COMODO
Creating Trust Online®

Comodo Forensic Analysis

Software Version 4.0

Administrator Guide

Guide Version 4.0.030119

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

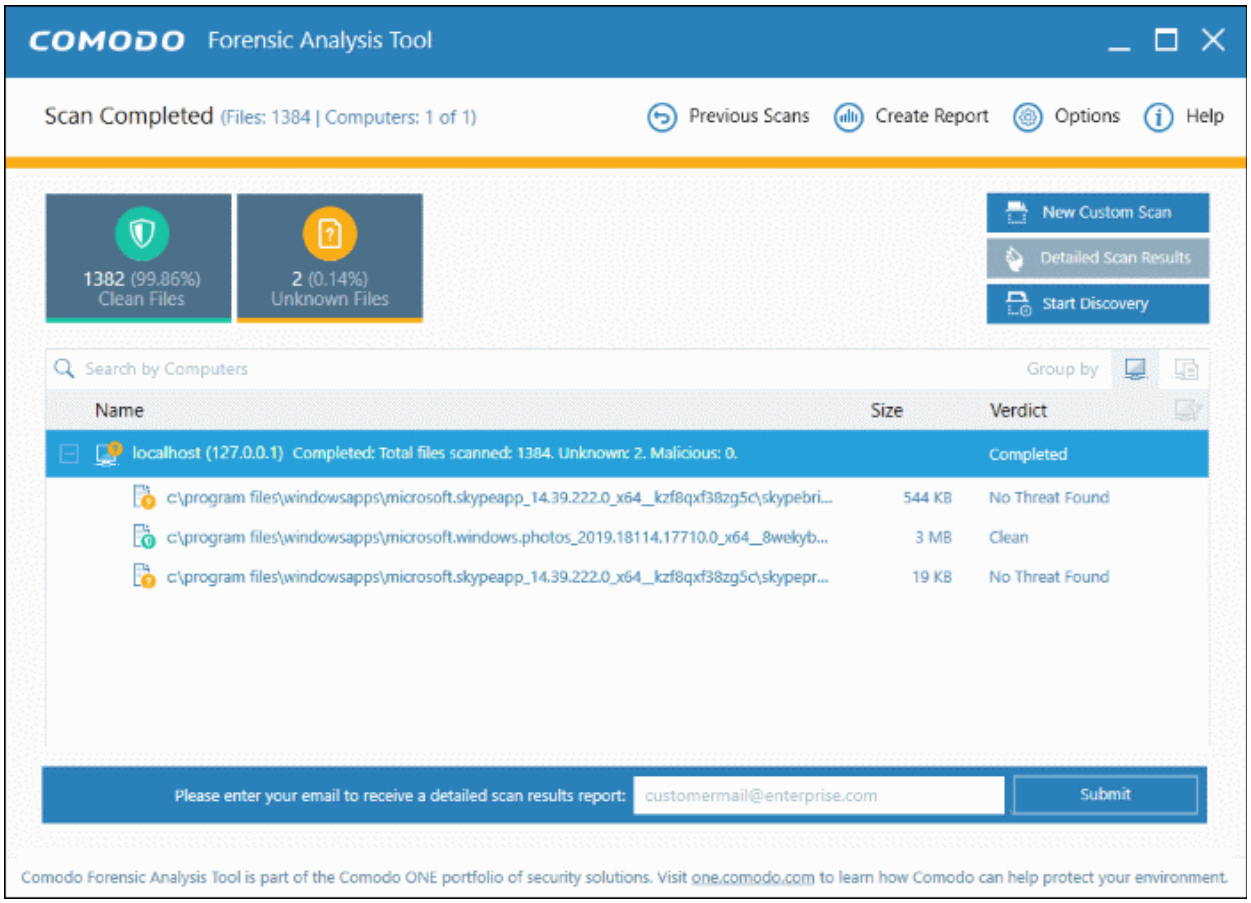
Table of Contents

1 Introduction to Comodo Forensic Analysis....3
2 Run Forensic Analysis....4
2.1 The Main Interface....5
3 Scan Computers....6
3.1 Scan computers in an Active Directory domain....8
3.2 Scan Computers in a Workgroup....13
3.3 Scan Computers by Network Addresses....20
3.4 Scan your Local Computer....24
4 Scan Results....30
5 Discover Computers....33
6 Reports....35
6.1 Executive Report....36
6.2 Device Report....37
6.3 Program Report....38
7 About Comodo Forensic Analysis....39
8 Agent Requirements....41
About Comodo Security Solutions....42

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 antivirus catches up to it. These malicious files reside on the victim's computer during this whole time, 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.



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. The scan discovers all computers available in a given network
- 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

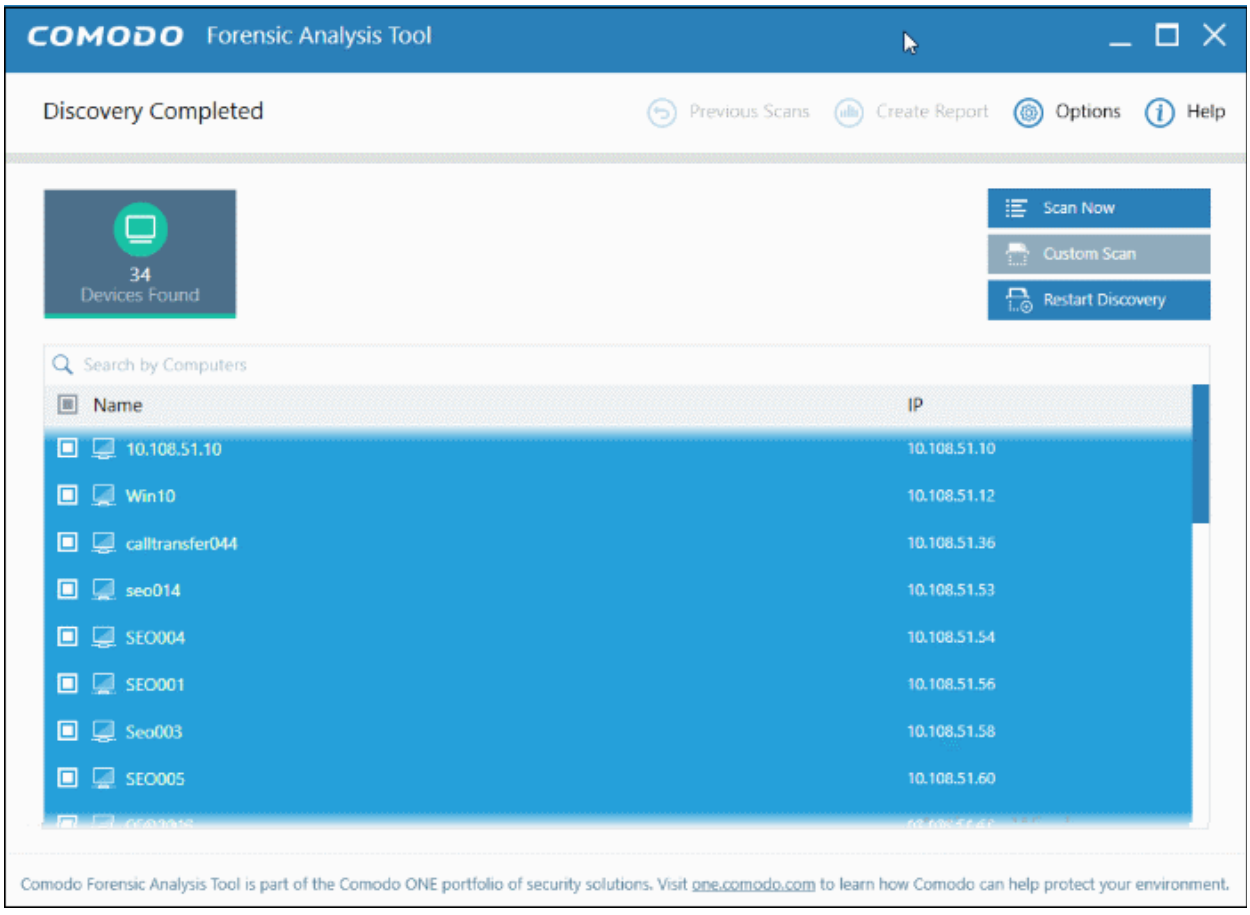
This guide takes you through the use of Comodo Forensic Analysis and is broken down into the following sections:

- Introduction to Comodo Forensic Analysis
- Run Forensic Analysis
- Scan Computers
  - Scan Computers in an AD Domain
  - Scan Computers in a Workgroup
  - Scan Computers by Network Addressees
  - Scan your Local Computer
- Scan Results
- Discover Computers
- Reports
  - Executive Report
  - Device Report
  - Program Report

2 Run Forensic Analysis

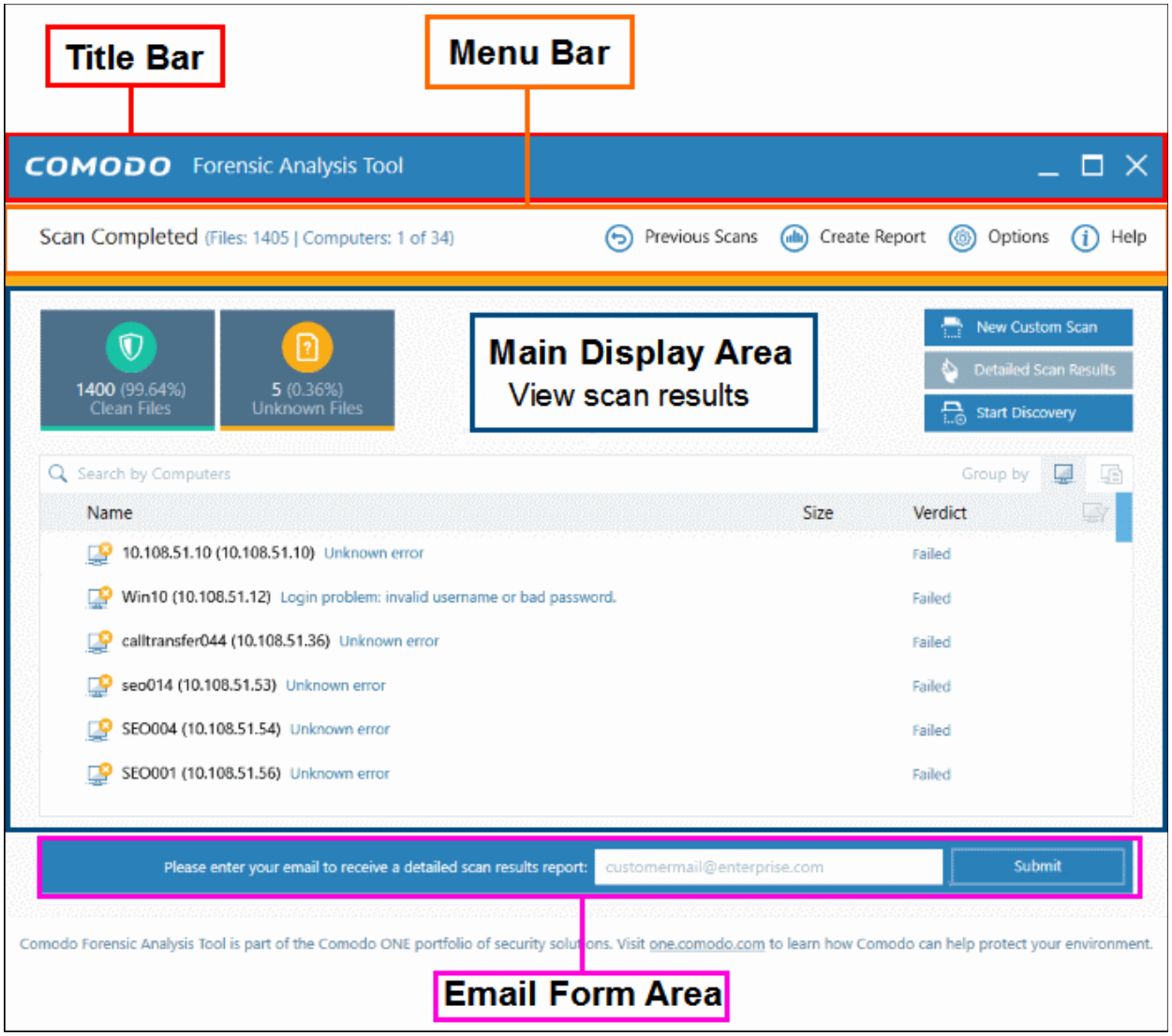
Comodo Forensic Analysis can be downloaded from **https://enterprise.comodo.com/freeforensicanalysis/**

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



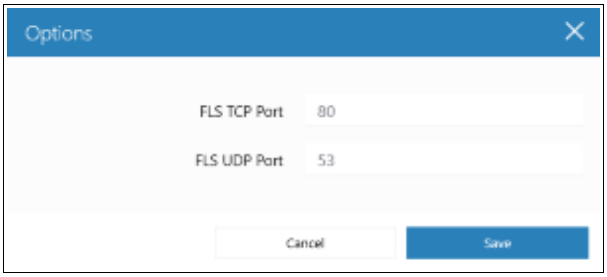
2.1 The Main Interface

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.



  - **Create Reports** - Generate a detailed report of the scan results. See '**Reports**' for more details.
  - **Previous Scans** - Shows your most recent scans.
  - **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.

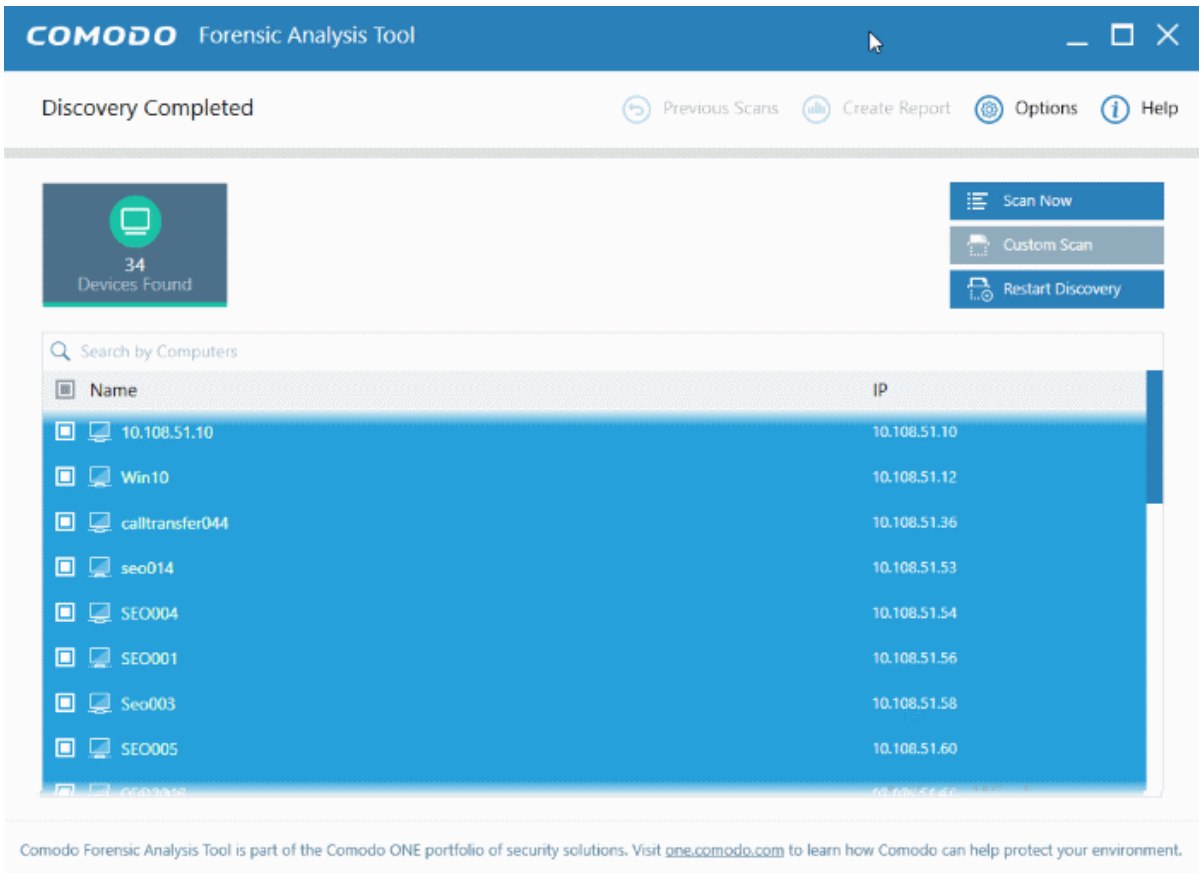
- **Main Display Area** - Displays details of scanned endpoints and the results from Valkyrie. Refer to the sections '**Scan Computers**' and '**Scan Results**' for more details. Also contains controls for launching local and custom scans:
  - **Scan Now** - Scan endpoints on your local network to identify unknown files. Refer to section '**Scanning Computers**' for more details.
  - **New Custom Scan** - Scan endpoints in a Workgroup, Active Directory, or Network Addresses. You can also scan your local computer. Refer to the section '**Scan Computers**' for more details.
  - **Detailed Scan Results** – Opens Valkyrie results. Valkyrie is Comodo's file-verdict system, which comprehensively tests files to see if they exhibit malicious behaviour.
  - **Start/Restart Discovery** – Identify the number of machines available in the given network. See **Discover Computers** for more details.
- **Email Form Area** - Enter your email address after the Valkyrie analysis is complete to receive a detailed scan report.

3 Scan Computers

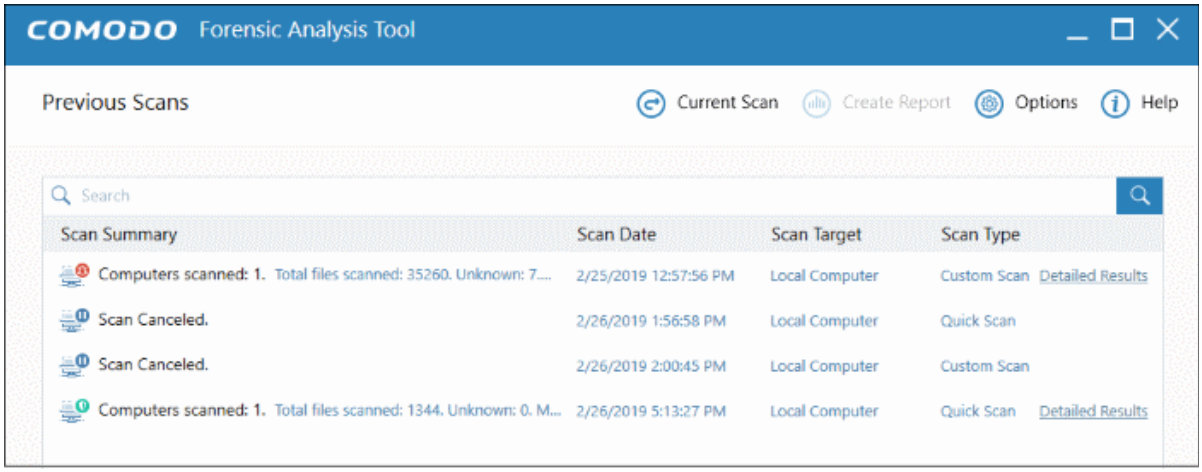
You can use any of the following methods to scan your target computers:

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

Unknown files discovered by the scan are automatically submitted to Comodo Valkyrie for further analysis. The Forensic Analysis tool shows results from the initial scan, and in-depth results from Valkyrie.



