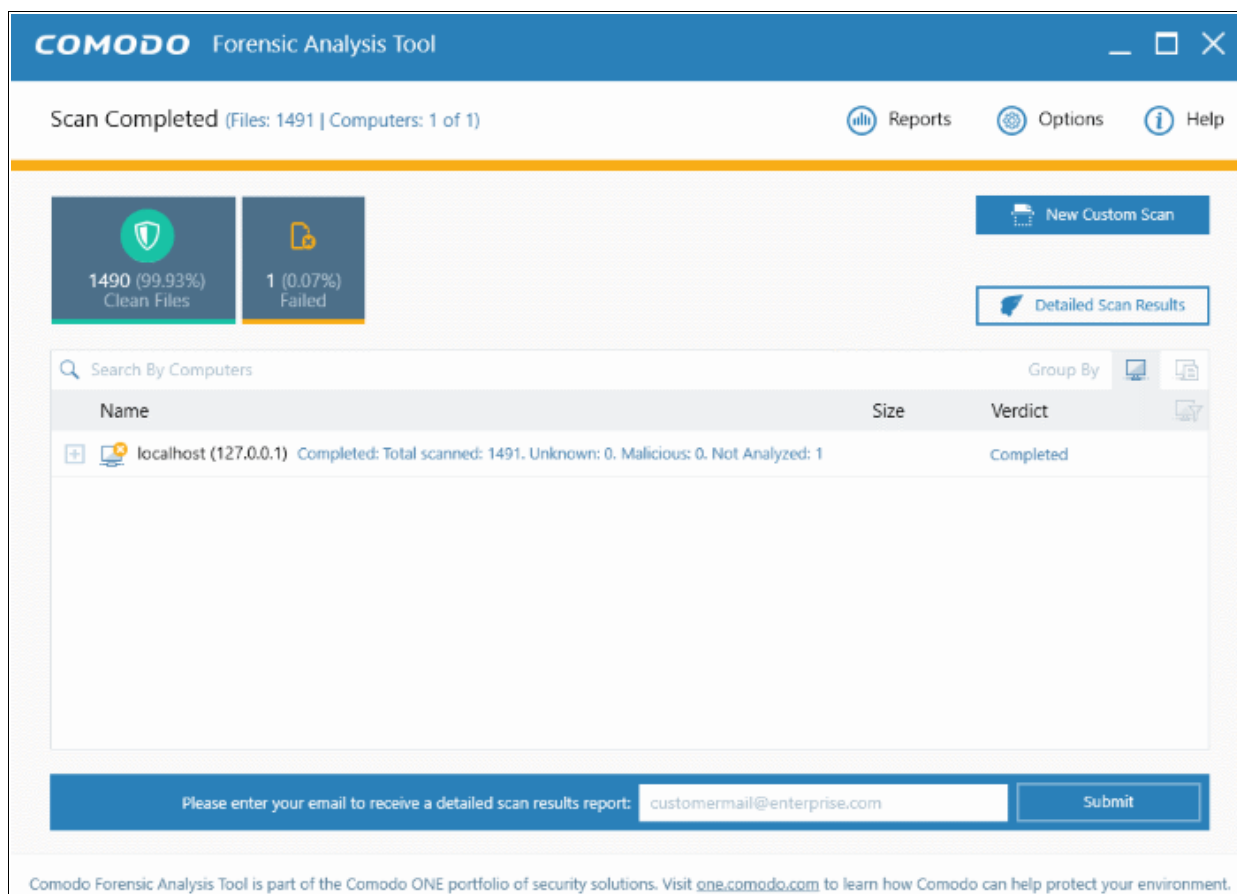


The screenshot displays the Comodo Forensic Analysis Tool interface. At the top, a progress bar indicates "15.71% Scan In Progress... (Files: 480 | Computers: 0 of 1)". Navigation links for "Reports", "Options", and "Help" are visible. Two summary cards show "477 (99.38%) Clean Files" and "3 (0.63%) In Analysis". A "Stop Scan" button is located in the top right. Below is a table with columns for "Name", "Size", and "Verdict". The table contains one entry for "localhost (127.0.0.1)" with "480 scanned (15.71%). Unknown: 0. Malicious: 0. In Analysis 3." and a verdict of "In Progress". At the bottom, there is a form to "Please enter your email to receive a detailed scan results report:" with the email "customermail@enterprise.com" and a "Submit" button. A footer note states: "Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment."

Name	Size	Verdict
localhost (127.0.0.1)	480 scanned (15.71%). Unknown: 0. Malicious: 0. In Analysis 3.	In Progress

Scan progress will be displayed for each computer and the total scan progress shown on the title bar.