- **Previous Scans** – View the results of your recent scans in chronological order. Double-click on the name of the scan to view the last CFA scan result page
- **Detailed Results** - View Valkyrie results. Files with an 'unknown' trust rating are uploaded to Valkyrie for more in-depth tests.
- **Current Scan** - Return to the present results screen
- You can also use the search box to look for specific scan results:



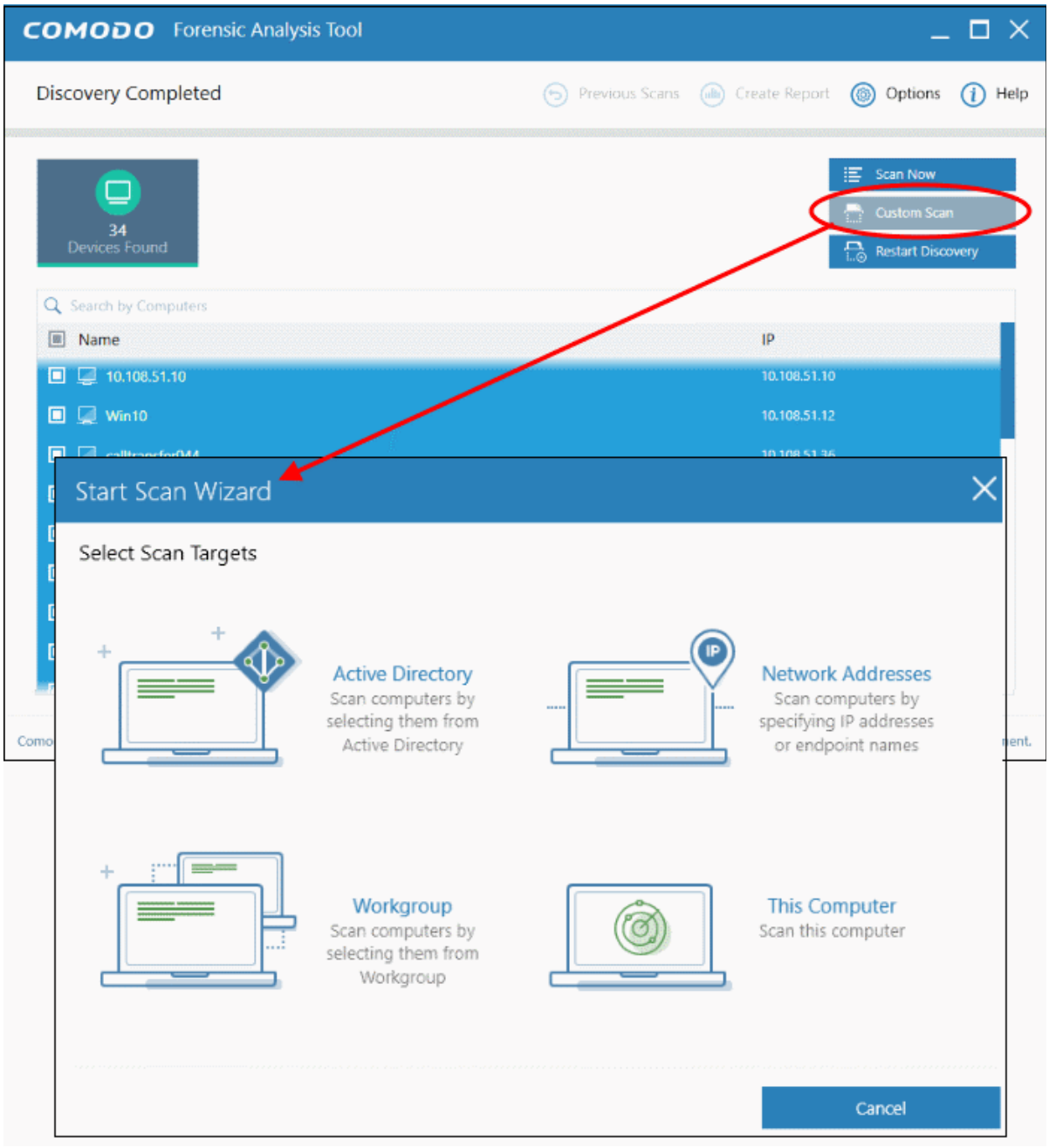
Refer to the following sections for more details:

- **Scan computers in an Active Directory domain**
- **Scan computers in a Workgroup**
- **Scan computers by Network Address**
- **Scan your Local Computer**

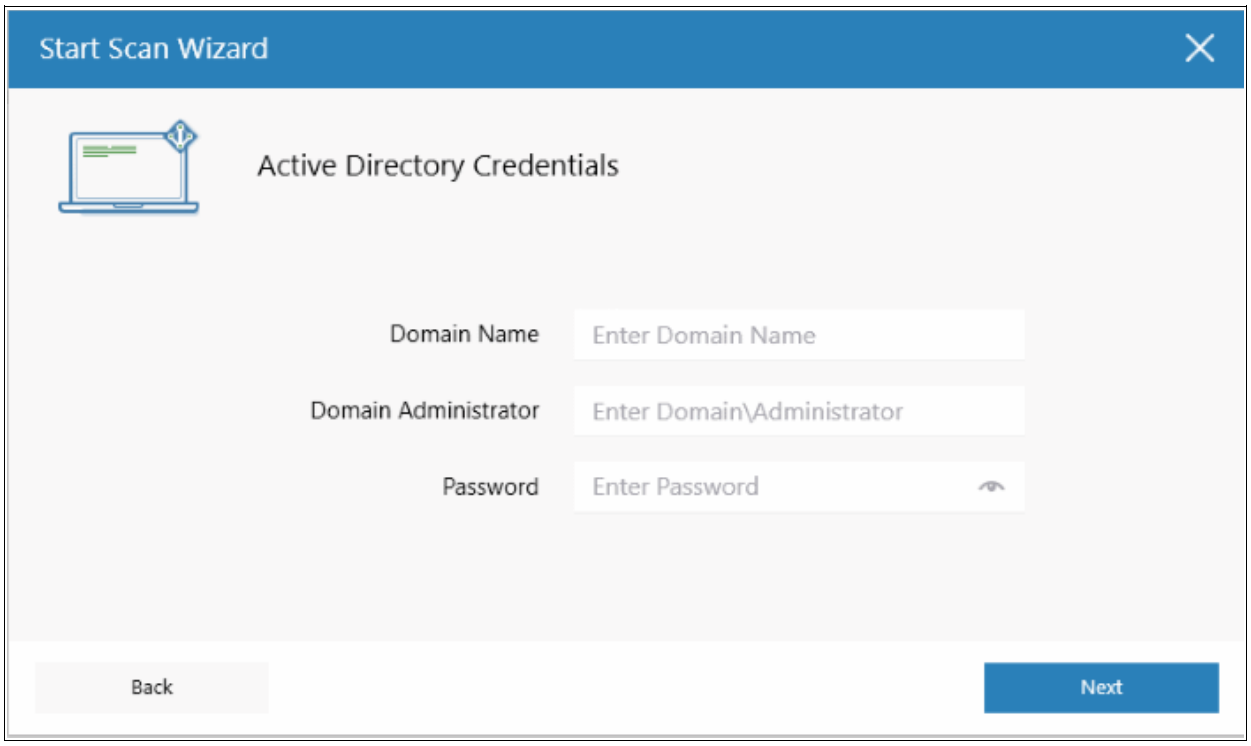
3.1 Scan computers in an Active Directory domain

The Active Directory method lets you import and scan all endpoints in a domain.

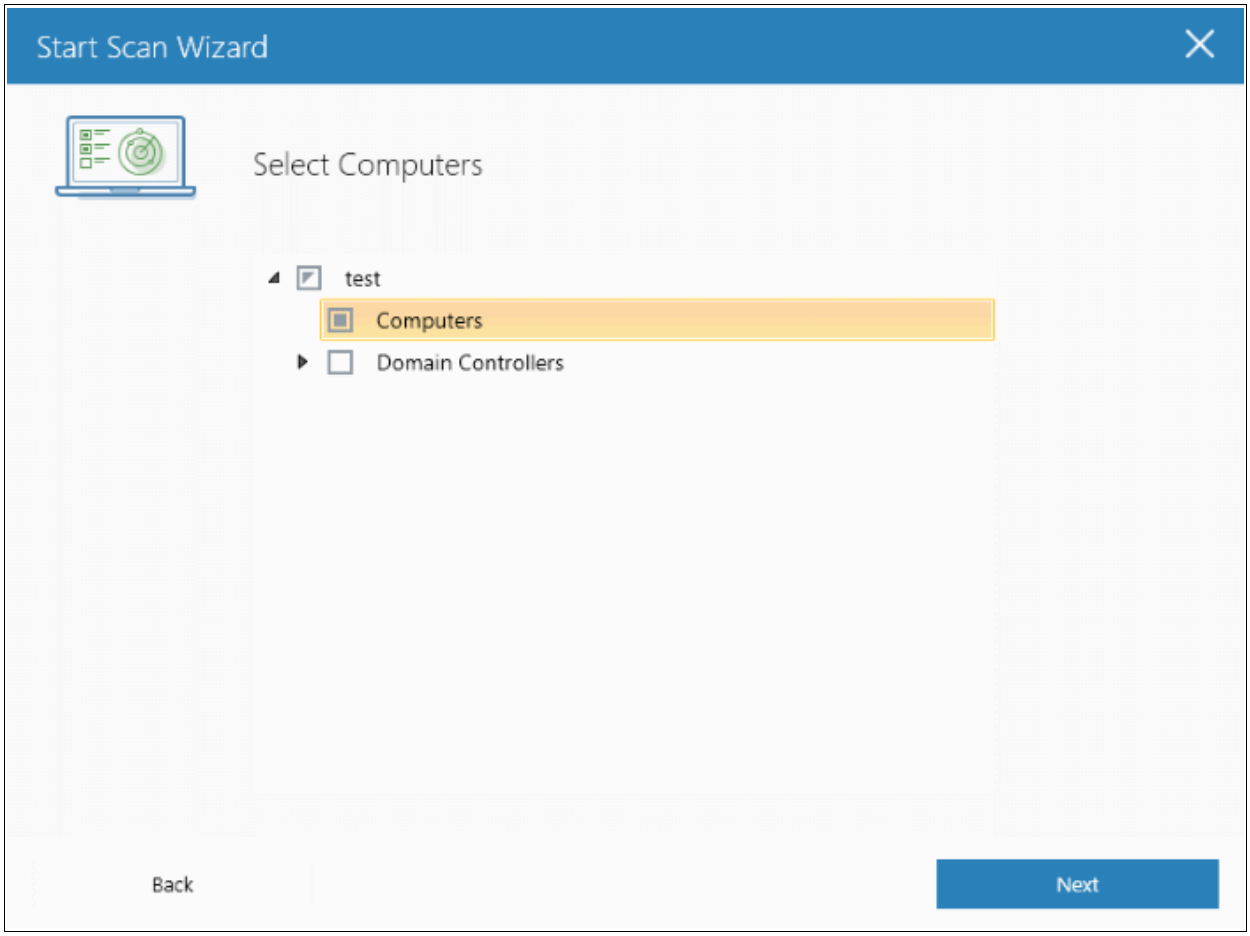
- Click 'Custom Scan' on the home screen to open the scan wizard:

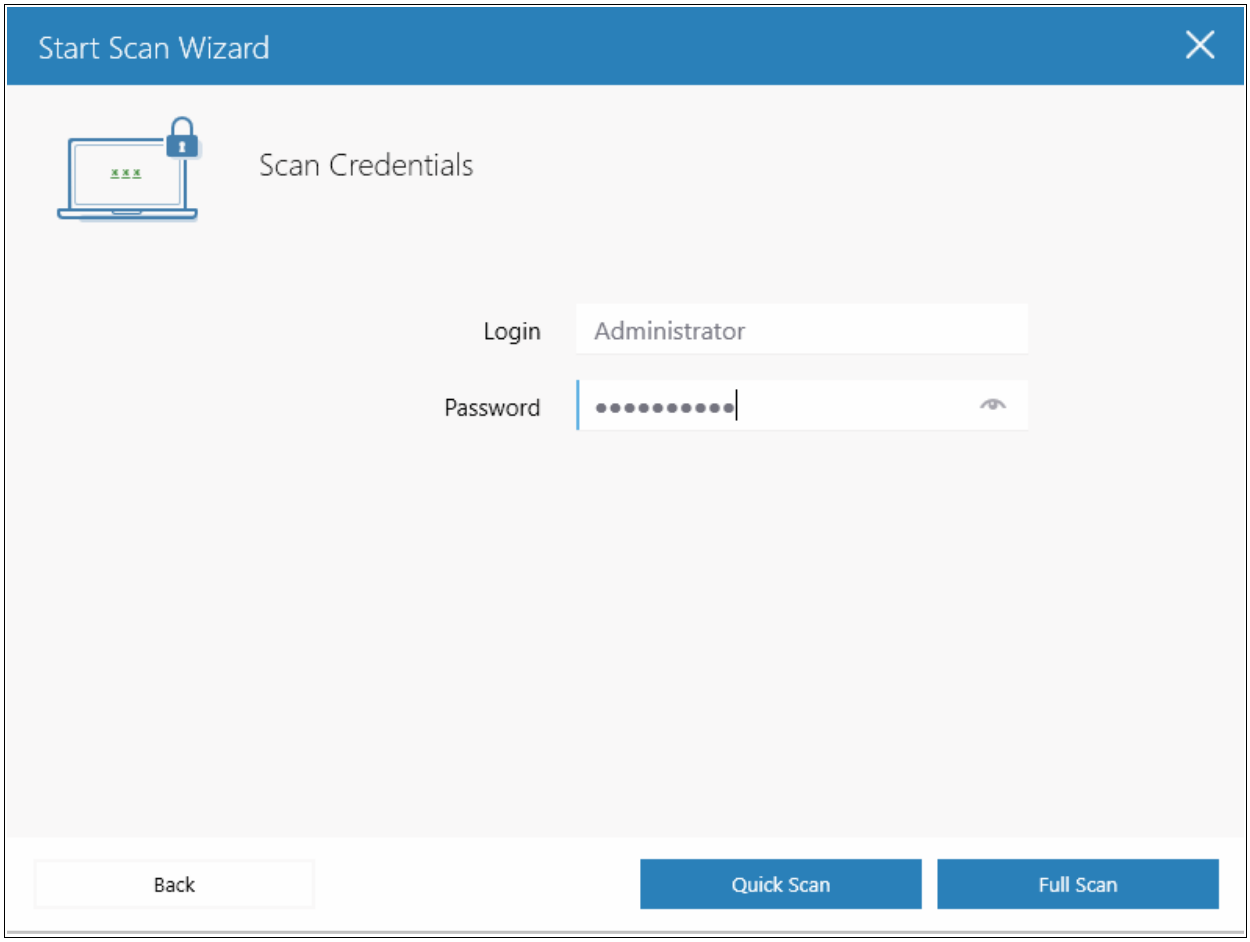


- Select 'Active Directory' to open the AD configuration screen.
- Enter the domain name and login details of your Active Directory domain:

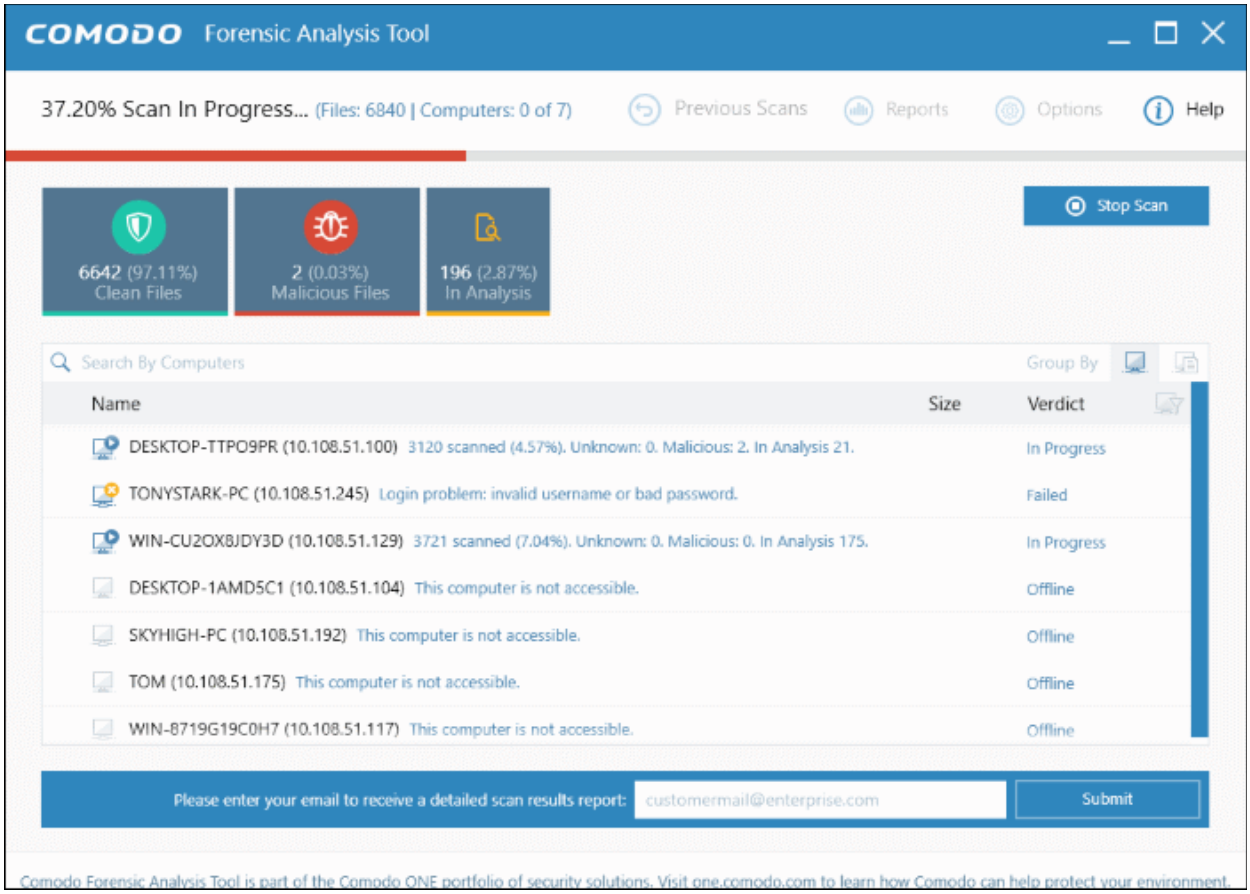


- After successful authentication, the 'Select Computers' screen will open. Choose the endpoints you want to scan then click next:



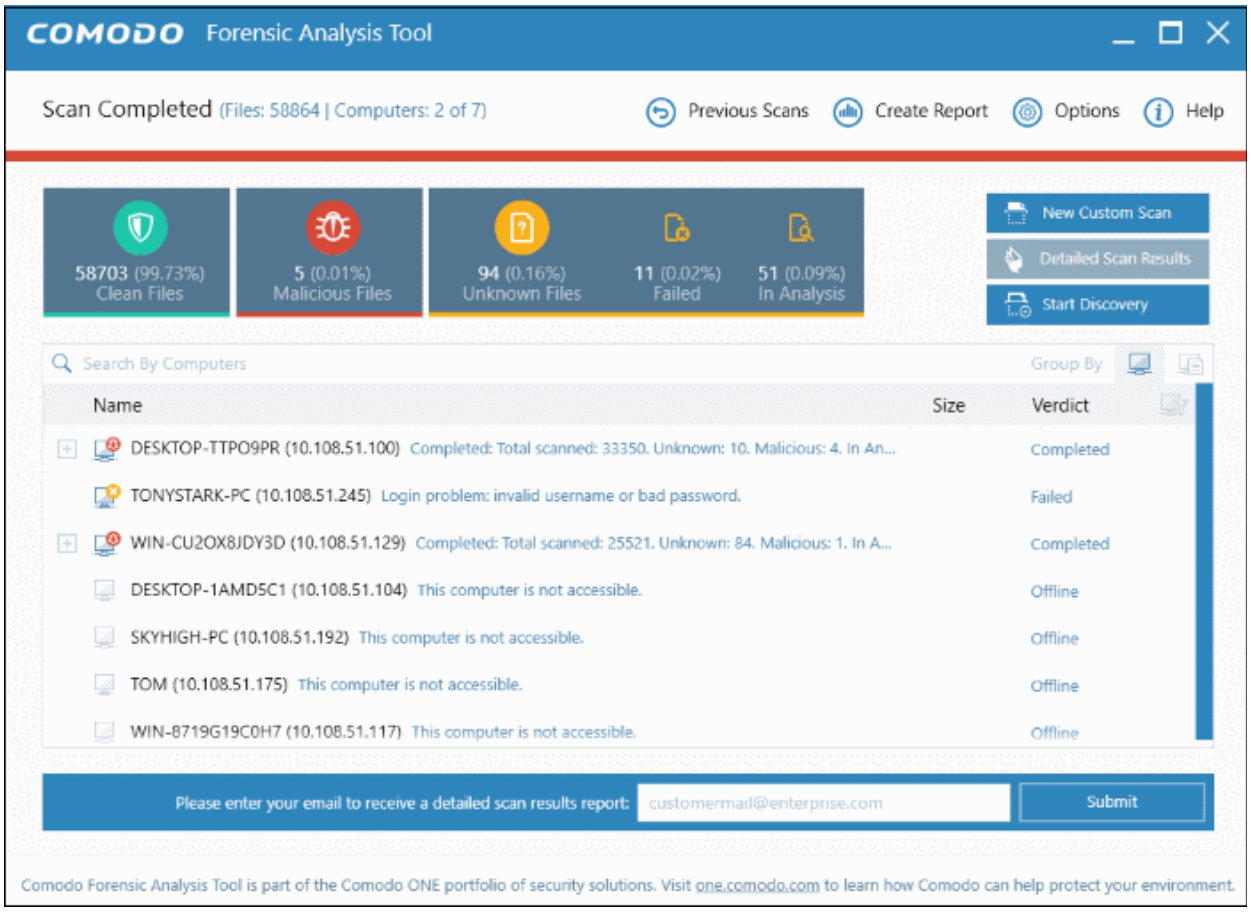


- Next, choose one of the following scan types:
  - **Quick Scan:** Scans critical and commonly infected areas of target endpoints
  - **Full Scan:** Scans all files and folders on target endpoints.