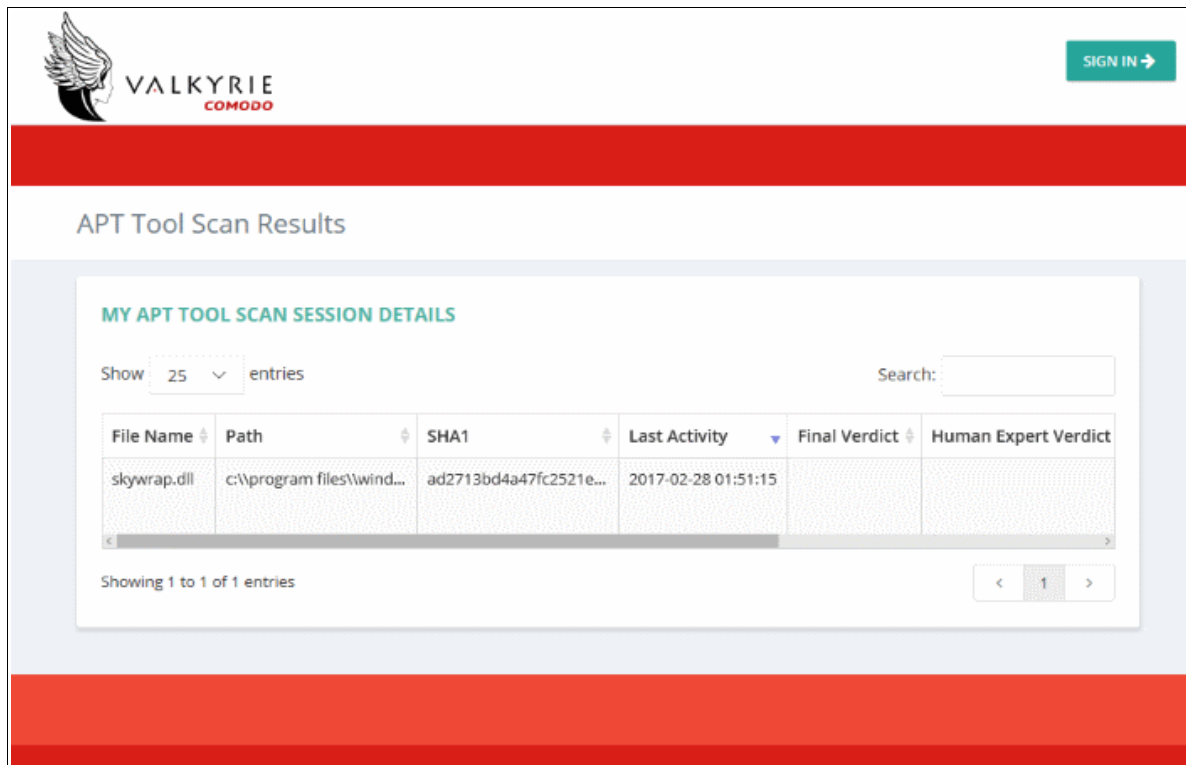
- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.
- After the scan is complete, the results will be displayed in the CFA interface. All unknown files will be uploaded to Valkyrie for further testing:



- The results interface contains details of each scan you have run along with verdicts for each file discovered
- The results of an 'in-progress' scan will be displayed after the scan finishes.
- Results can be displayed in two ways:
  - **Group by Computer:** Scan results will display total number of computers scanned and the number of unknown files found on those computers.
  - **Group by File:** Scan results will show the name and number of instances of scanned files.
- Unknown files will be uploaded to Valkyrie for analysis. Valkyrie is an online file verdict service which analyzes the behavior of unknown files with a range of static and dynamic tests. You need not have login details for Valkyrie to view the Valkyrie results via CFA tool.

You can view Valkyrie results by clicking the 'Detailed Scan Results' button.

- Enter your email address in the field at the bottom to receive a report on the Valkyrie analysis on unknown files.



The screenshot displays the Valkyrie portal interface. At the top left is the Valkyrie logo, and at the top right is a 'SIGN IN' button. The main heading is 'APT Tool Scan Results'. Below this is a section titled 'MY APT TOOL SCAN SESSION DETAILS'. It includes a 'Show 25 entries' dropdown and a search box. A table lists scan results with columns for File Name, Path, SHA1, Last Activity, Final Verdict, and Human Expert Verdict. One entry is visible: skywrap.dll at c:\program files\wind... with SHA1 ad2713bd4a47fc2521e... and Last Activity 2017-02-28 01:51:15. The bottom of the table shows 'Showing 1 to 1 of 1 entries' and a pagination control.

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict
skywrap.dll	c:\program files\wind...	ad2713bd4a47fc2521e...	2017-02-28 01:51:15		

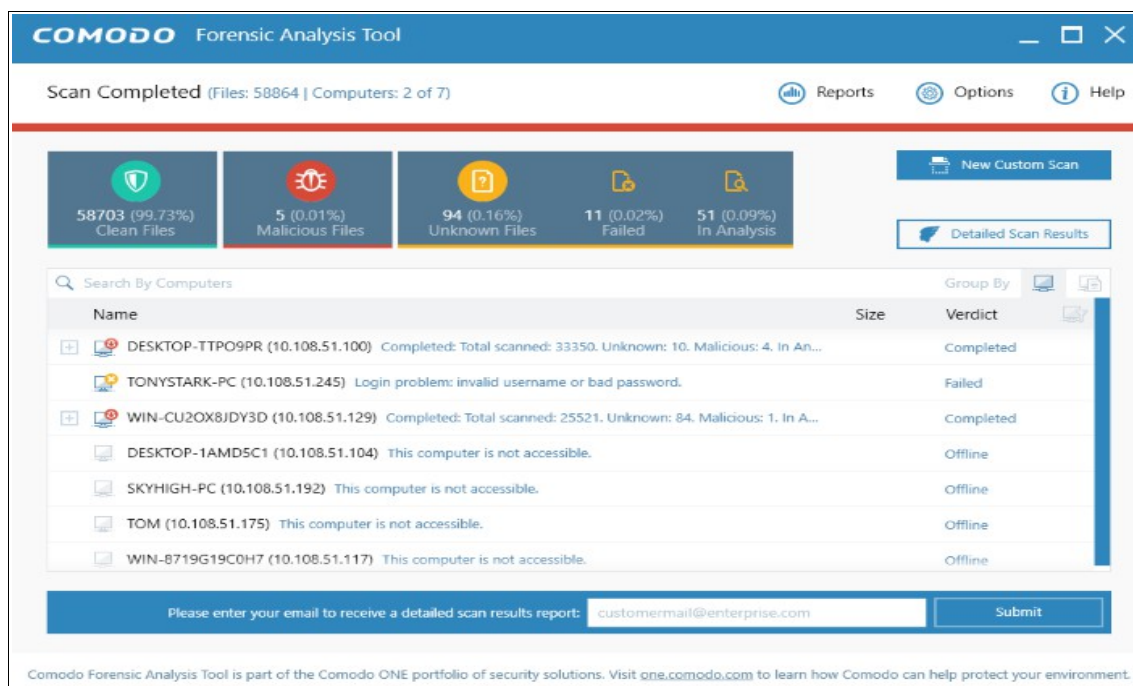
Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.


Refer to the section '[Scan Results](#)' for more details.

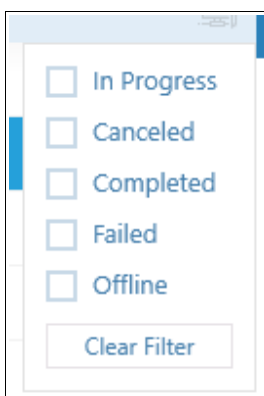
## 4 Scan Results


Scan results will be automatically shown in the CFA interface after a scan finishes. The initial scan checks the reputation of each file against Comodo's file-lookup service, a huge database of blacklisted and white-listed files. Blacklisted files will be flagged as malicious and should be deleted or quarantined. White-listed files are safe to run.

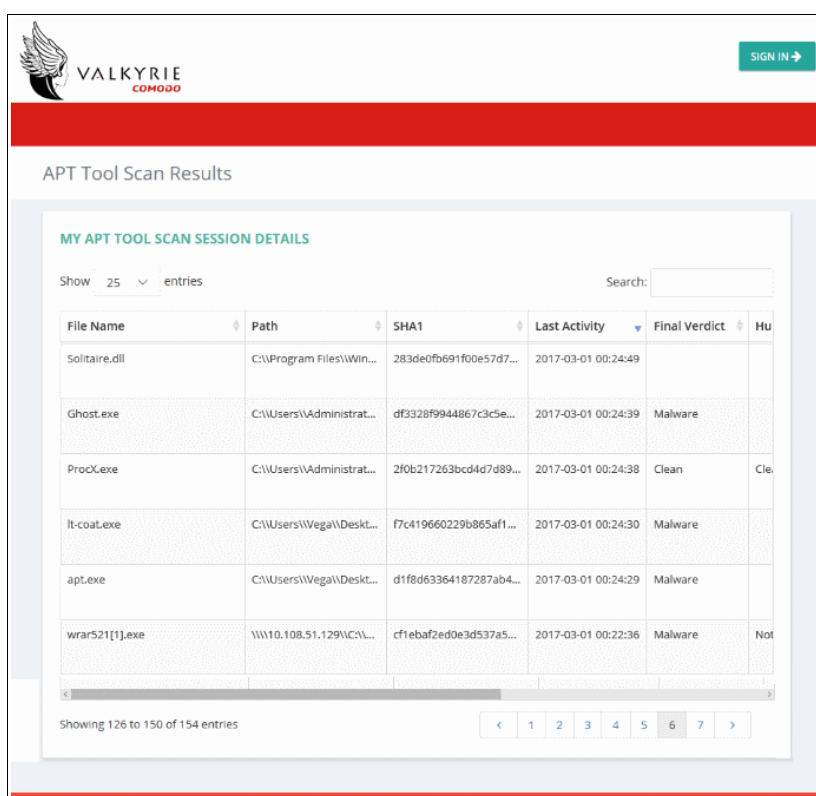
If a file is not on either the blacklist or whitelist, then it is categorized as 'unknown'. Unknown files are automatically submitted to Comodo Valkyrie where they will undergo a range of static and dynamic behavior tests to discover whether they are malicious or not. The CFA interface displays results of both files analyzed by Forensic Analysis and Valkyrie analysis.