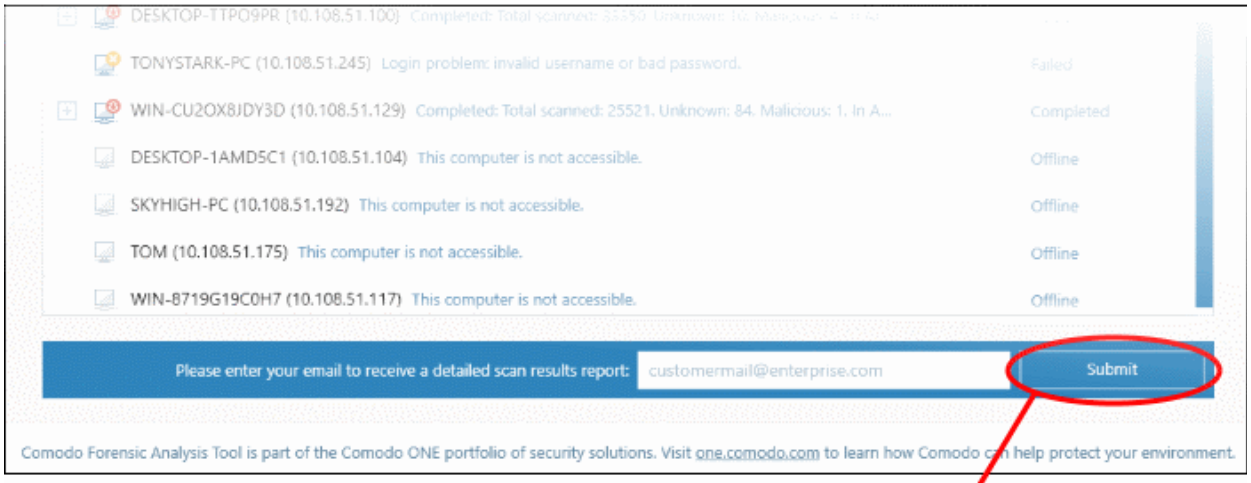


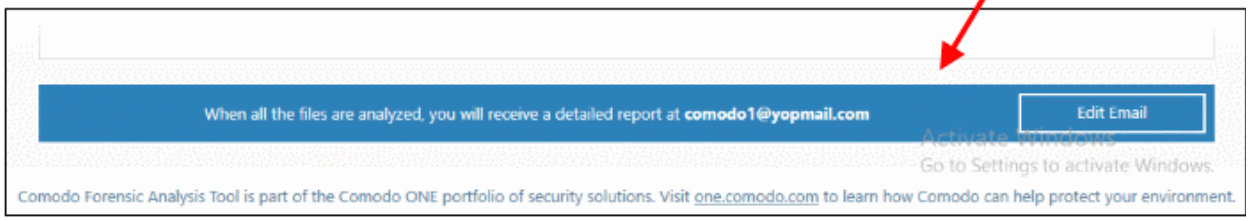
Scan progress is shown for each computer. Overall progress is shown on the title bar.

- **Stop Scan** - Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:

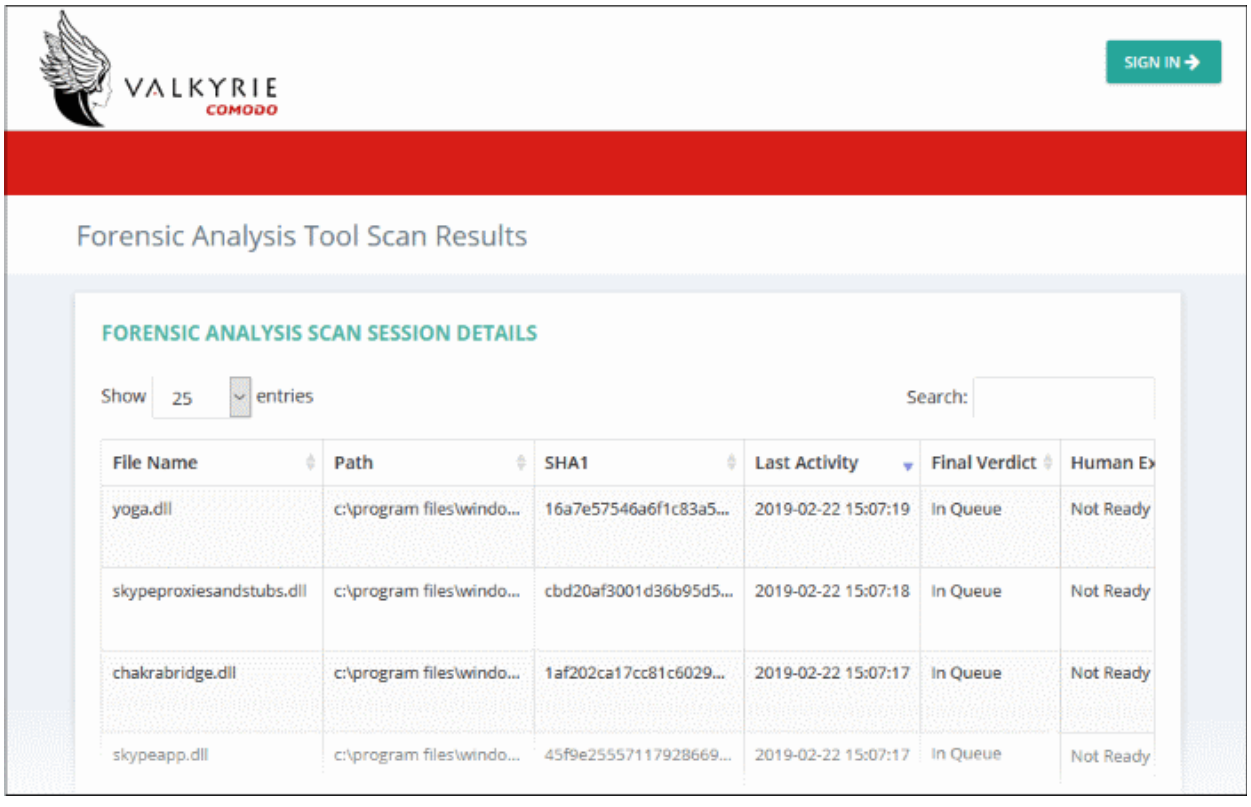


- There are two ways you can view the results:
  - **Group by Computer**: Shows each computer on a separate row. Expand any row to view unknown files found on that computer.
  - **Group by File**: Shows each unknown file on a separate row. Expand any row to view the endpoints on which the file was found.
- **Detailed Scan Results** – Receive a report from Comodo Valkyrie about the unknown files on your network. Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.
  - Enter your email address in the field at the bottom
  - Click 'Submit' to receive the report at the address you supplied.





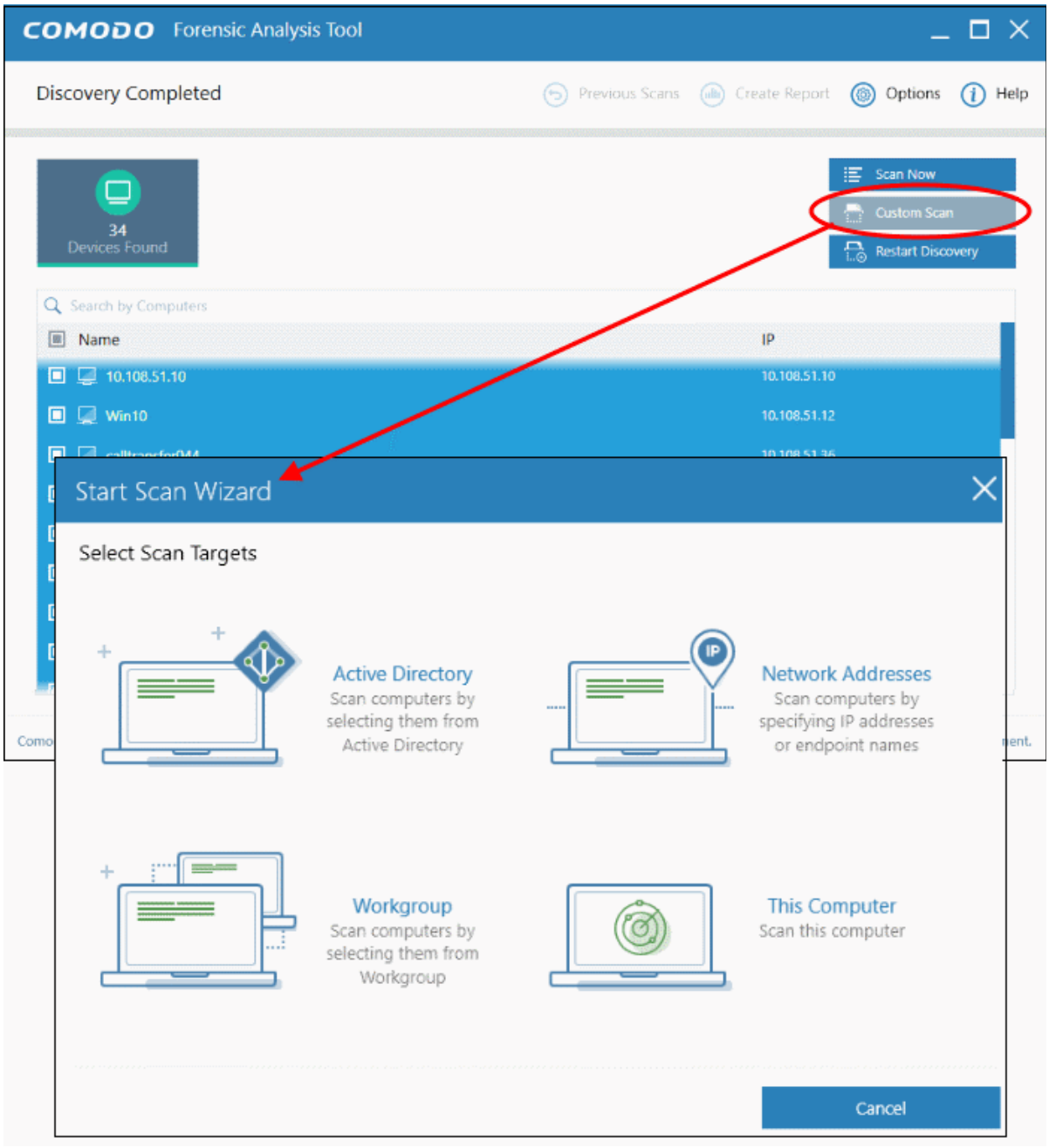
Valkyrie results in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.



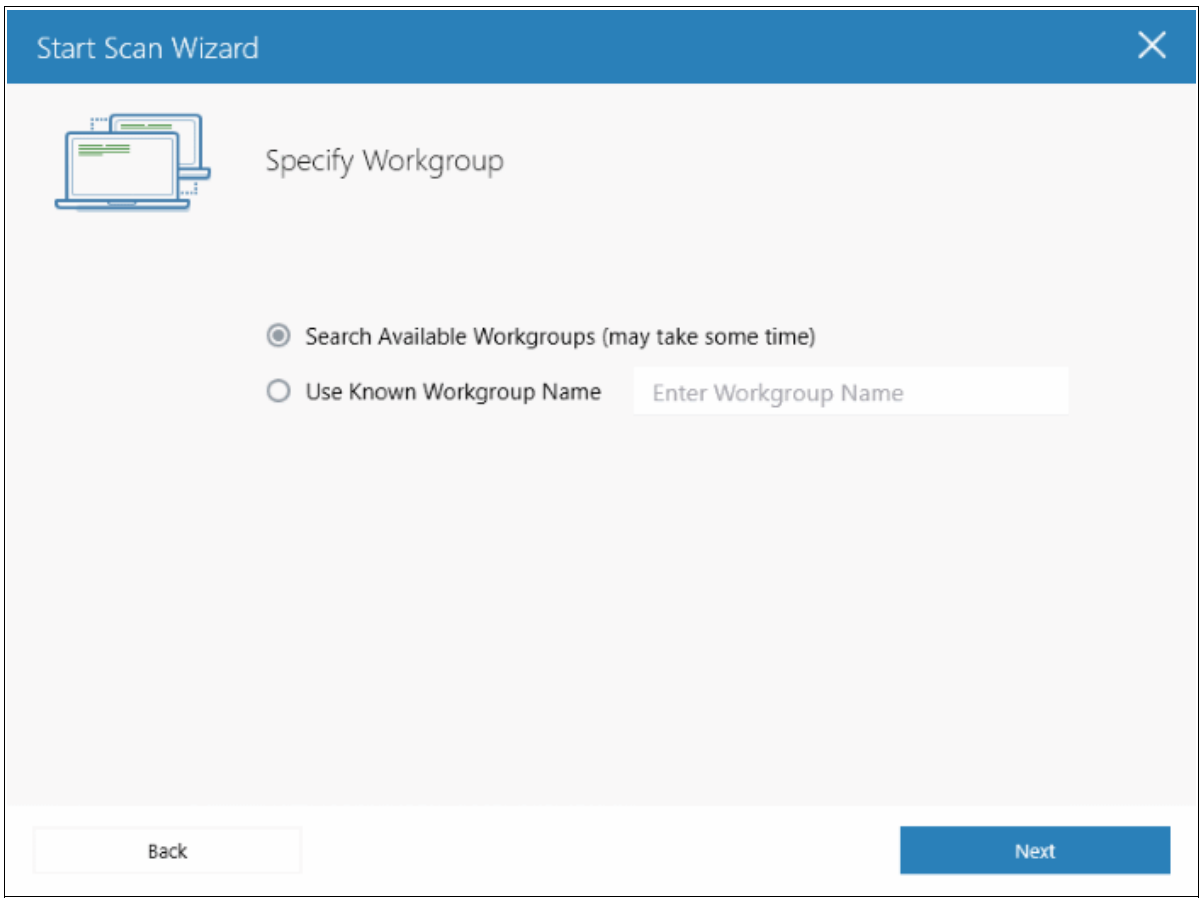
Refer to the section '**Scan Results**' for more details.

3.2 Scan Computers in a Workgroup

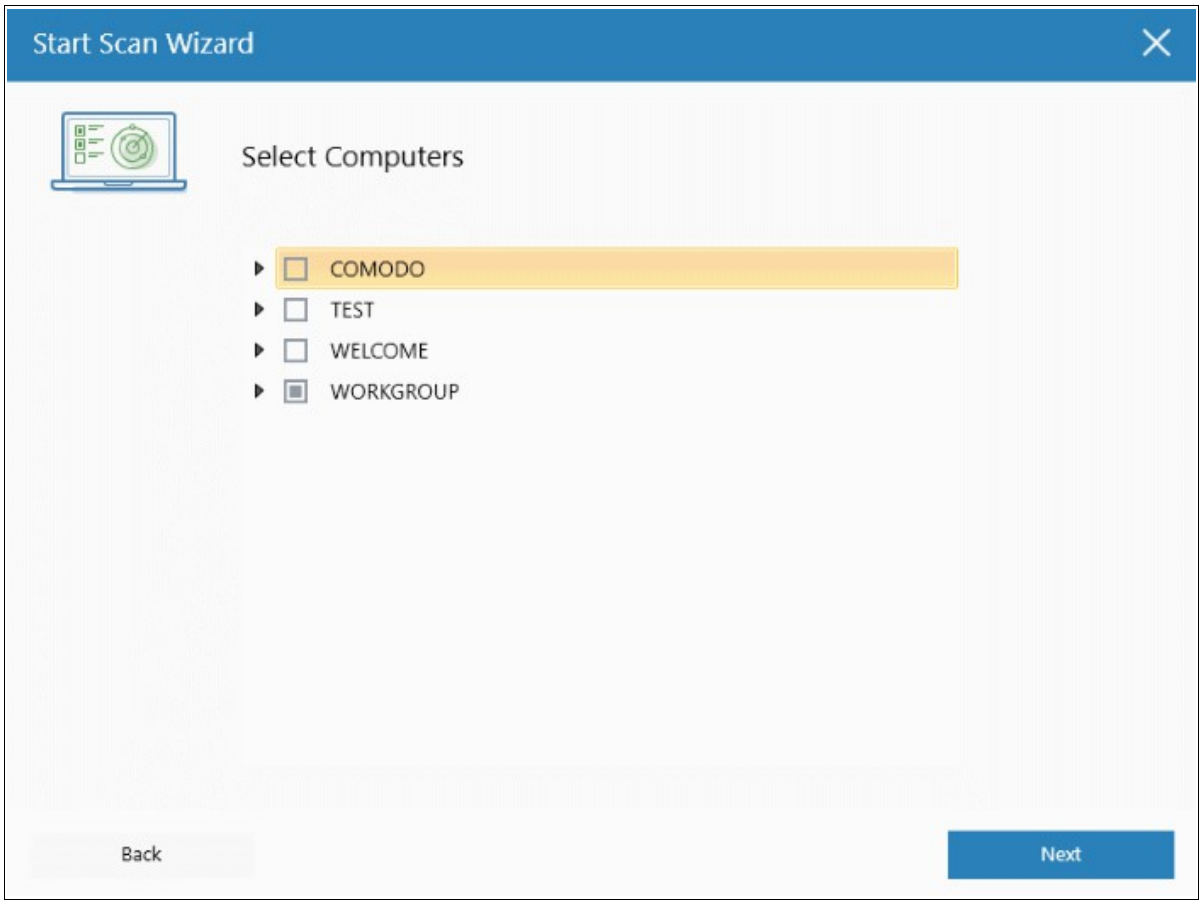
- Click 'Custom Scan' on the home screen to open the scan wizard:



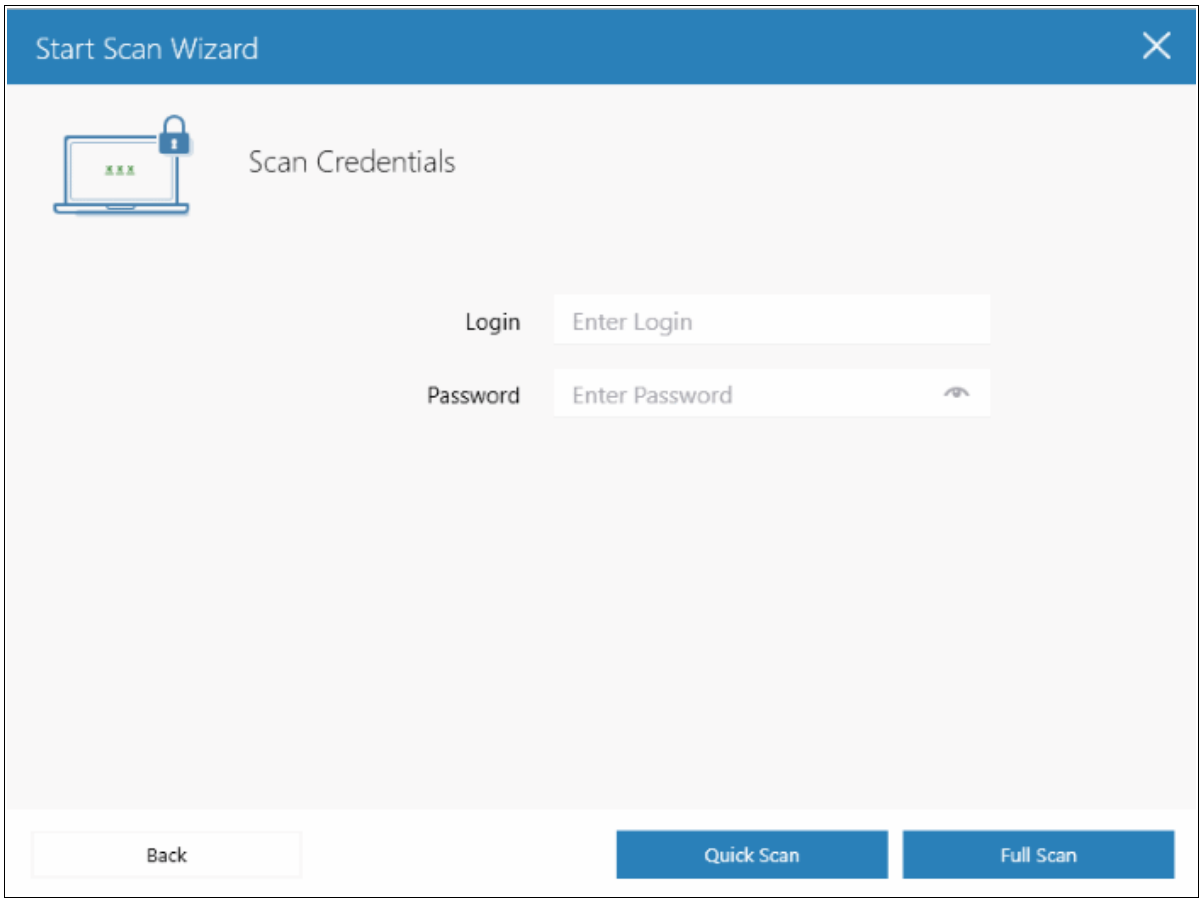
- Click 'Workgroup'
- Select from available Workgroups, or enter the name of a Workgroup



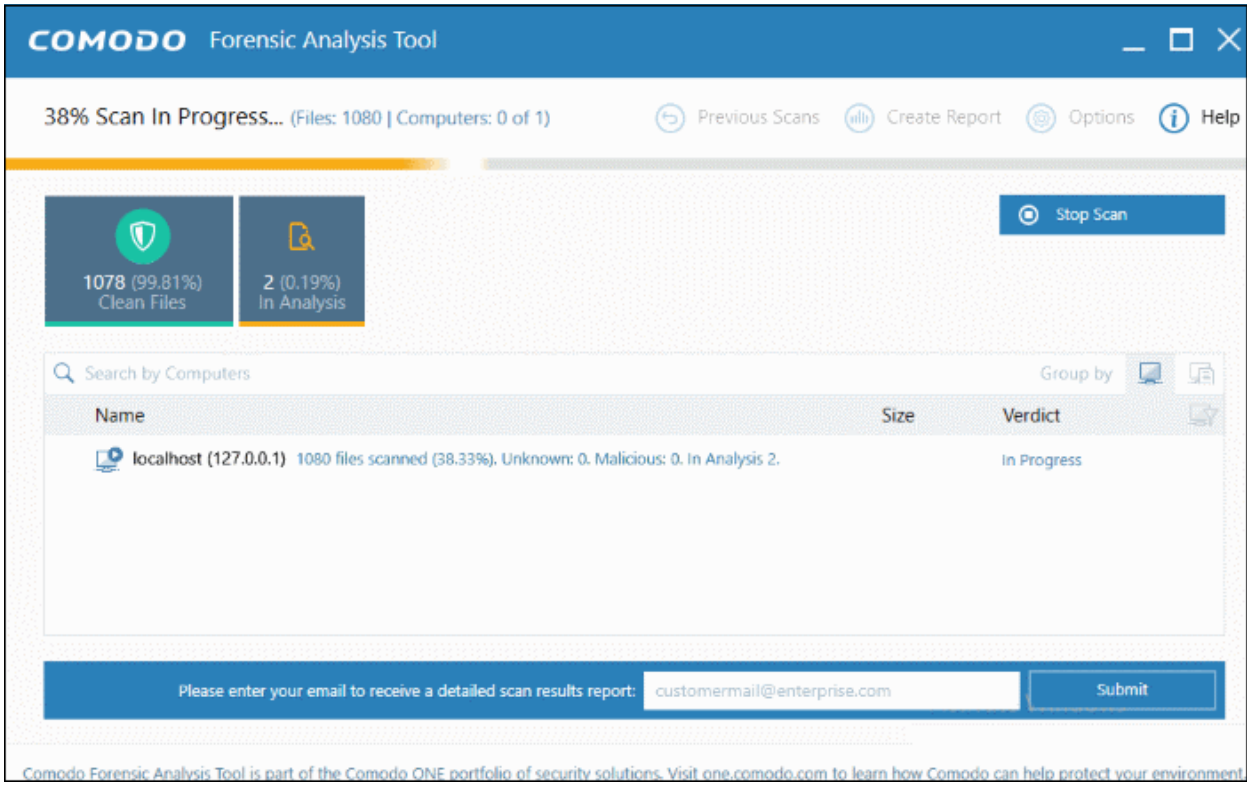
- Select the computers you want to scan.



- 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.

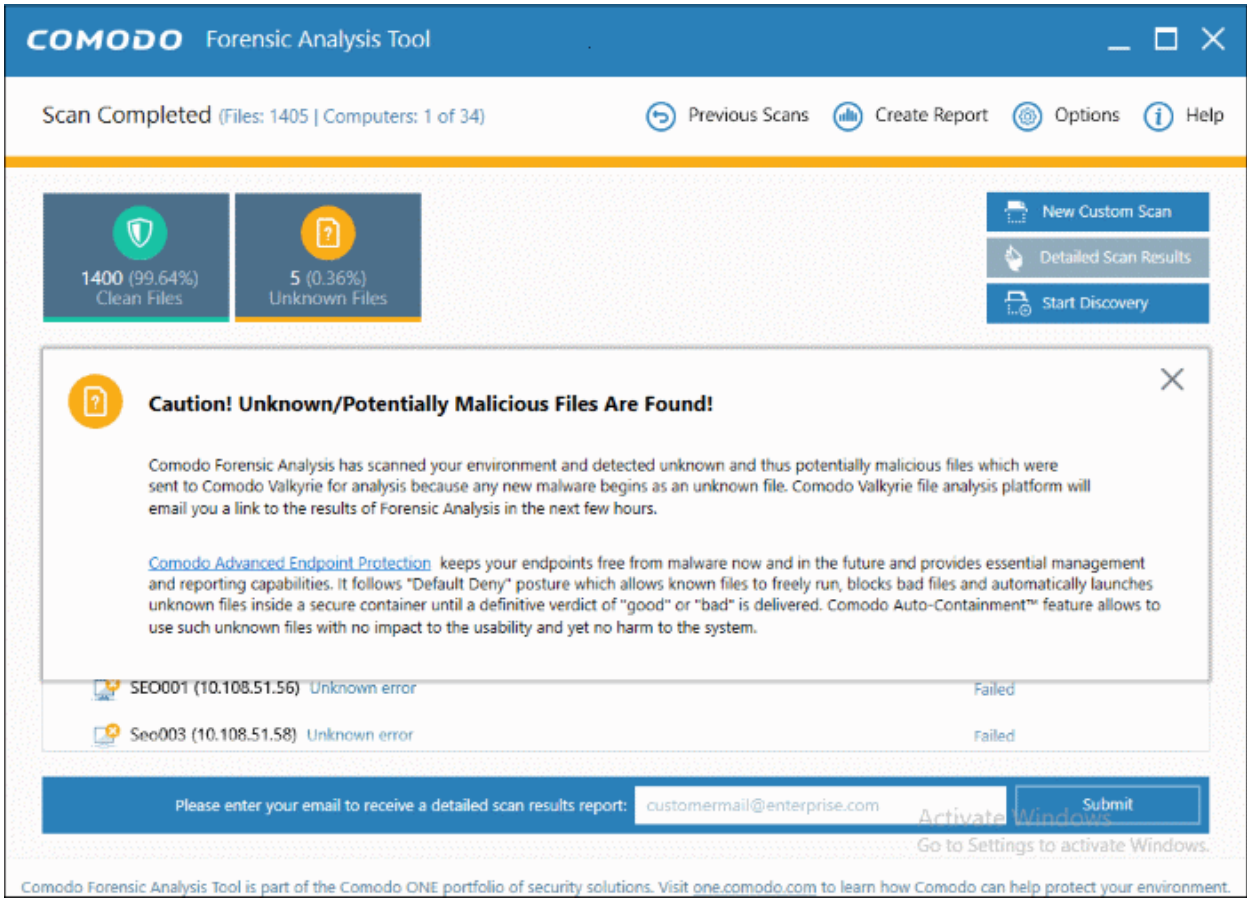


After successful authentication, the scanning of endpoints in the Workgroup will start.

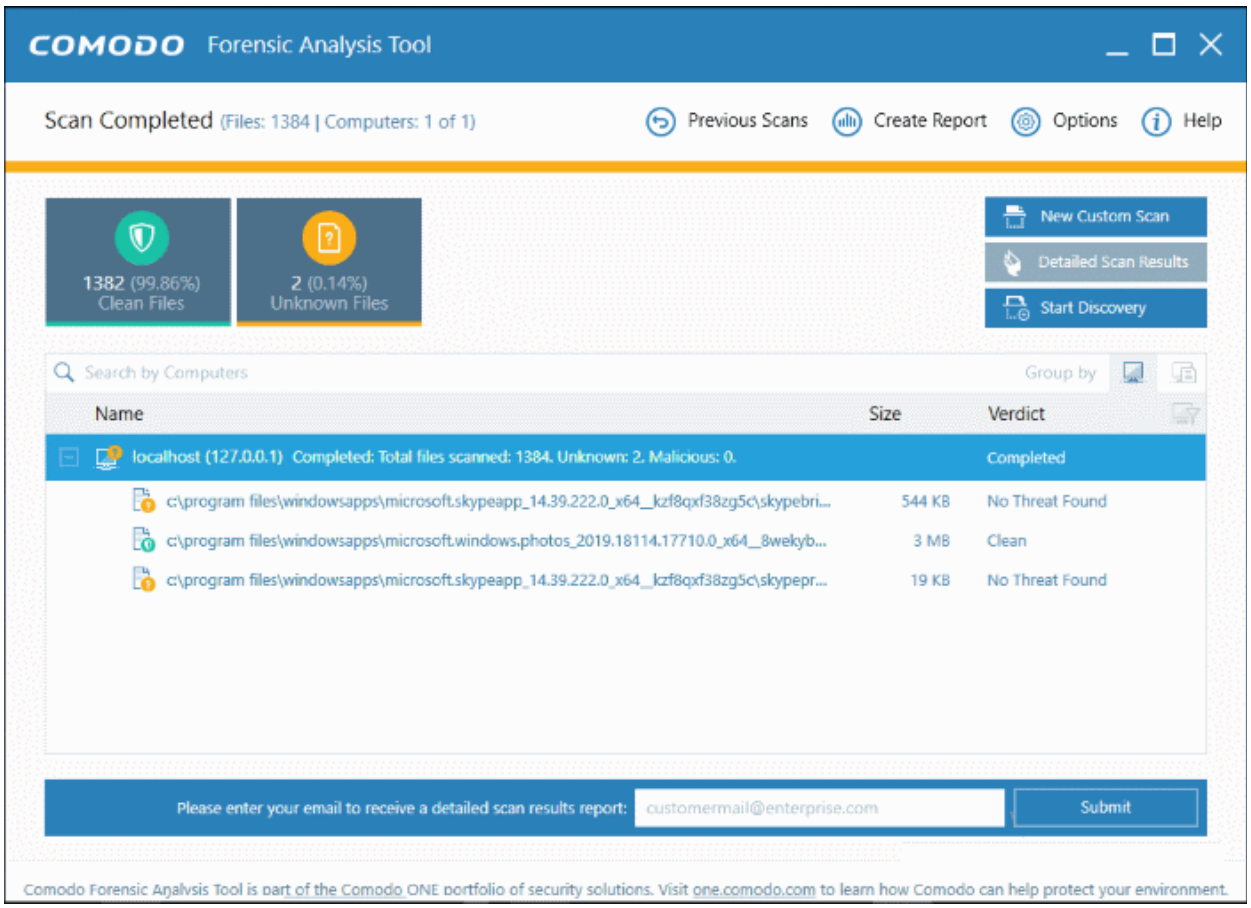


Scan progress is shown for each computer. Overall progress is shown on the title bar.

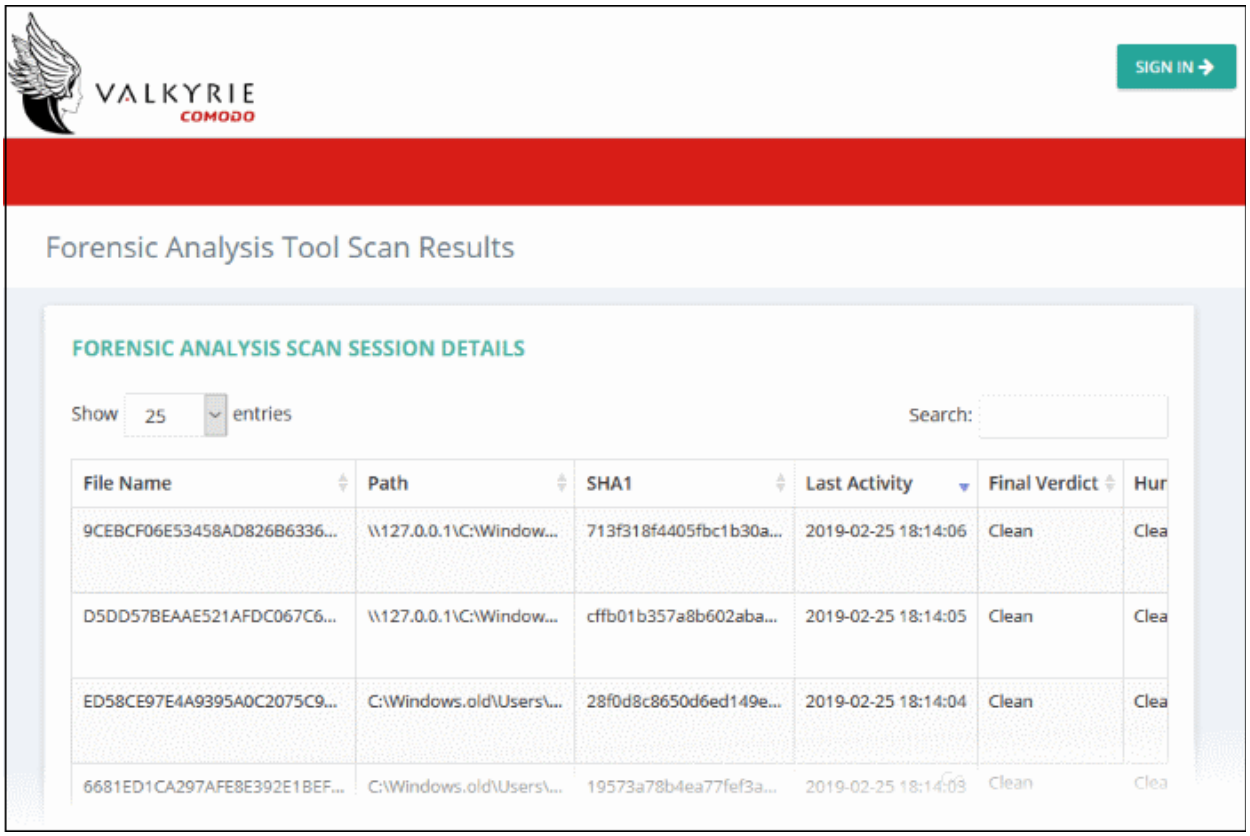
- **Stop Scan** - Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:



- The results interface contains details of each scan you have run along with verdicts for each file discovered



- There are two ways you can view the results:
  - **Group by Computer**: Shows each computer on a separate row. Expand any row to view unknown files found on that computer.
  - **Group by** File: Shows each unknown file on a separate row. Expand any row to view the endpoints on which the file was found.
- **Detailed Scan Results** – Receive a report from Comodo Valkyrie about the unknown files on your network. Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.
  - Enter your email address in the field at the bottom
  - Click 'Submit' to receive the report at the address you supplied.



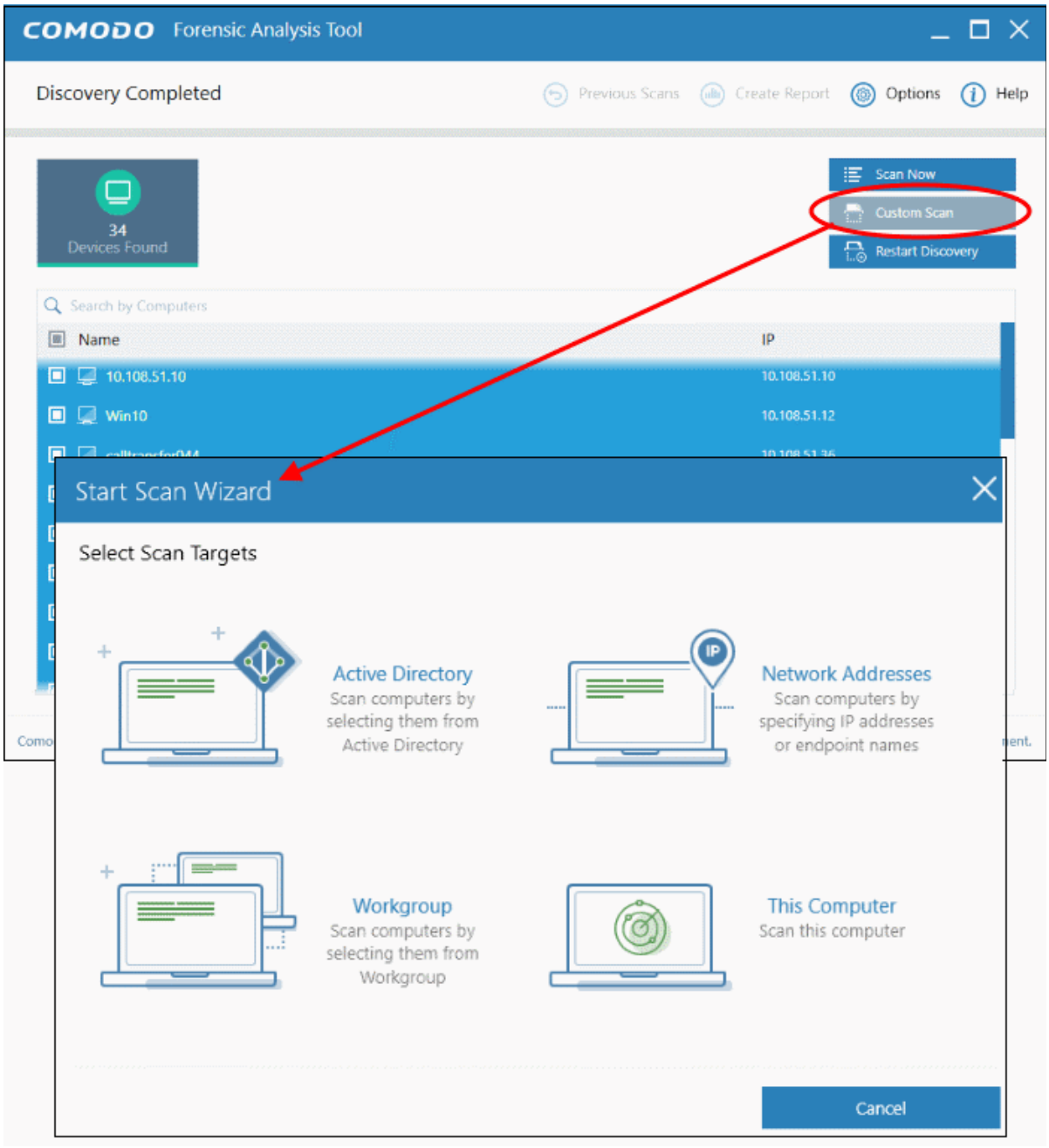
Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

Refer to the section '**Scan Results**' for more details.