- Scan results are listed for each computer. Each row has a quick summary of the scan results, including total files scanned and how many were malicious or unknown.
- Click the plus symbol beside an endpoint to view unknown and malicious files detected by the scan.
- Click the icons next to 'Group By' to view results by 'Computer' or by 'Files'.
- Expand an endpoint's results then click the 'Name', 'Size' or 'Verdict' column headers to sort files in order of the column name.
- To search for a particular endpoint, enter its name or IP address in the 'Search' box at the top right. Clear the search box to display all endpoints again.
- Click the funnel icon on the right  to filter endpoints by scan status:



- In Progress – Endpoints which have a scan currently running
  - Canceled - Endpoints on which a scan was aborted
  - Completed -Endpoints on which a scan has successfully finished
  - Failed - Endpoints on which CFA was unable to complete a scan
  - Offline - Endpoints which are not responding at this time
- If the filter icon is blue  then filter(s) are applied. Click 'Clear Filter' to display all endpoints again.
  - Unknown files are uploaded to Valkyrie for analysis. You can view the results of the Valkyrie analysis by clicking the 'Detailed Scan Results' button. This will open the Valkyrie results page:



Valkyrie Detailed Analysis Results - Table of Column Descriptions	
Column Header	Description
File Name	The name of the submitted file
Path	The IP of the endpoint and the file's path details
SHA1	The SHA1 hash value of the file.
Last Activity	The date and time the last activity of analysis was performed.
Final Verdict	The Valkyrie dynamic and <b>static analysis</b> results for the file. The results available are: <ul style="list-style-type: none"> <li>• Clean - The file is safe to run</li> <li>• No Threat Found - No malware found in the file, but cannot say it is safe to run</li> </ul>

	<ul style="list-style-type: none"> <li>Malware - The file is a malware and should not be run</li> </ul>
Human Expert Verdict	<p>The results of the file after Human expert analysis:</p> <ul style="list-style-type: none"> <li>Clean - File is safe to run</li> <li>Malware - The file is a malware file</li> <li>Potentially Unwanted Application (PUA) - Applications such as Adware, Spyware and so on</li> <li>No Threat Found - No malware found in the file, but cannot say it is safe to run</li> <li>Not Ready - Indicates manual analysis of the file is in progress</li> </ul>
Human Expert Analysis Status	<p>Indicates the status of files submitted for Human Expert analysis. The statuses are:</p> <ul style="list-style-type: none"> <li>In Queue - The analysis has not started</li> <li>In Progress - The analysis has started and in progress</li> <li>Analysis Completed - The analysis is completed and verdict displayed under the 'Manual Verdict' column</li> <li>Objected - Indicates the user wants a re-analysis of the file. If the user thinks that the initial manual verdict for the file is wrong, he/she can submit it again for another manual analysis.</li> <li>Objection Completed - Indicates the manual re-analysis is completed.</li> </ul>
Request Type	<p>Indicates the type of input given to receive Valkyrie results.</p> <ul style="list-style-type: none"> <li>Queried - The file were automatically uploaded to Valkyrie</li> <li>Manual - The files were manually uploaded to Valkyrie</li> </ul>
Actions	<p>The available actions are:</p> <ul style="list-style-type: none"> <li> - View Info - You can view the complete details of the results for the file such as summary, static analysis, dynamic analysis and file details.</li> <li> - Download Automatic Analysis Report - Allows you to download the report in PDF format.</li> <li> - View Virus Total Result - Takes you to the Virus Total website that displays its results for the file.</li> <li> - Send to Manual Analysis - Allows you to submit the file for manual analysis by Comodo technicians.</li> </ul>

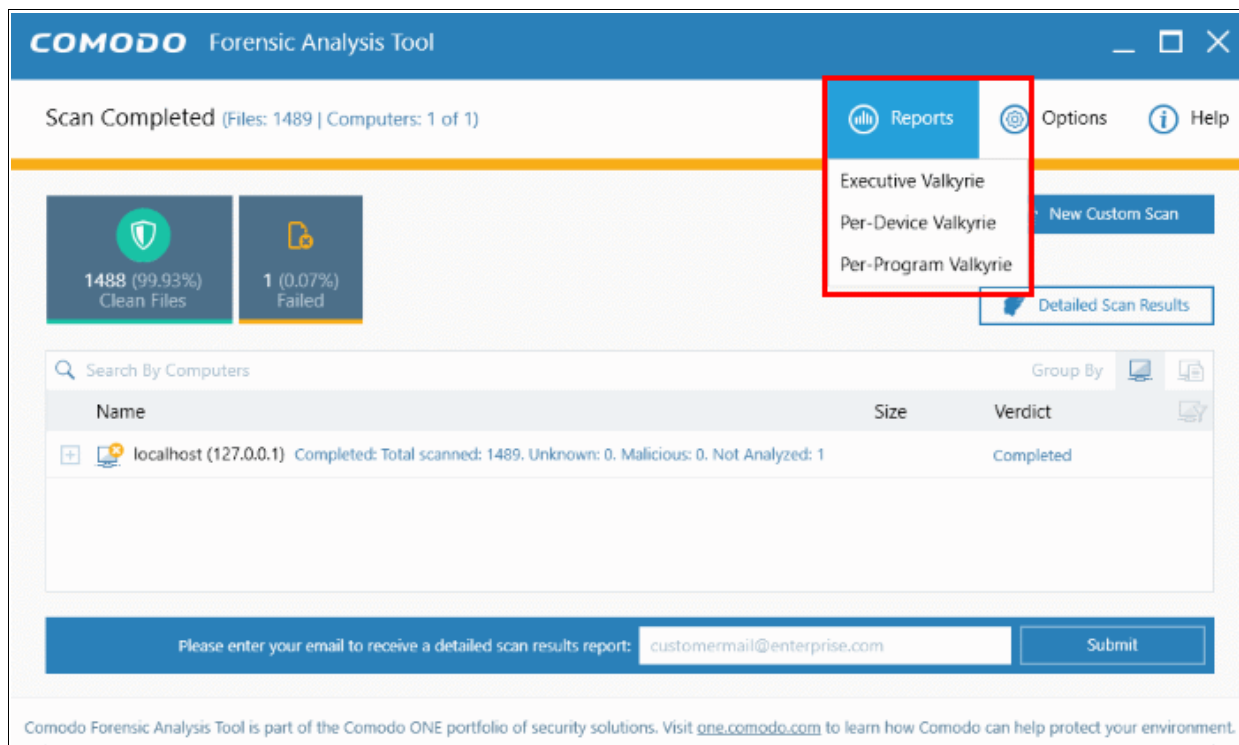
You can also view detailed Valkyrie results in the reports area. See [5. Reports](#) for more details.