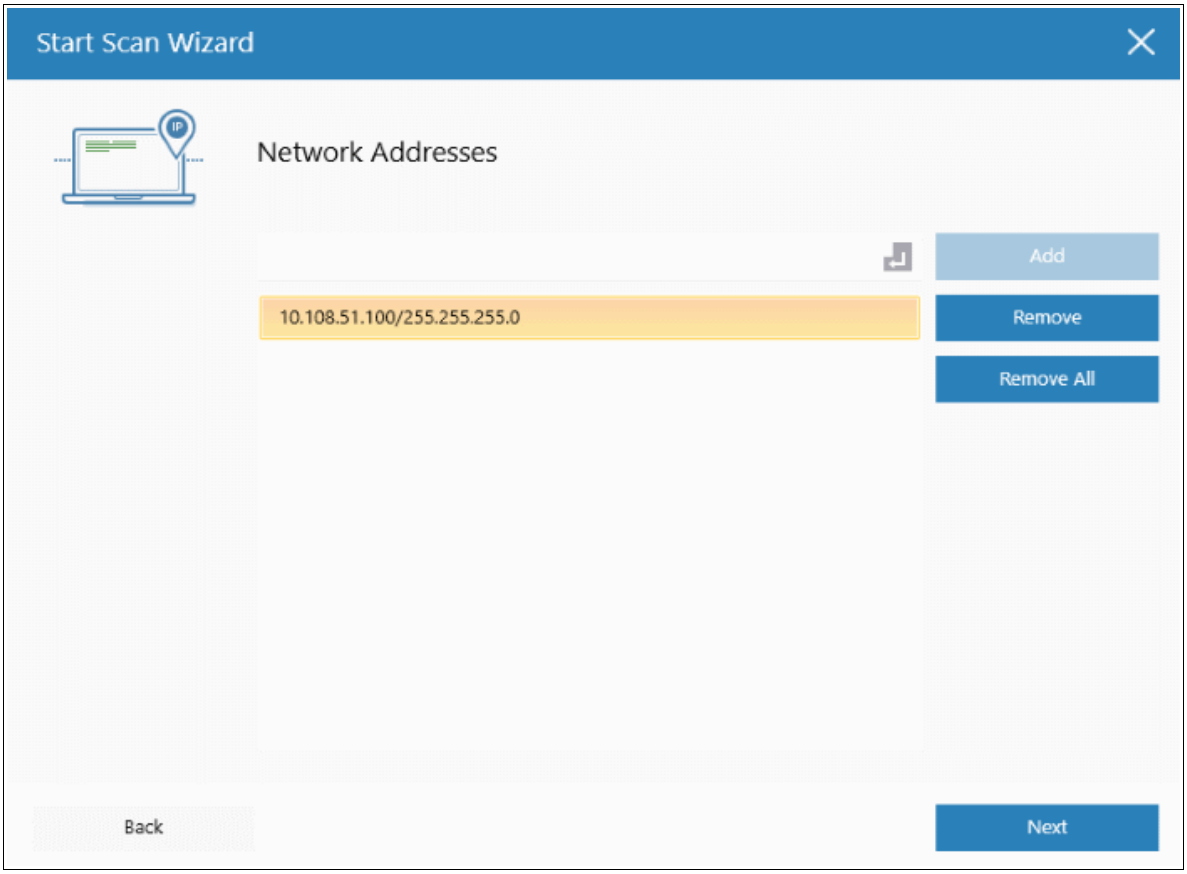
3.3 Scan Computers by Network Addresses

Scan computers by IP address/range, or host-name.

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



- Select 'Network Addresses' to configure scan targets:

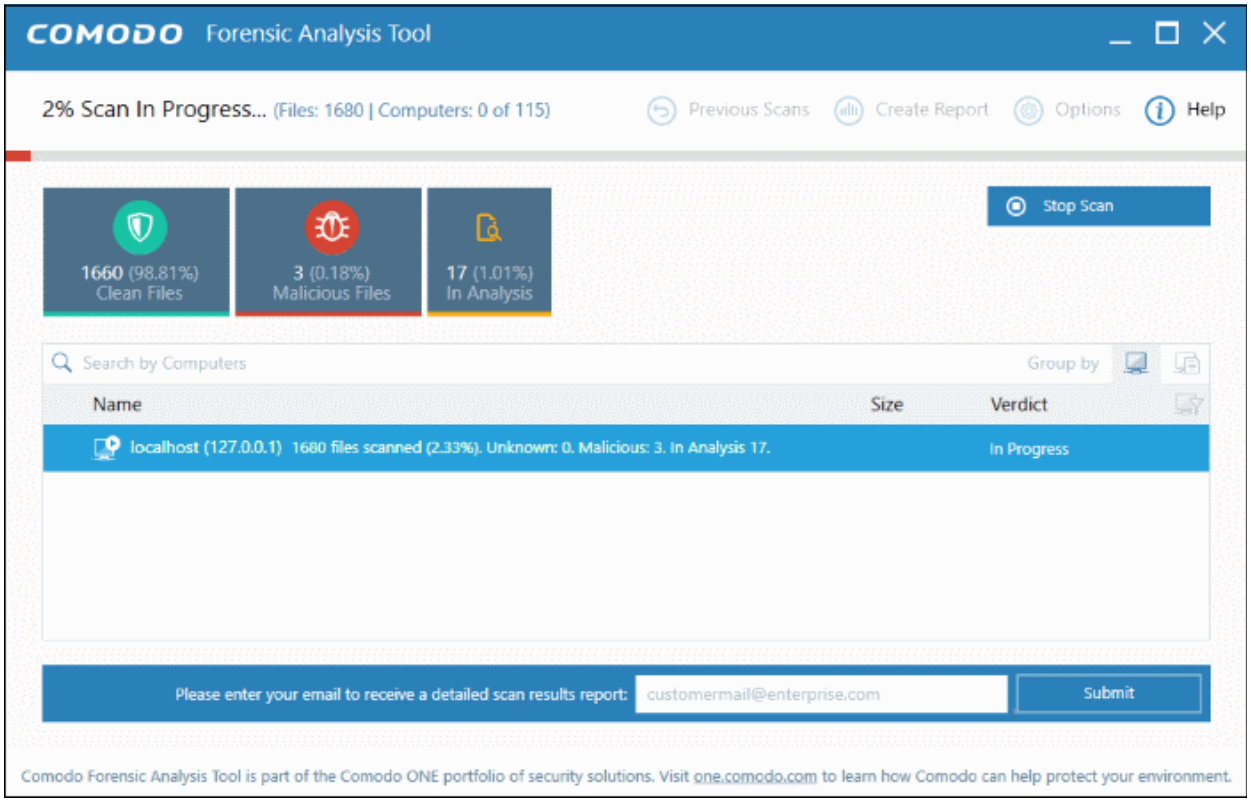


- Network Address: Enter the IP address, IP range or host name as shown below:
  - IP - 10.0.0.1
  - IP Range - 10.0.0.1-10.0.0.5
  - IP Subnet - 10.0.0.0/24 or 10.0.0.0/255.255.255.0
  - Computer Name - Home Computer
- Click the 'Add' button

Repeat the process to add more targets.

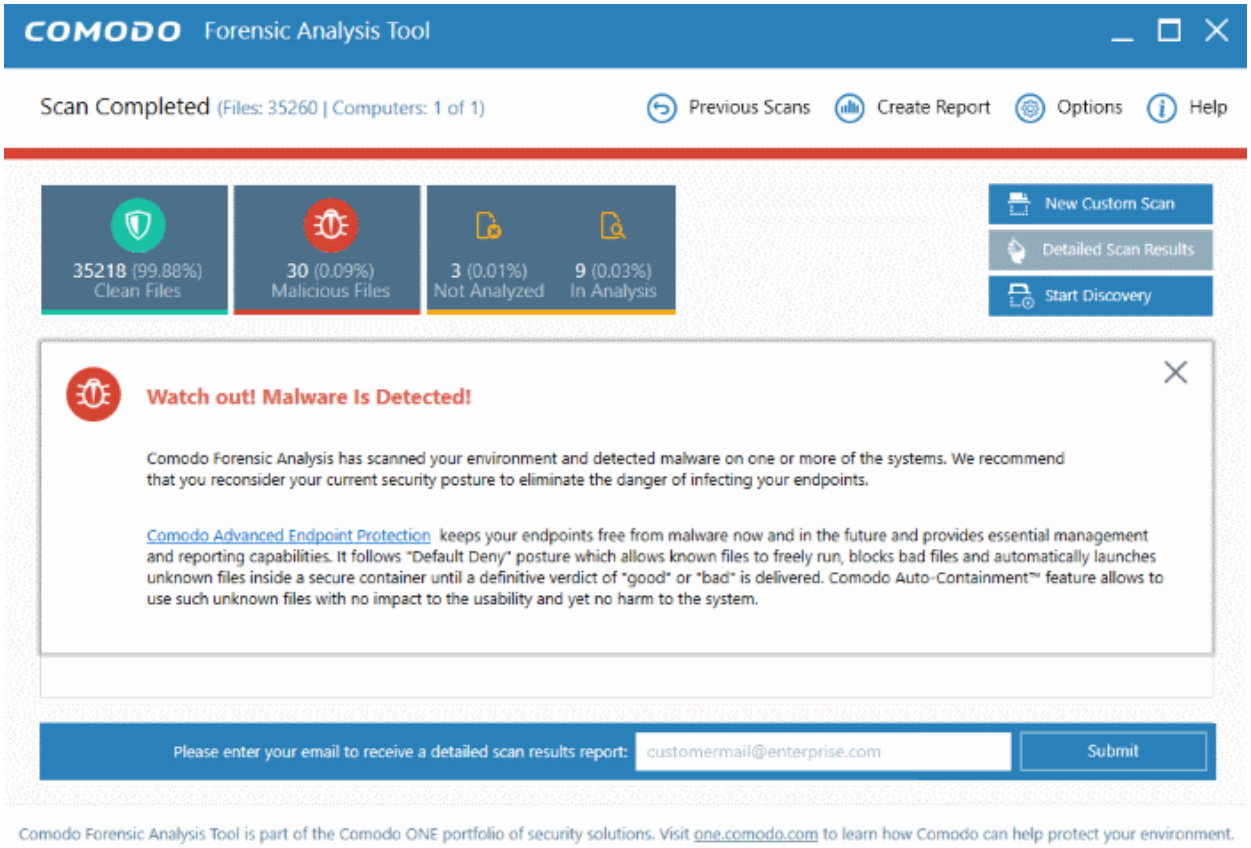
- Click 'Next' to continue.
- Login to the target device using either use the existing administrator credentials, or custom credentials.
- Next, choose one of the following scan types:
  - **Quick Scan**: Scans critical and commonly infected areas of target endpoints
  - **Full Scan**: Scans all files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

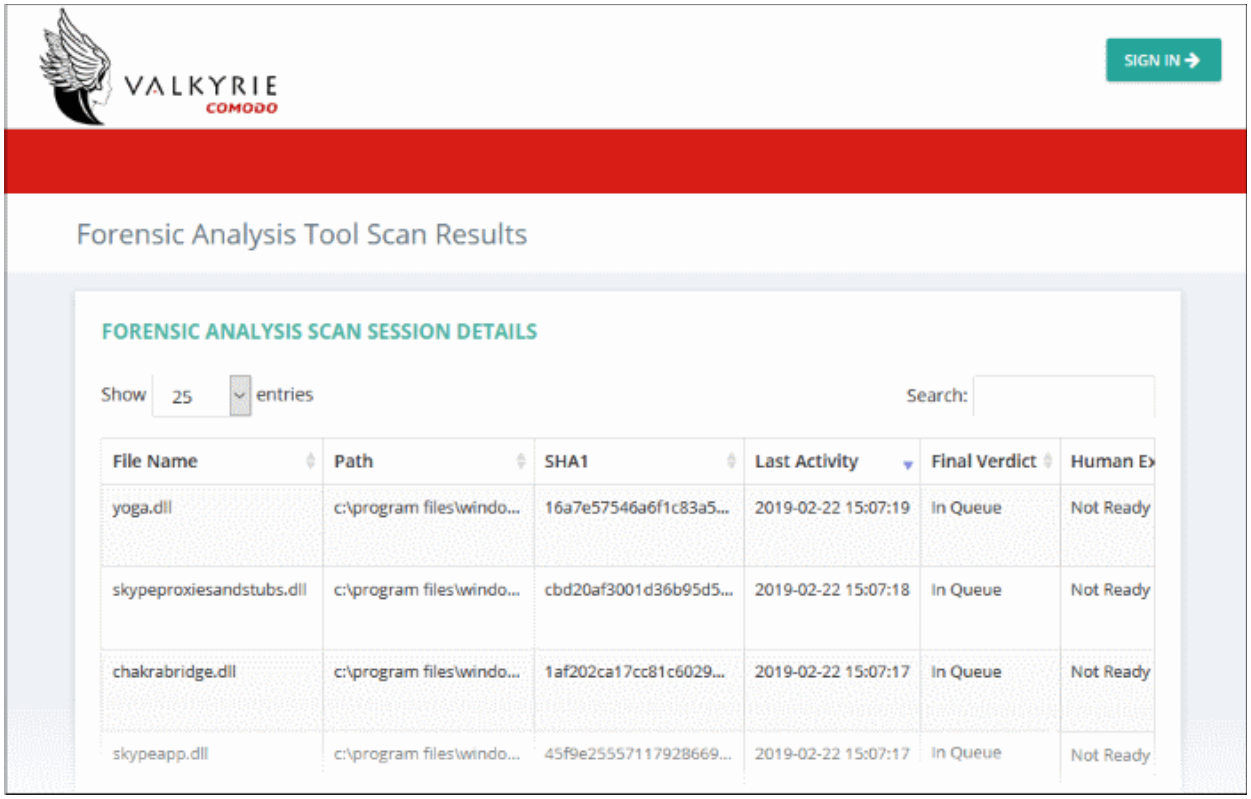


Scan progress is shown for each computer. Overall progress is shown on the title bar.

- **Stop Scan** - Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:



- There are two ways you can view the results:
  - **Group by Computer**: Shows each computer on a separate row. Expand any row to view unknown files found on that computer.
  - **Group by File**: Shows each unknown file on a separate row. Expand any row to view the endpoints on which the file was found.
- **Detailed Scan Results** – Receive a report from Comodo Valkyrie about the unknown files on your network. Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.
  - Enter your email address in the field at the bottom
  - Click 'Submit' to receive the report at the address you supplied.



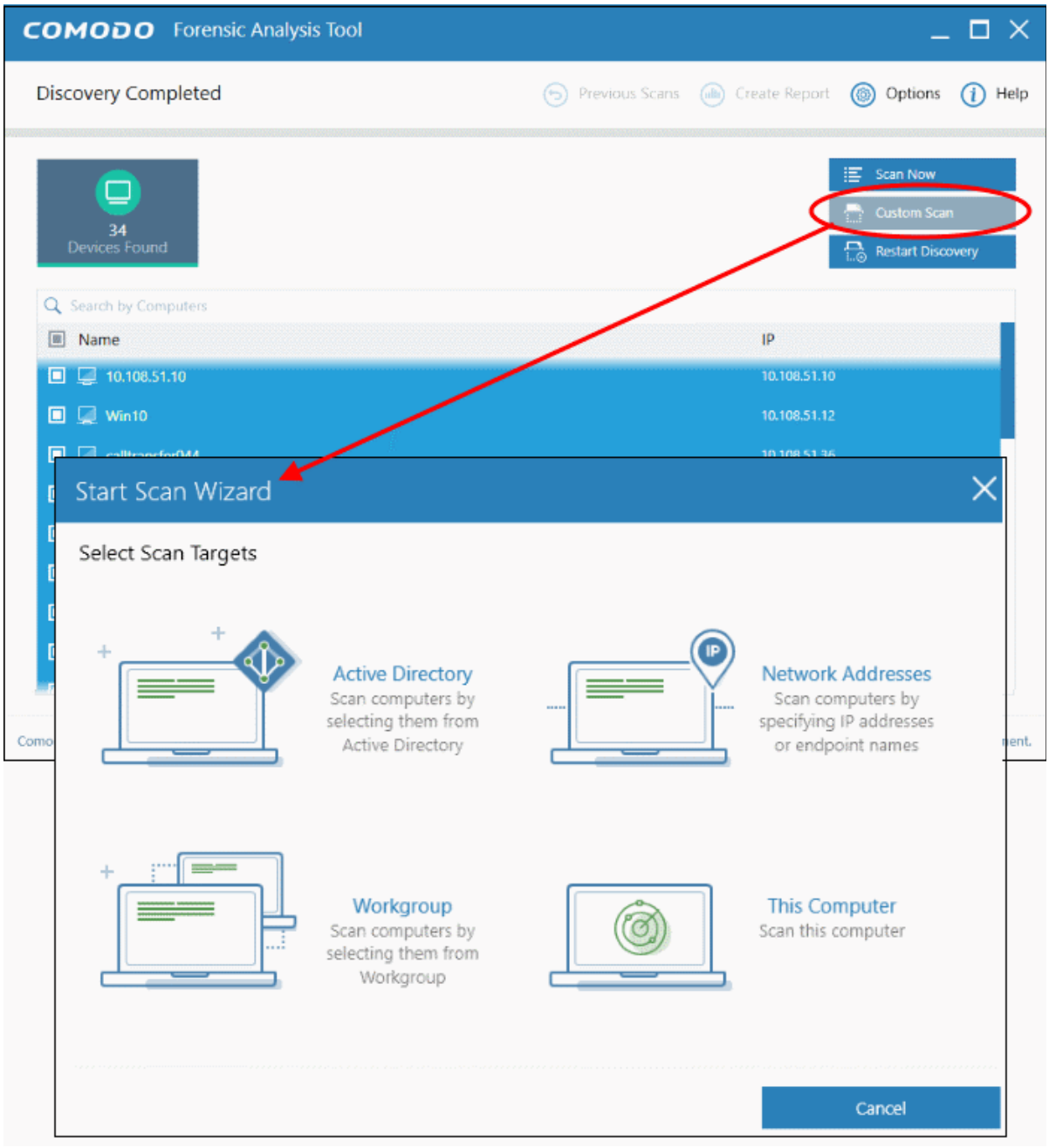
Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

Refer to the section '**Scan Results**' for more details.

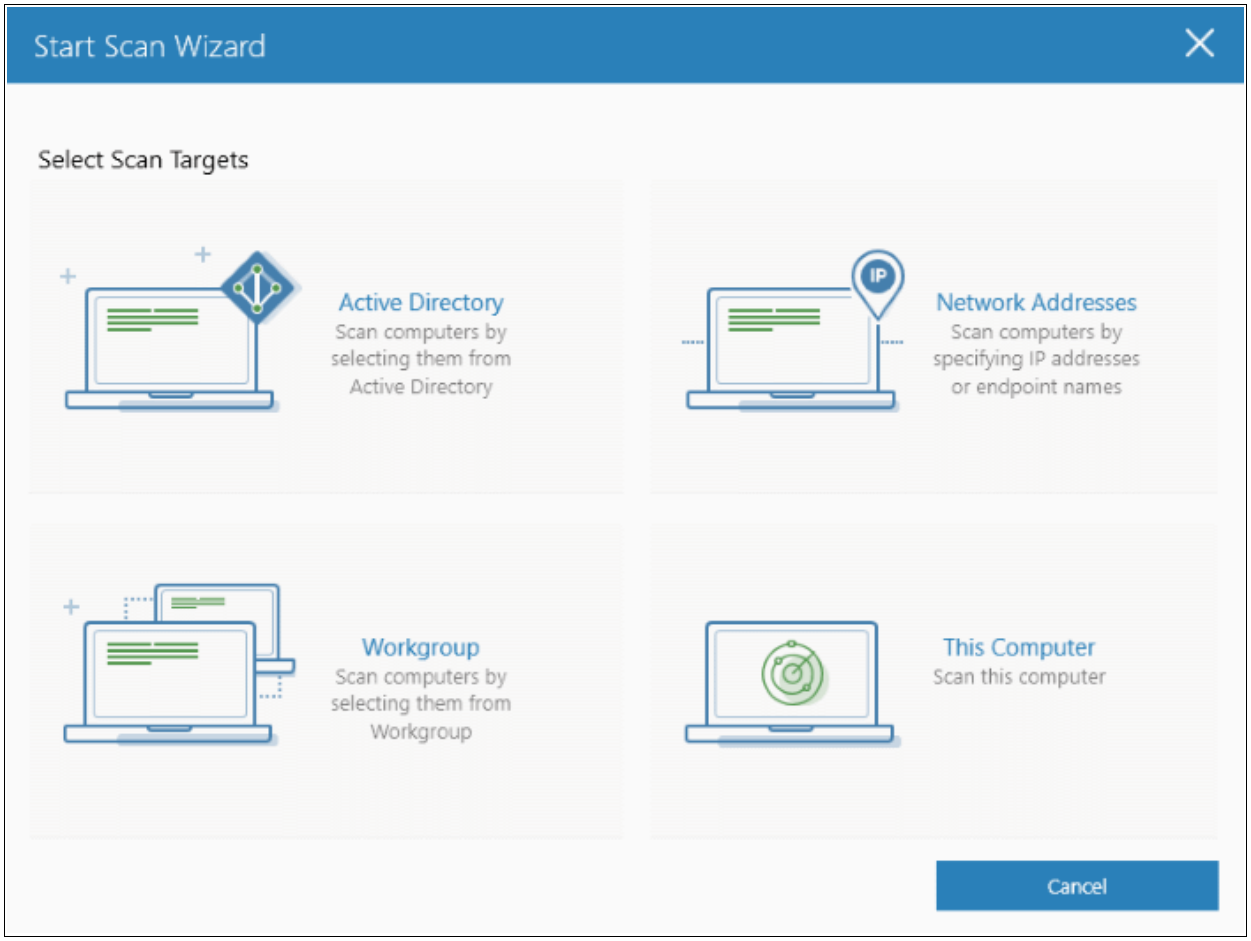
3.4 Scan your Local Computer

The local computer options lets you scan files, folders and drives on the computer you are using.

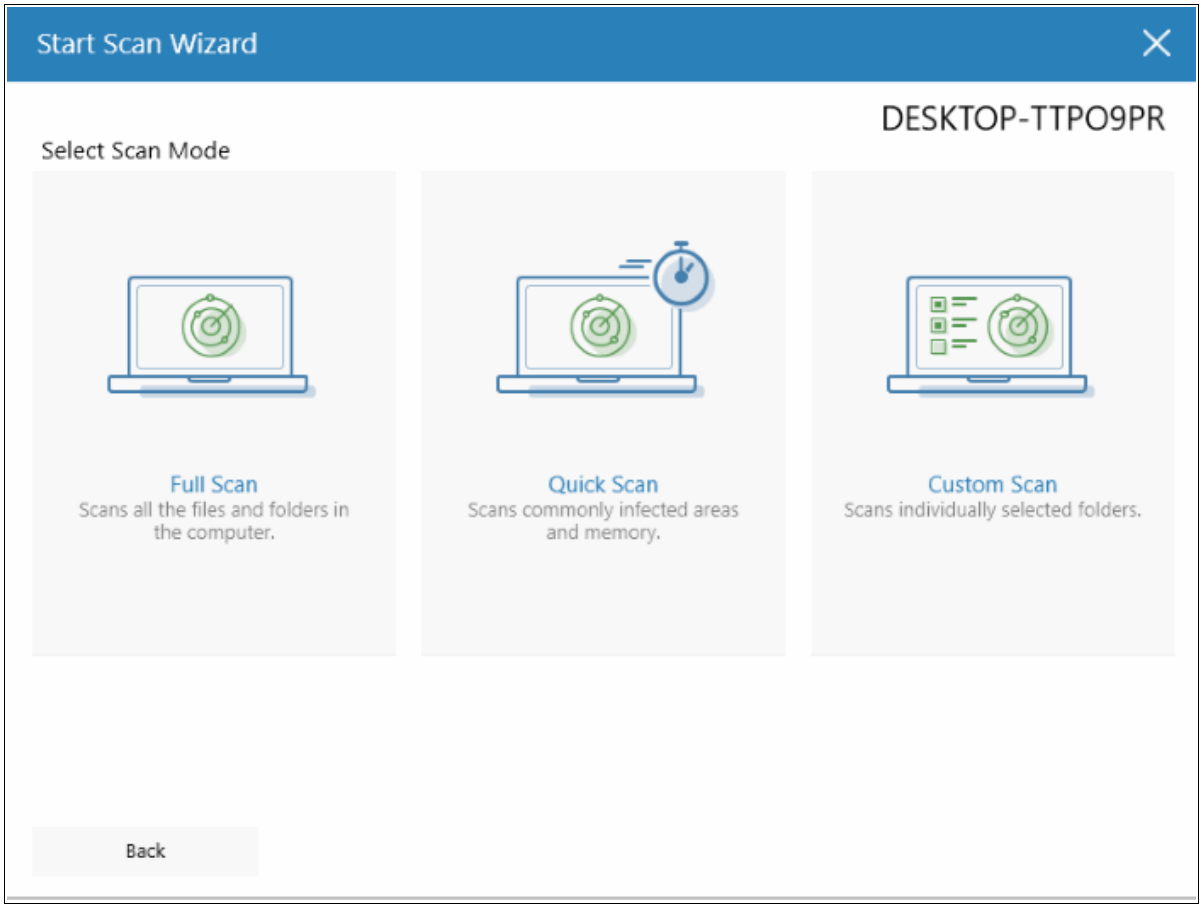
- Click 'Custom Scan' on the home screen to open the scan wizard:



- Click 'This Computer'

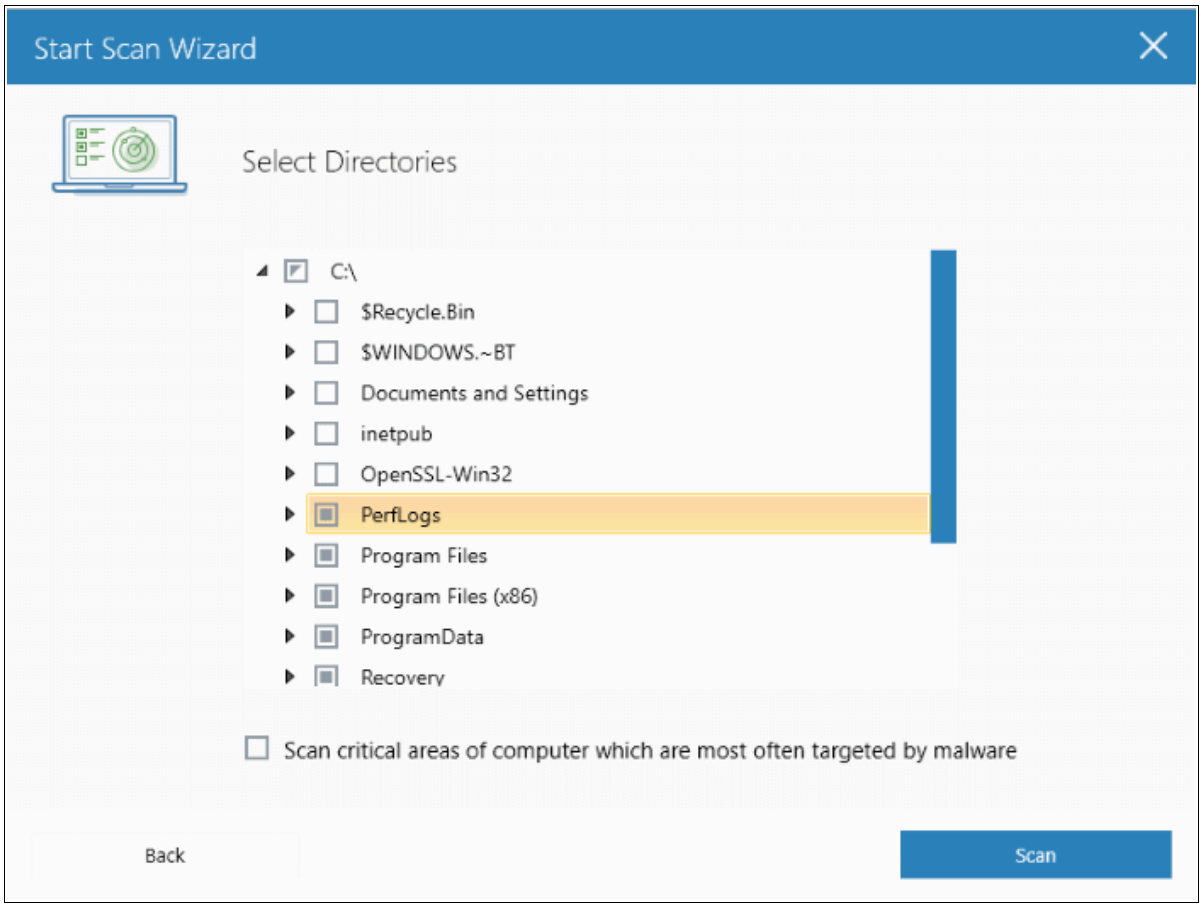


The three scan types will open.

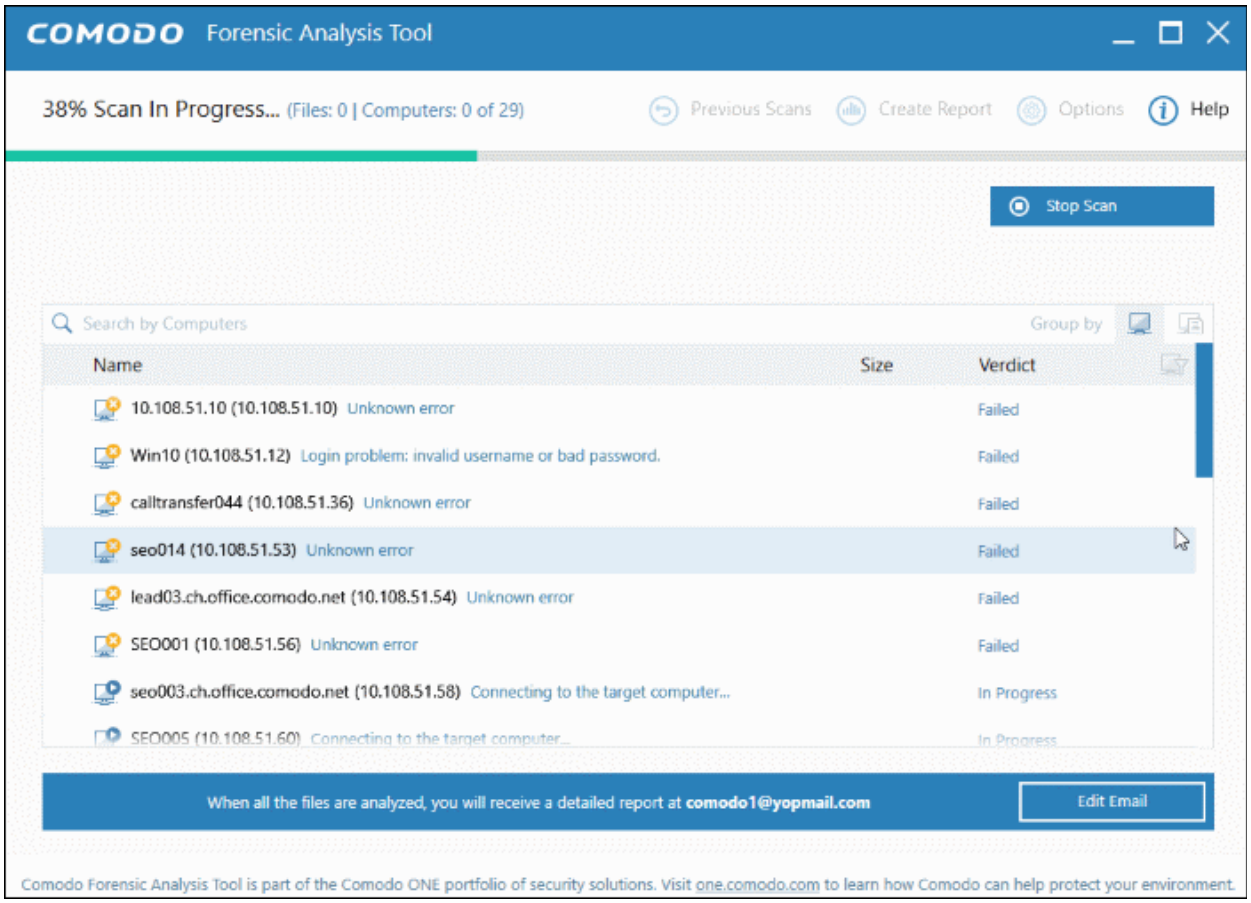


- Select the endpoints that you want to scan and choose one of the following scan types:
  - **Quick Scan**: Scan critical and commonly infected areas of your computer.
  - **Full Scan**: Scan all files and folders on your computer.
  - **Custom Scan**: Scan selected files or folders.

If you choose the 'Quick' or 'Full Scan' options then the scan will begin immediately. If you select 'Custom Scan', then you first choose the directories and files you want to scan:

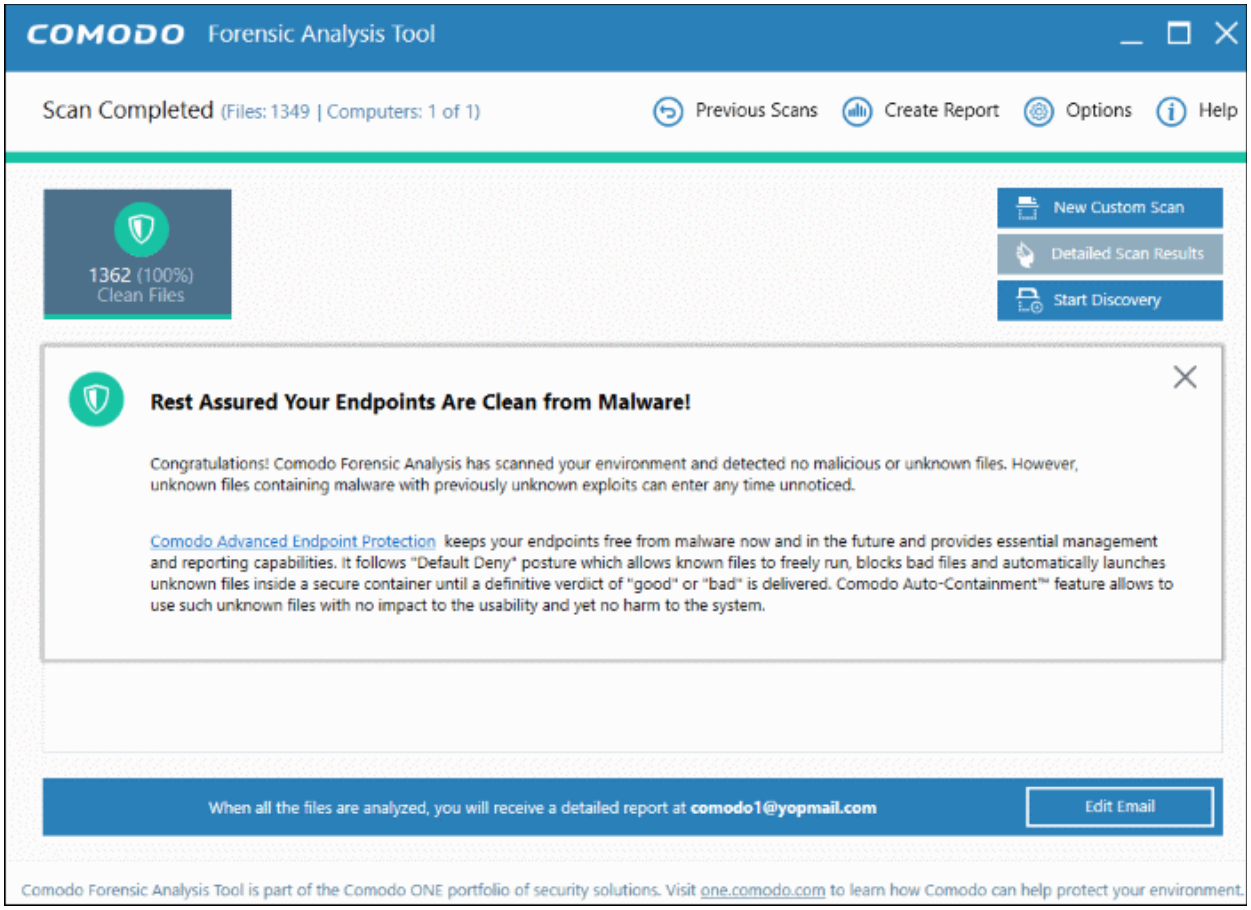


- Select 'Scan critical areas...' to scan frequently targeted areas of your computer in addition to the items in your custom scan.
- Click 'Scan' to begin the scan.

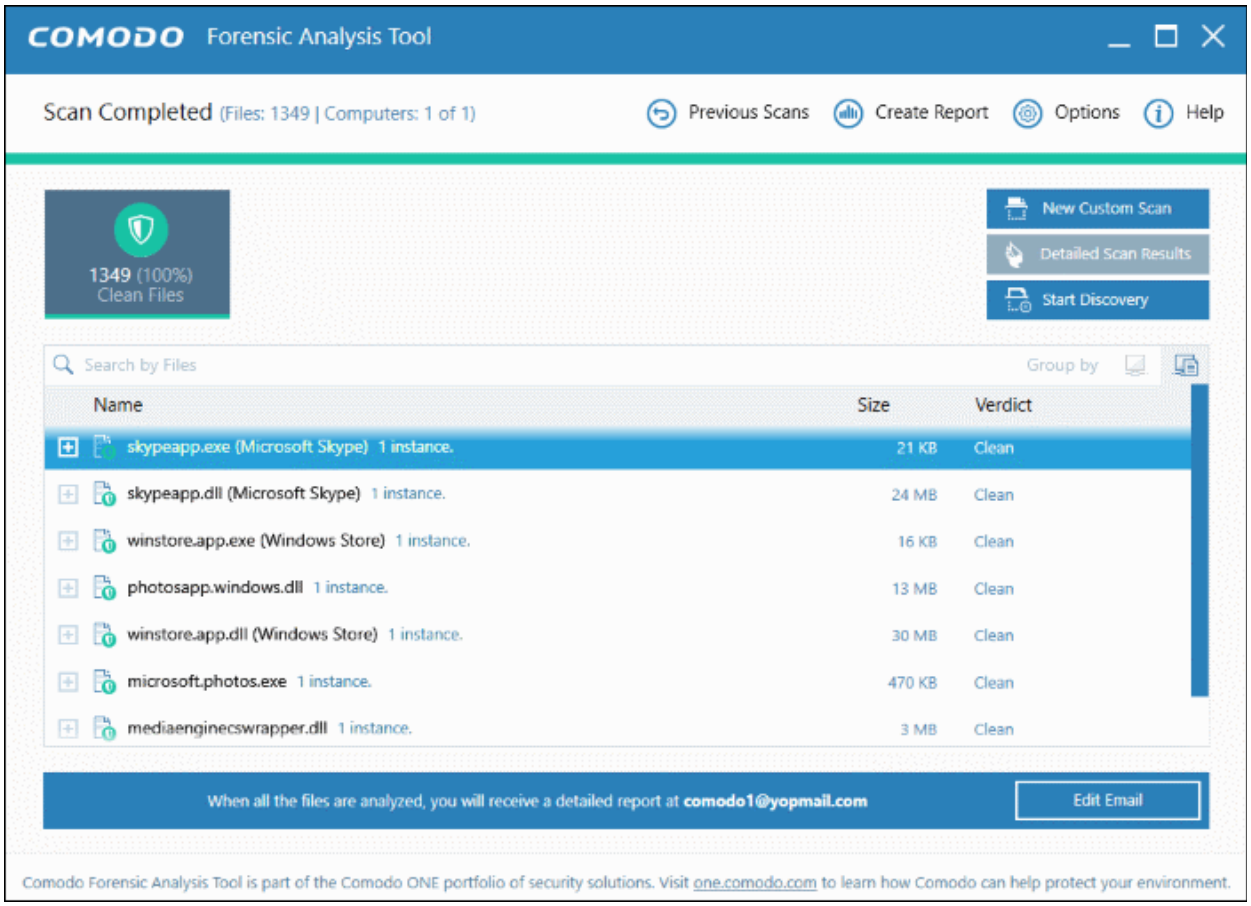


Scan progress is shown at the top of the interface.