## 5 Reports

Valkyrie reports are divided into three categories - Executive Valkyrie Report, Per Device Valkyrie Report and Per

## Program Valkyrie Report.

- The executive report provides an overview of scan parameters and charts which outline the number of devices scanned, the number of unknown programs found and more.
- The per device report details how many trusted programs, unknown programs and malicious programs were found on specific endpoints.
- The per program report shows how of each analyzed file impacted your network. This includes the names and IP addresses of the devices on which the file was found.



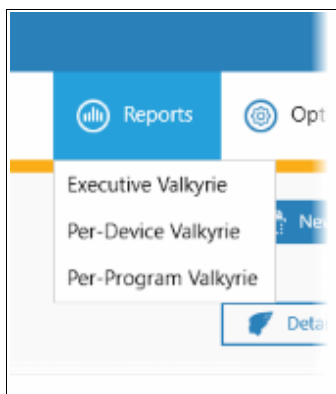
Refer to the following sections for more details:

- **Executive Valkyrie Report**
- **Device Valkyrie Report**
- **Program Valkyrie Report**

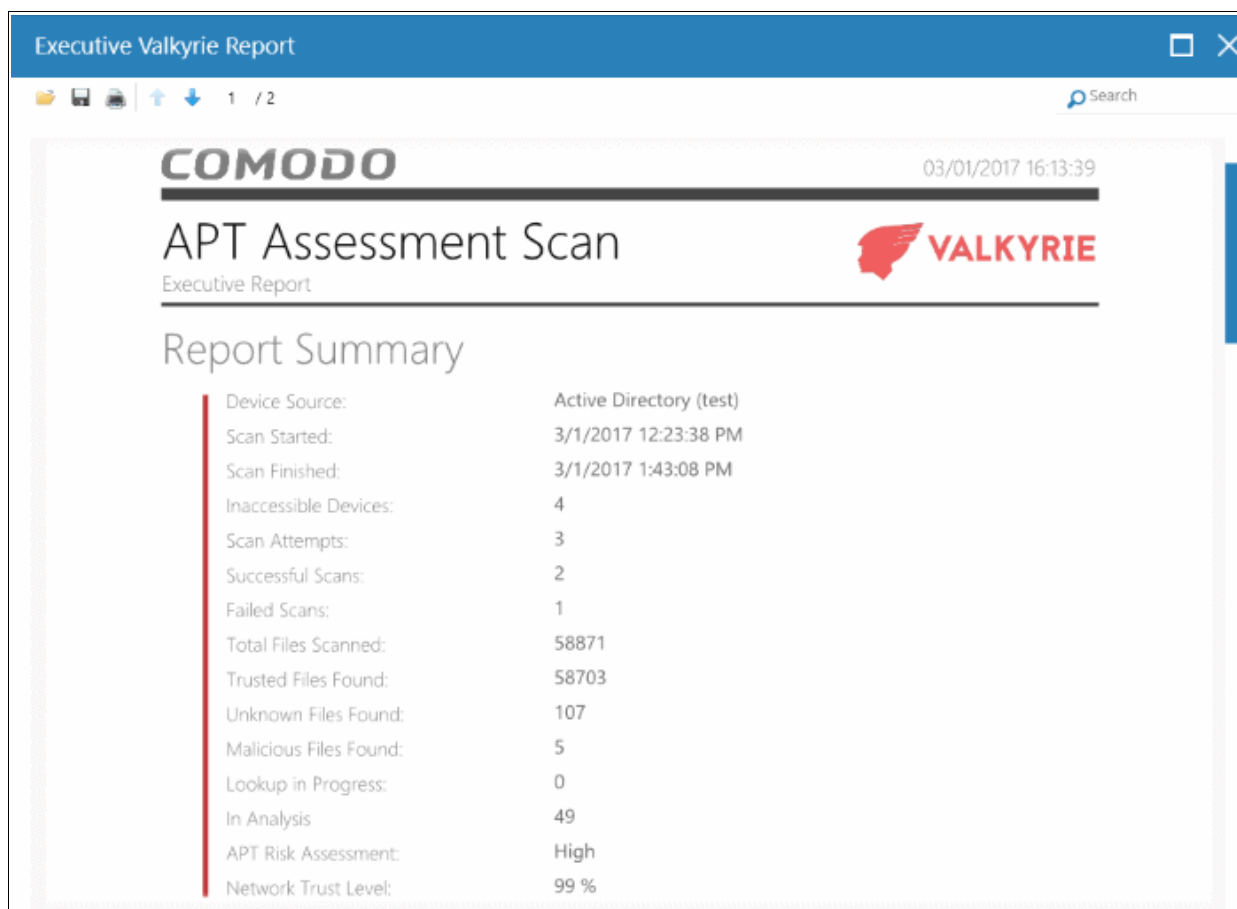
## 5.1 Executive Valkyrie Report

The executive report is a summary of scan results which provides details such as when the scan was started and finished, number of devices scanned and so on. The programs rating on the scanned devices and scanned devices' file rating are also available.