- **Stop Scan** - Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:



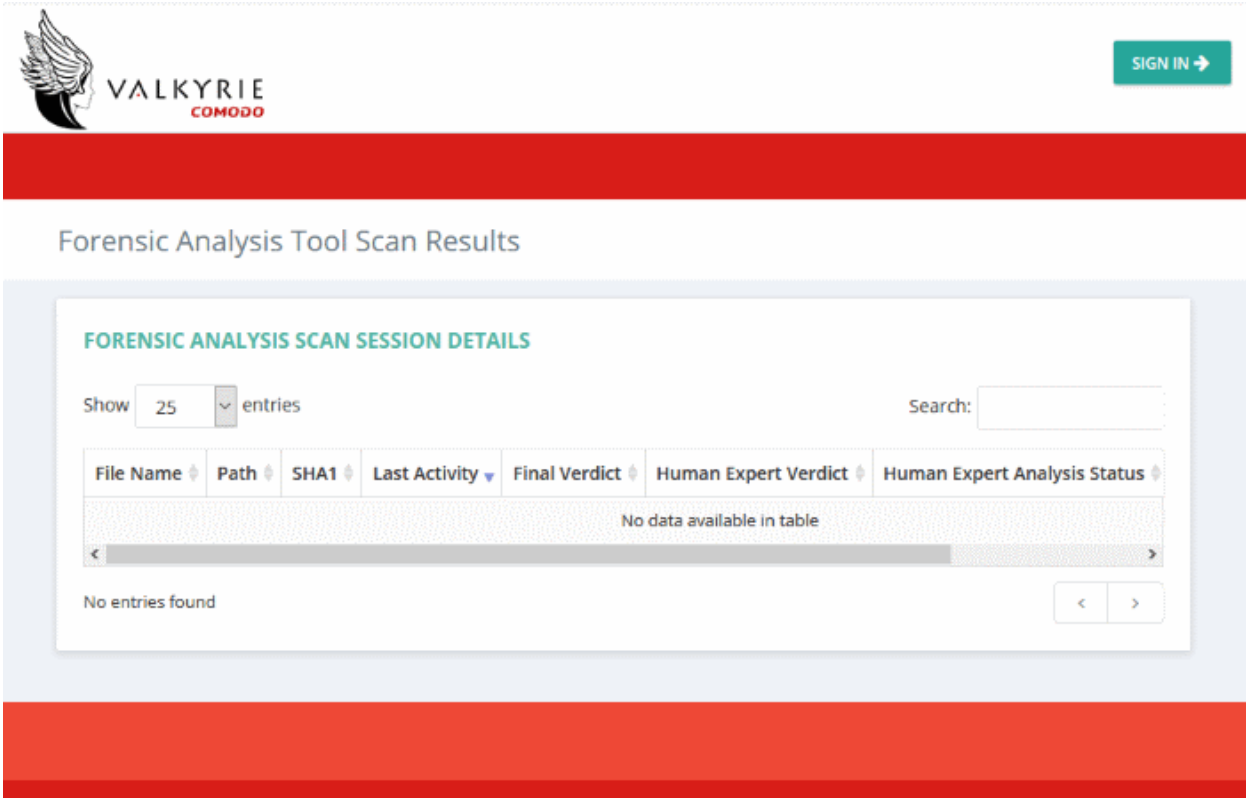
- The results interface contains details of each scan you have run along with verdicts for each file discovered



Detailed Scan Results – Receive a report from Comodo Valkyrie about the unknown files on your network. Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.

Enter your email address in the field at the bottom

Click 'Submit' to receive the report at the address you supplied.

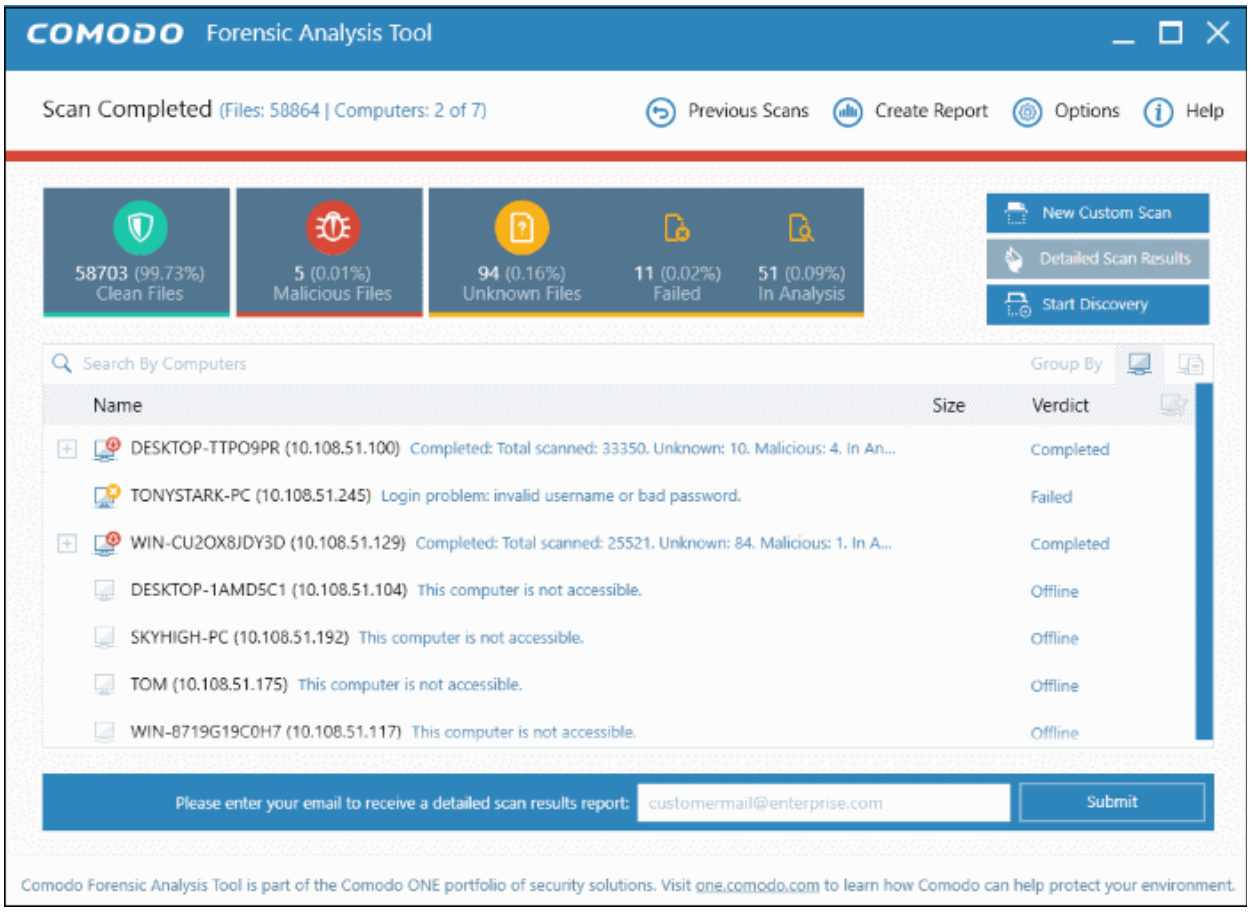


When your computer is free of unknown files, you will not find any data when you click the 'Detailed Scan Results' button.

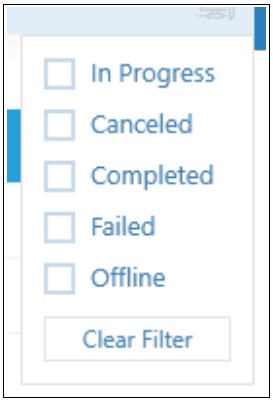
Valkyrie results are shown in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

4 Scan Results

- Scan results are automatically shown in the CFA interface after a scan finishes.
- The scan checks the reputation of each file against Comodo's file-lookup service, a huge database of blacklisted and white-listed files.
- Blacklisted files are 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 behavioral tests to discover whether they are malicious or not.
- The CFA interface displays results of both files analyzed by Forensic Analysis and Valkyrie analysis:



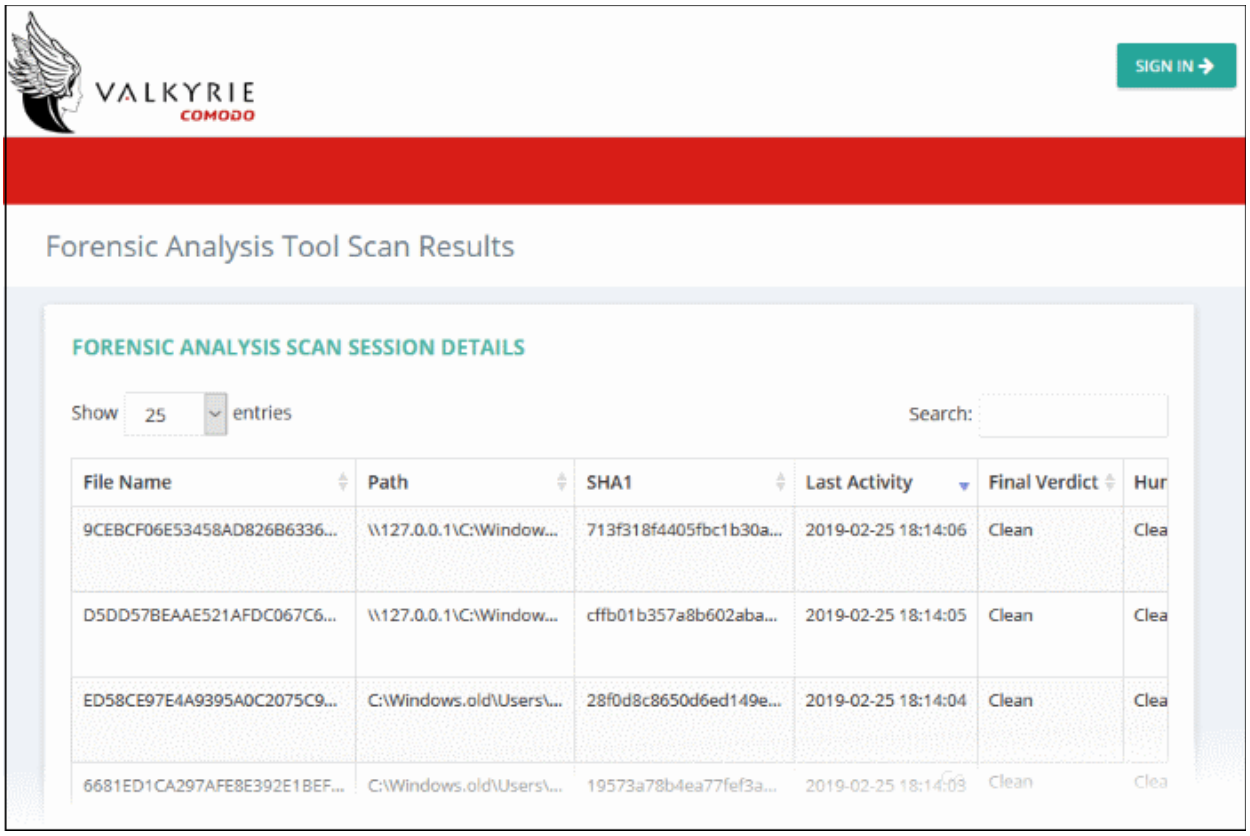
- Scan results are listed for each computer. Each row has a quick summary of the scan results, including total files scanned and how many were malicious or unknown.
- Click the plus symbol beside an endpoint to view unknown and malicious files detected by the scan.
- Click the icons next to 'Group By' 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:



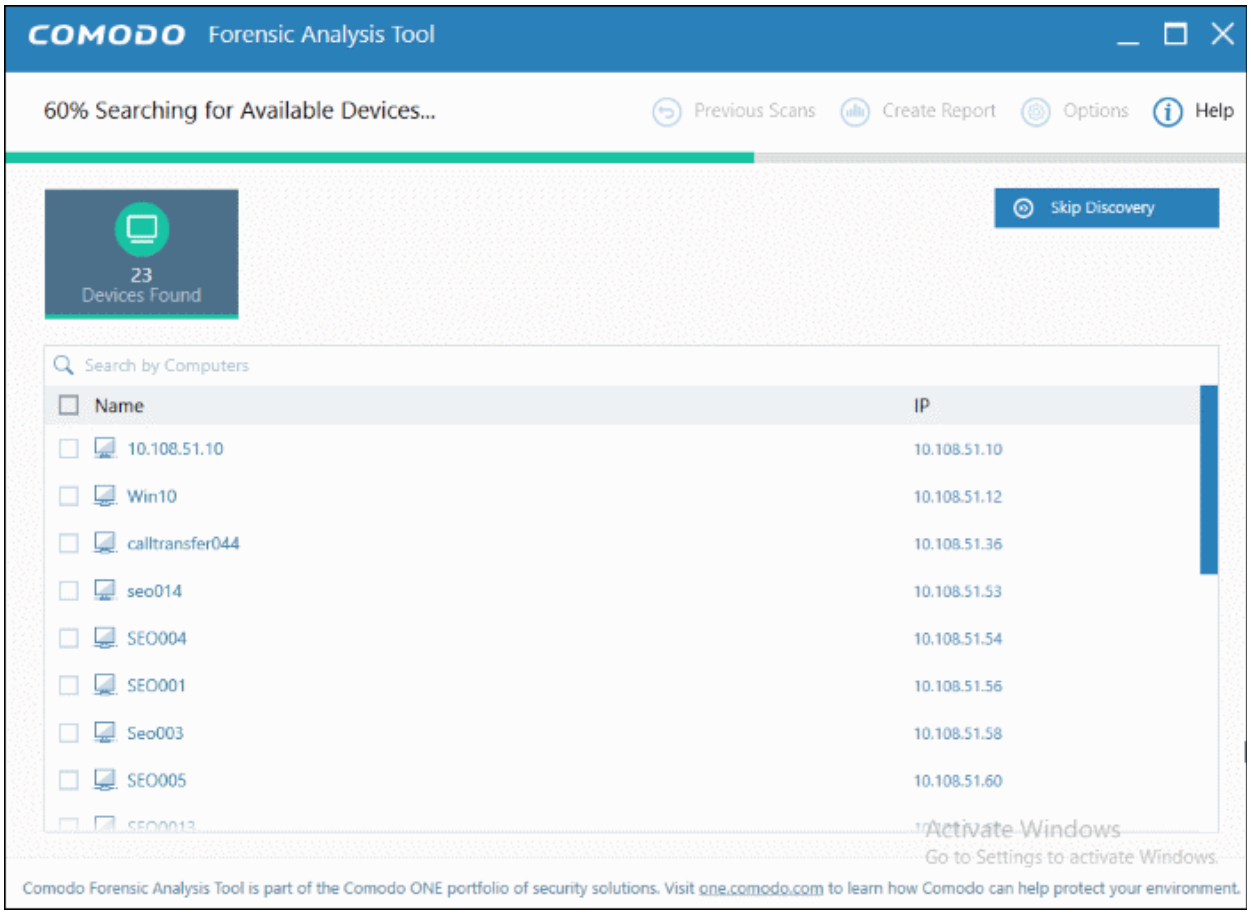
Valkyrie Detailed Analysis Results - Table of Column Descriptions	
Column Header	**Description**
File Name	The name of the submitted file
Path	The IP of the endpoint and the file's path details
SHA1	The SHA1 hash value of the file.
Last Activity	The date and time the last activity of analysis was performed.
Final Verdict	The Valkyrie dynamic and **static analysis** results for the file. The results available are: • Clean - The file is safe to run • No Threat Found - No malware found in the file, but cannot say it is safe to run • Malware - The file is a malware and should not be run
Human Expert Verdict	The results of the file after Human expert analysis: • Clean - File is safe to run

	• Malware - The file is a malware file • Potentially Unwanted Application (PUA) - Applications such as Adware, Spyware and so on • No Threat Found - No malware found in the file, but cannot say it is safe to run • Not Ready - Indicates manual analysis of the file is in progress
Human Expert Analysis Status	Indicates the status of files submitted for Human Expert analysis. The statuses are: • In Queue - The analysis has not started • In Progress - The analysis has started and in progress • Analysis Completed - The analysis is completed and verdict displayed under the 'Manual Verdict' column • 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. • Objection Completed - Indicates the manual re-analysis is completed.
Request Type	Indicates the type of input given to receive Valkyrie results. • Queried - The file were automatically uploaded to Valkyrie • Manual - The files were manually uploaded to Valkyrie
Actions	The available actions are:  - View Info - You can view the complete details of the results for the file such as summary, static analysis, dynamic analysis and file details.  - Download Automatic Analysis Report - Allows you to download the report in PDF format.  - View Virus Total Result - Takes you to the Virus Total website that displays its results for the file.  - Send to Manual Analysis - Allows you to submit the file for manual analysis by Comodo technicians.

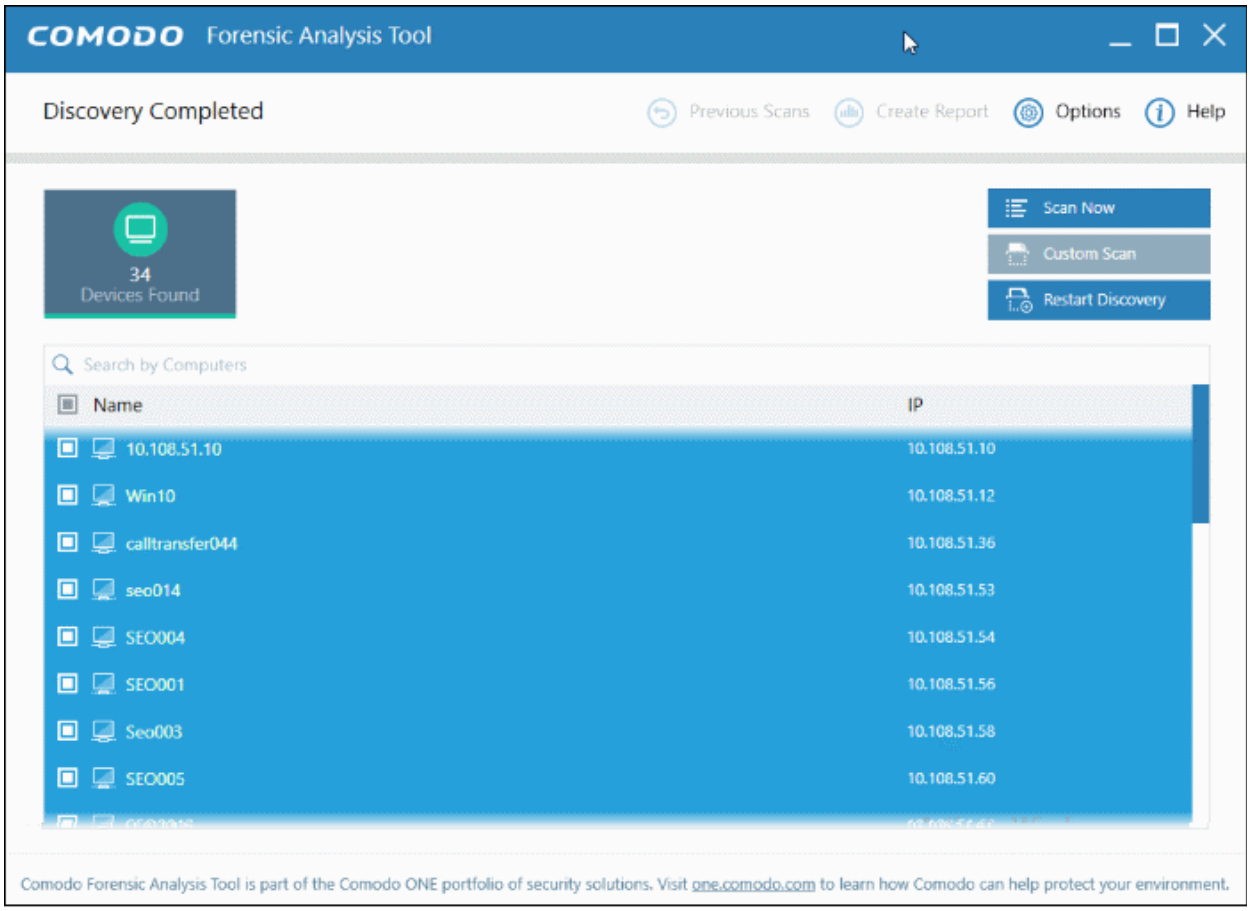
You can also view detailed Valkyrie results in the reports area. See **Reports** for more details.

5 Discover Computers

- The software starts to discover all computers on your local network when you first launch the tool.
- You can skip discovery if you do not want to scan local machines.