- To generate an executive report, click 'Reports' and then click 'Executive Valkyrie'.



The report will be generated and displayed:



Scroll down to view the full report. Note - please save the report if you wish to keep it for further reference. The report will not be available in the interface after the application is closed. To save the report, click the folder icon at the top-left, copy the report file and save in another location.

- **Report Summary** - General scan details, including the number of devices scanned, date and time of the scan, number of malware found and so on.
- **Summary Charts** - Details of programs found on scanned devices and the overall file rating of scanned devices.
  - **Programs Rating Over Scanned Devices** - Chart showing the trust rating of programs discovered on scanned devices. Shows the percentage of trusted programs, unknown programs, malicious programs, and programs for which analysis is still in progress.
  - **Scanned Devices Rating** - Pie chart which shows the percentage of devices that are safe, infected, at risk and not yet scanned.



## 5.2 Device Valkyrie Report

The 'Per Device Report' shows the trust rating of files on each device scanned. It includes details of malicious items found on each device, unknown files found, files that are still in-analysis and the path of files.

- To generate a 'Per Device' report, click 'Reports' and then 'Per Device Valkyrie'.

The report will be generated and displayed:

**COMODO** 3/1/2017 4:59:49 PM

---

# APT Assessment Scan

Detailed Per-Device Report

---

## Report Summary

Device Source:	Active Directory (test)
Scan Started:	3/1/2017 12:23:38 PM
Scan Finished:	3/1/2017 1:43:08 PM
Inaccessible Devices:	4
Scan Attempts:	3
Successful Scans:	2
Failed Scans:	1
Total Files Scanned:	58871
Trusted Files Found:	58703
Unknown Files Found:	107
Malicious Files Found:	5
Lookup In Progress:	0
In Analysis:	49
APT Risk Assessment:	High
Network Trust Level:	99 %

Scroll down to view the full report. Note - please save the report if you wish to keep it for further reference. The report will not be available in the interface after the application is closed. To save the report, click the folder icon at the top-left, copy the report file and save in another location.

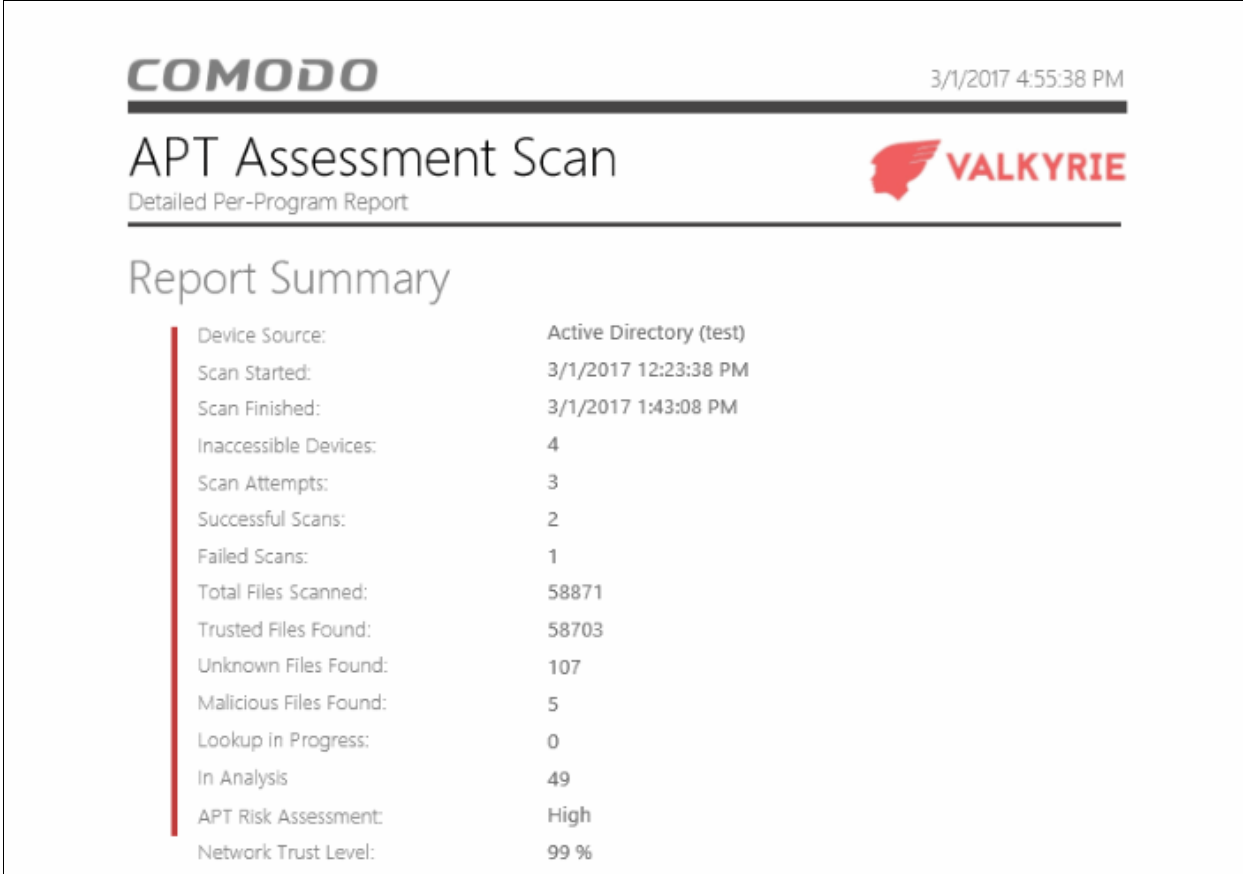
- **Report Summary** - General scan details, including the number of devices scanned, date and time of the scan, number of malware found and so on.
- **Summary Chart** - Bar chart showing the top 10 endpoints that contain unknown/malware files.
- **Details per Device** - Inventory of files discovered on each endpoint. This includes the name of the device, quantity of malicious/unknown files, the path of each malicious/unknown file and more.

## 5.3 Program Valkyrie Report

The 'Per Program Report' shows the footprint of each file analyzed by Valkyrie. This includes details of each malicious/unknown file found, the devices on which they were found, the path of the files and more.

- To generate a 'Per Program' report, click 'Reports' and then click 'Per Program Valkyrie'.

The report will be generated and displayed:




**COMODO** 3/1/2017 4:55:38 PM

---

## APT Assessment Scan

Detailed Per-Program Report



---

### Report Summary

Device Source:	Active Directory (test)
Scan Started:	3/1/2017 12:23:38 PM
Scan Finished:	3/1/2017 1:43:08 PM
Inaccessible Devices:	4
Scan Attempts:	3
Successful Scans:	2
Failed Scans:	1
Total Files Scanned:	58871
Trusted Files Found:	58703
Unknown Files Found:	107
Malicious Files Found:	5
Lookup in Progress:	0
In Analysis	49
APT Risk Assessment:	High
Network Trust Level:	99 %

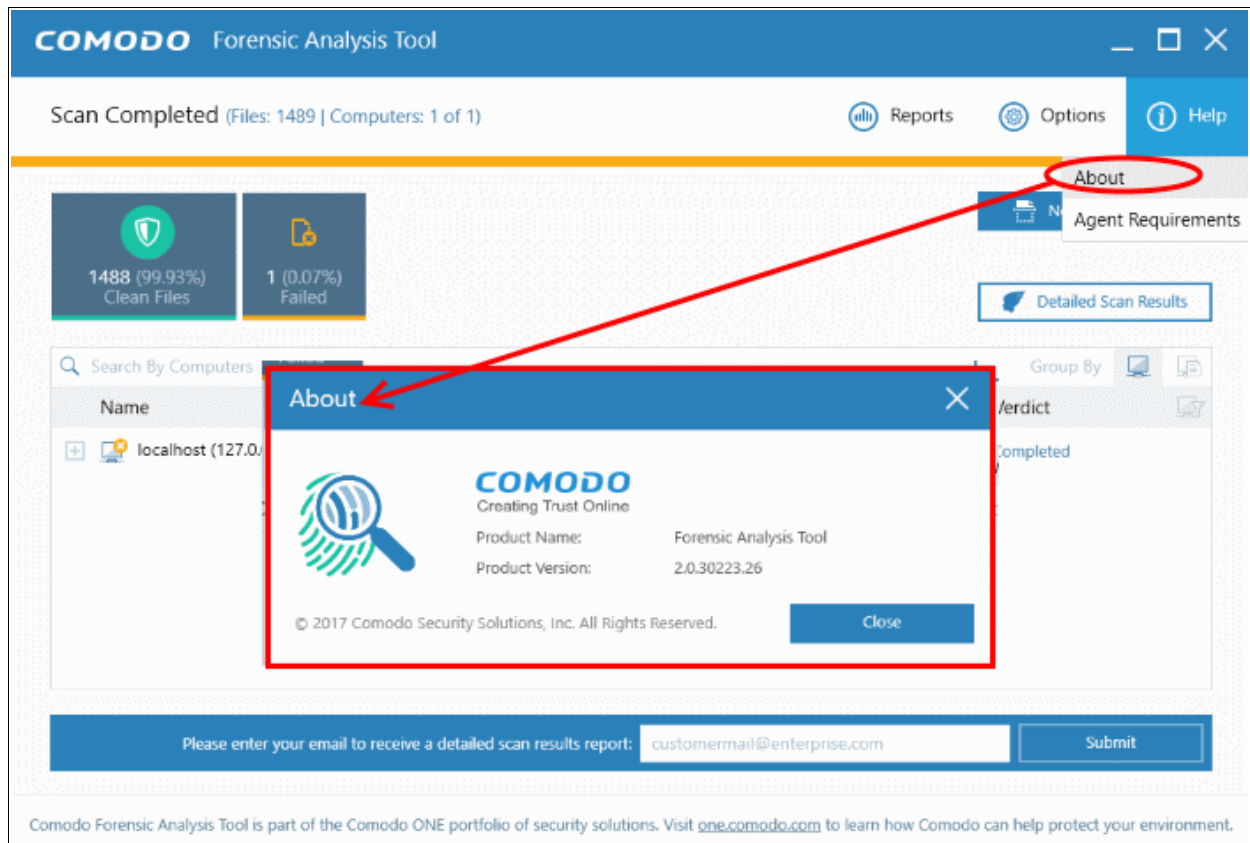
Scroll down to view the full report. Note - please save the report if you wish to keep it for further reference. The report will not be available in the interface after the application is closed. To save the report, click the folder icon at the top-left, copy the report file and save in another location.