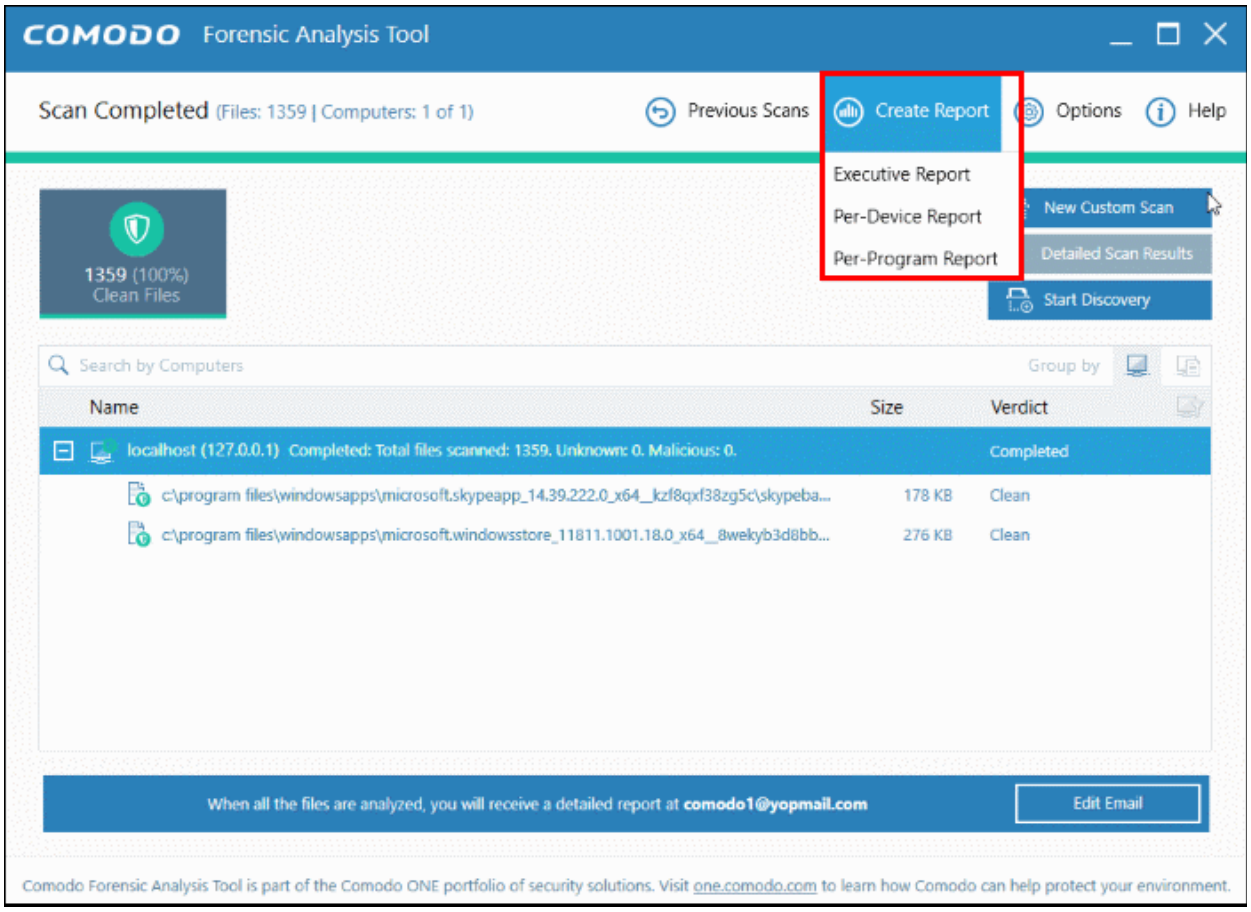
All discovered computers are shown in the results screen. You can now scan these machines for unknown files:



6 Reports

There are three types of report you can order:

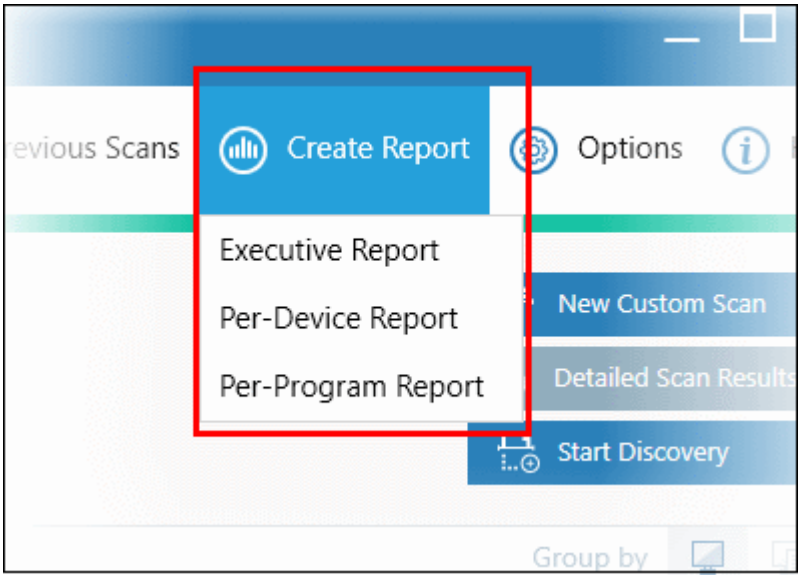
- Executive report - An overall report which shows the scope of the scan, the number of devices scanned, the number of unknown programs found and more.
- Per device report – Groups the results by computer. Details how many trusted programs, unknown programs and malicious programs were found on specific machines.
- Per program report – Shows the impact of a file on your network. Shows the names and IP addresses of the devices on which the file was found.



Refer to the following sections for more details:

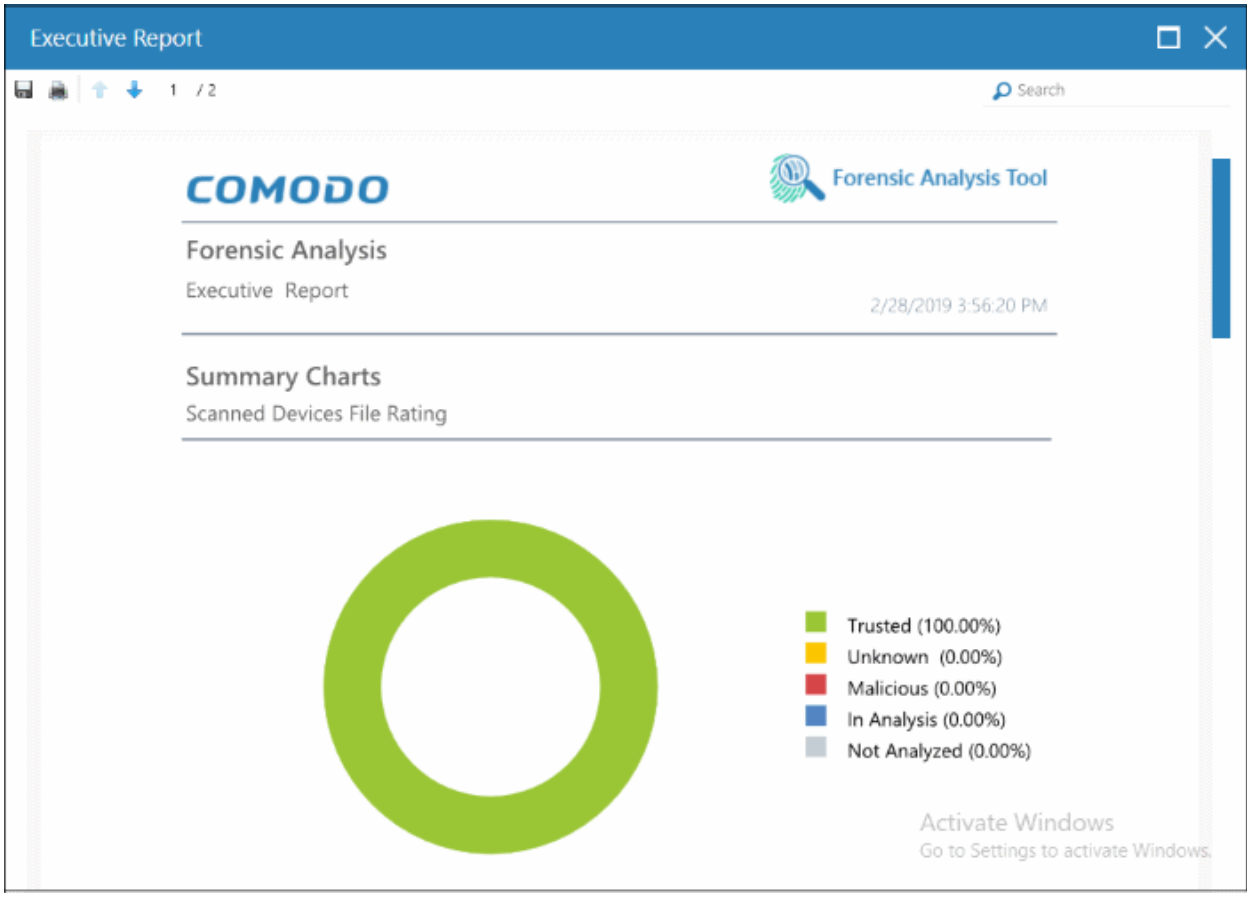
- **Executive Report**
- **Device Report**
- **Program Report**

6.1 Executive Report



- Click 'Reports' and then 'Executive Report':

The report will be generated and displayed:



Scroll down to view the full report. You can 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 name 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.
  - **Scanned Devices File Rating** - 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.
  - **Device Assessment** - Pie chart which shows the percentage of devices that are safe, infected, at risk and not yet scanned.

6.2 Device 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.

- Click 'Reports' then 'Per Device Report'.

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.

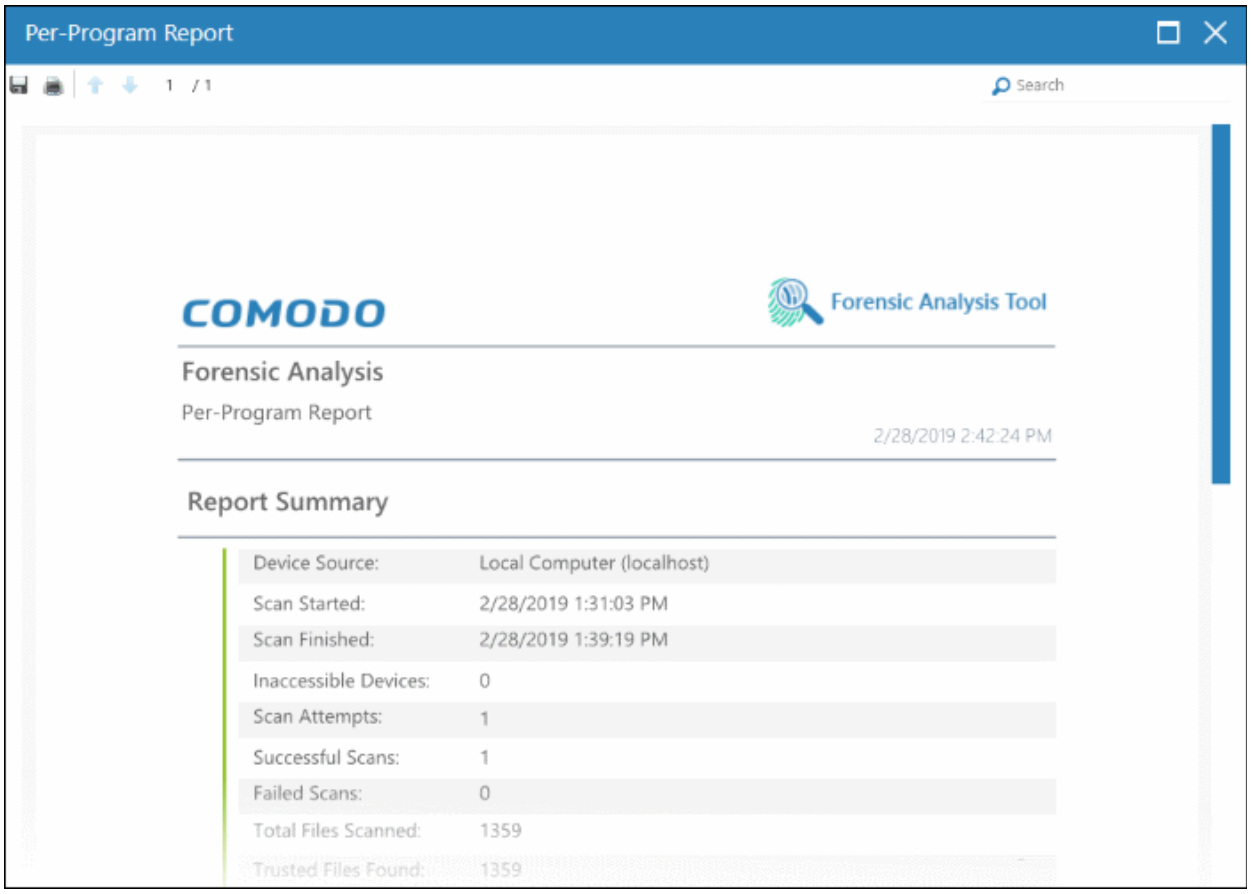
- **Report Summary** - General scan details, including the number of devices scanned, date and time of the scan, number of malware found and so on.
- **Summary Chart** - Bar chart showing the top 10 endpoints that contain unknown/malware files.
- **Details per Device** - Inventory of files discovered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

6.3 Program 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.

- Click 'Reports' then click 'Per Program Report'.

The report will be generated and displayed:



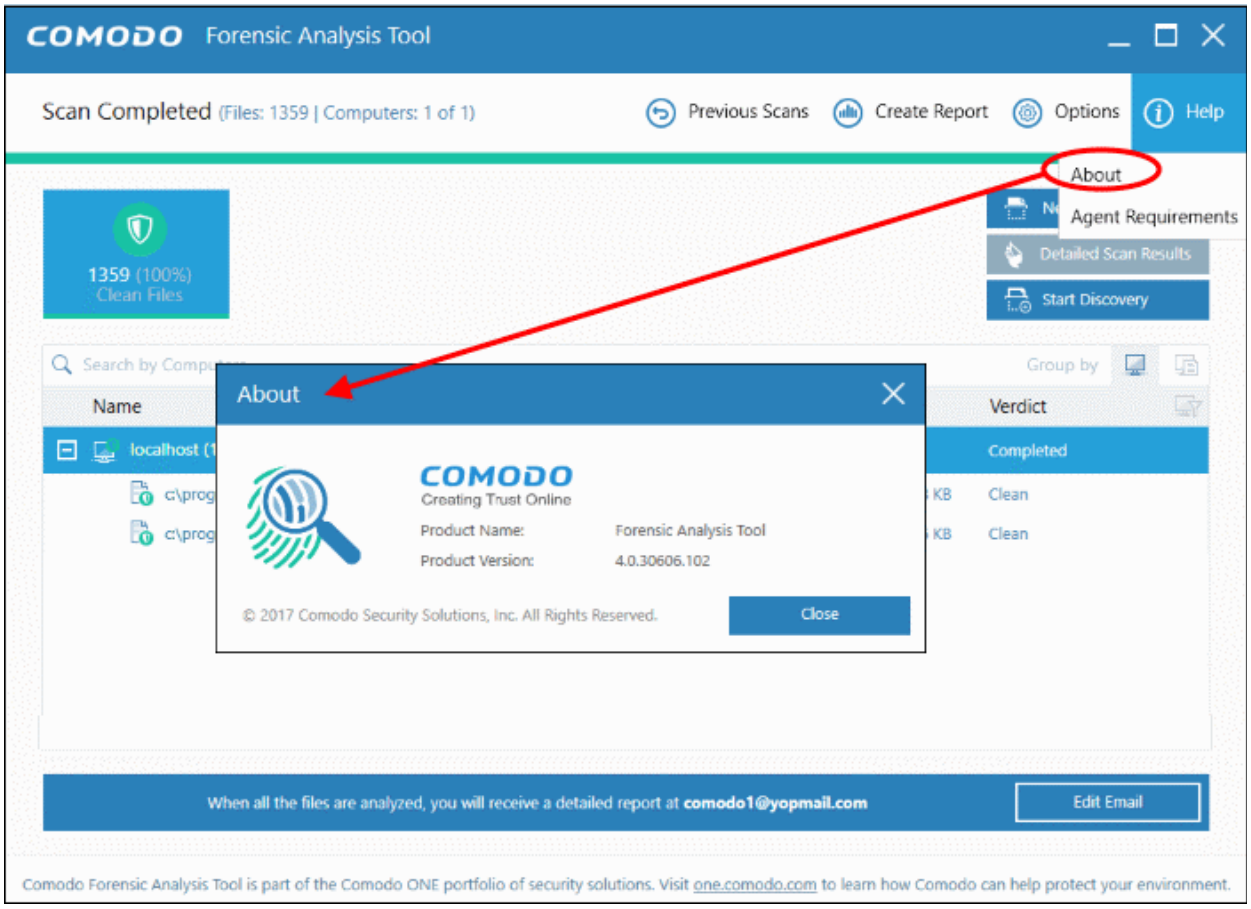
Scroll down to view the full report. Note - please save the report if you wish to keep it for further reference. The report will not be available in the interface after the application is closed. To save the report, click the folder icon at the top-left, copy the report file and save in another location.

- **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 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.

7 About Comodo Forensic Analysis

The 'About' dialog show product information and version number.

- Click 'Help' > 'About':



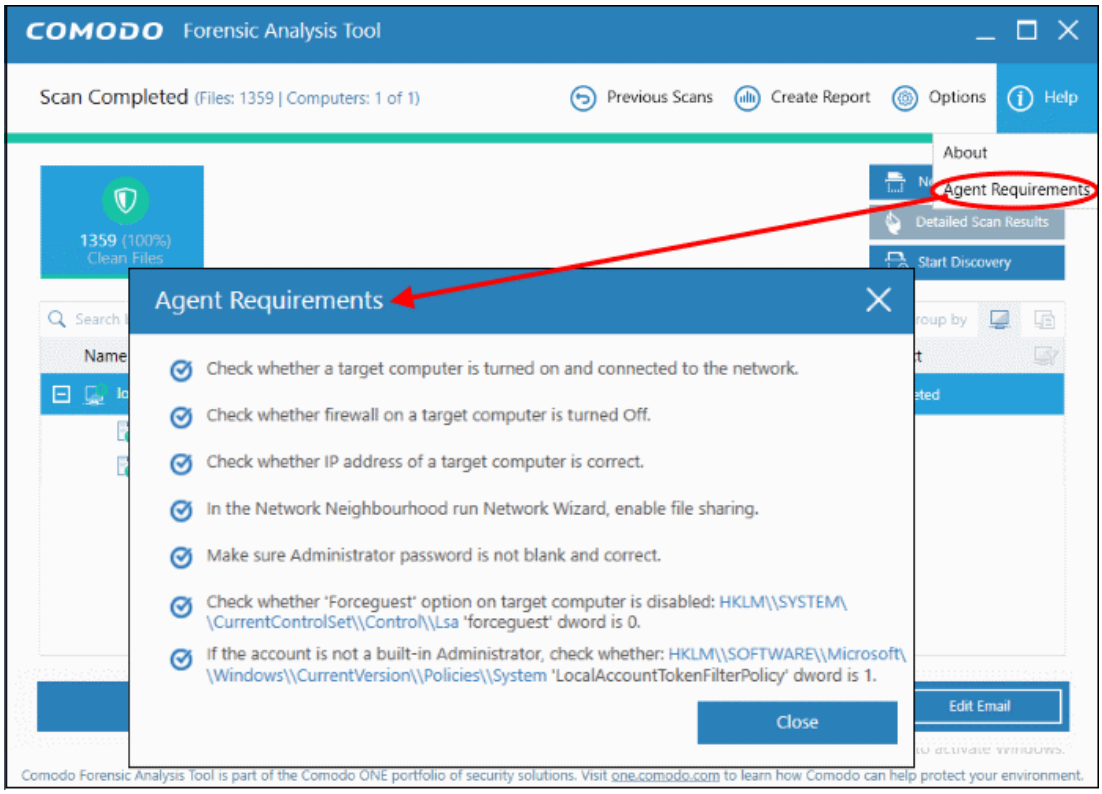
- Product Name - The full name of the product
- Product Version - The version number of the product

- Click the 'Close' button to return to the application.

8 Agent Requirements

The 'Agent requirements' window contains advice to help you run scans successfully.

- Click 'Help' > 'Agent Requirements':



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 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**