- **Report Summary** - General scan details, including the number of devices scanned, date and time of the scan, number of malware found and so on.
- **Summary Chart** - Shows the top 10 unknown/malicious programs in bar graph.
- **Details per Program** - Granular report showing the impact of each analyzed file on your network. This includes the names and IP addresses of the devices on which it was found on and the overall trust rating of the program.

## 6 About Comodo Forensic Analysis

The 'About' dialog provides the details of the product and its version number.

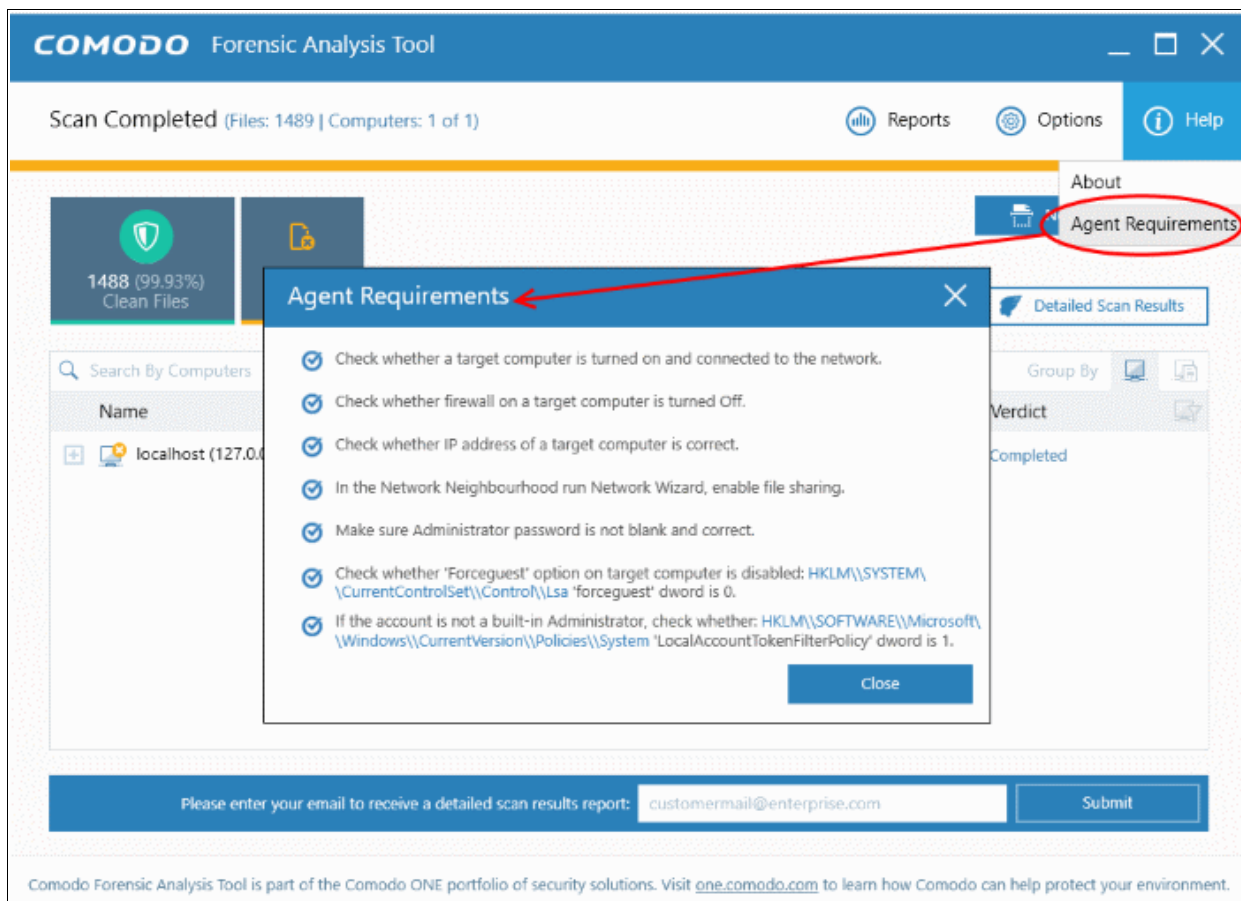
- To view the product details and its version number, click 'About' from the 'Help' in menu.



- Product Name - The full name of the product
- Product Version - The version number of the product
- Click the 'Close' button to return to the application.

## 7 Agent Requirements

The 'Agent requirements' item in the help menu provides configuration advice to help you run scans successfully:



## About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

## About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)