



Comodo Unknown File Hunter

Software Version 2.1

Administrator Guide

Guide Version 2.1.011317

Table of Contents

1 Introduction to Comodo Unknown File Hunter.....	3
2 Running Unknown File Hunter.....	4
2.1 The Main Interface.....	5
3 Scanning Computers.....	7
3.1 Scanning Computers using Active Directory.....	8
3.2 Scanning Computers using Workgroup.....	15
3.3 Scanning Computers by Network Addresses.....	21
3.4 Scanning Local Computer.....	25
3.5 Analyzing Files with Valkyrie	32
4 Scan Results.....	35
4.1 Comodo Unknown File Hunter Scan Results.....	36
4.2 Valkyrie Analysis Results.....	40
5 Reports.....	54
5.1 Executive Report.....	54
5.2 Device Report.....	56
5.3 Program Report.....	56
6 About Comodo Unknown File Hunter.....	57
7 Agent Requirements.....	58
About Comodo.....	60

1 Introduction to Comodo Unknown File Hunter

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 Unknown File Hunter (UFH) 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 UFH scanner allows you to upload 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 the results of these tests in the UFH interface.

Name	Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	
c:\program files\freedownloadmanager.org\free download manager\qt5qml.dll	2 MB
C:\Program Files (x86)\OpenOffice 4\program\unopkg.exe	11 KB
c:\program files\freedownloadmanager.org\free download manager\common.dll	416 KB
c:\program files\freedownloadmanager.org\free download manager\imageformats\qjpeg.dll	234 KB
c:\program files\freedownloadmanager.org\free download manager\libcef.dll	62 MB
c:\program files\freedownloadmanager.org\free download manager\swscale-4.dll	647 KB
c:\program files\freedownloadmanager.org\free download manager\avfilter-6.dll	2 MB
c:\program files\freedownloadmanager.org\free download manager\winwfpmontorex.exe	829 KB
c:\program files\freedownloadmanager.org\free download manager\sql\drivers\sqlite.dll	866 KB

Please [click here](#) to see the detailed results

1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)

Features

- No installation required, just run the portable application on any computer in the network
- Capable of scanning computers from Active Directory, Work Group and by Network Addressees
- Unknown files can be 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 UFH and is broken down into the following main sections.

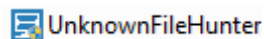
- **Introduction**

- **Running Unknown File Hunter**
- **Scanning Computers**
 - **Scanning Computers using Active Directory**
 - **Scanning Computers using Workgroup**
 - **Scanning Computers by Network Addressees**
 - **Scanning Local Computer**
 - **Analyzing Files with Valkyrie**
- **Scan Results**
 - **Unknown File Hunter Tool Scan Results**
 - **Valkyrie Analysis Results**
- **Reports**
 - **Executive Report**
 - **Device Report**
 - **Program Report**

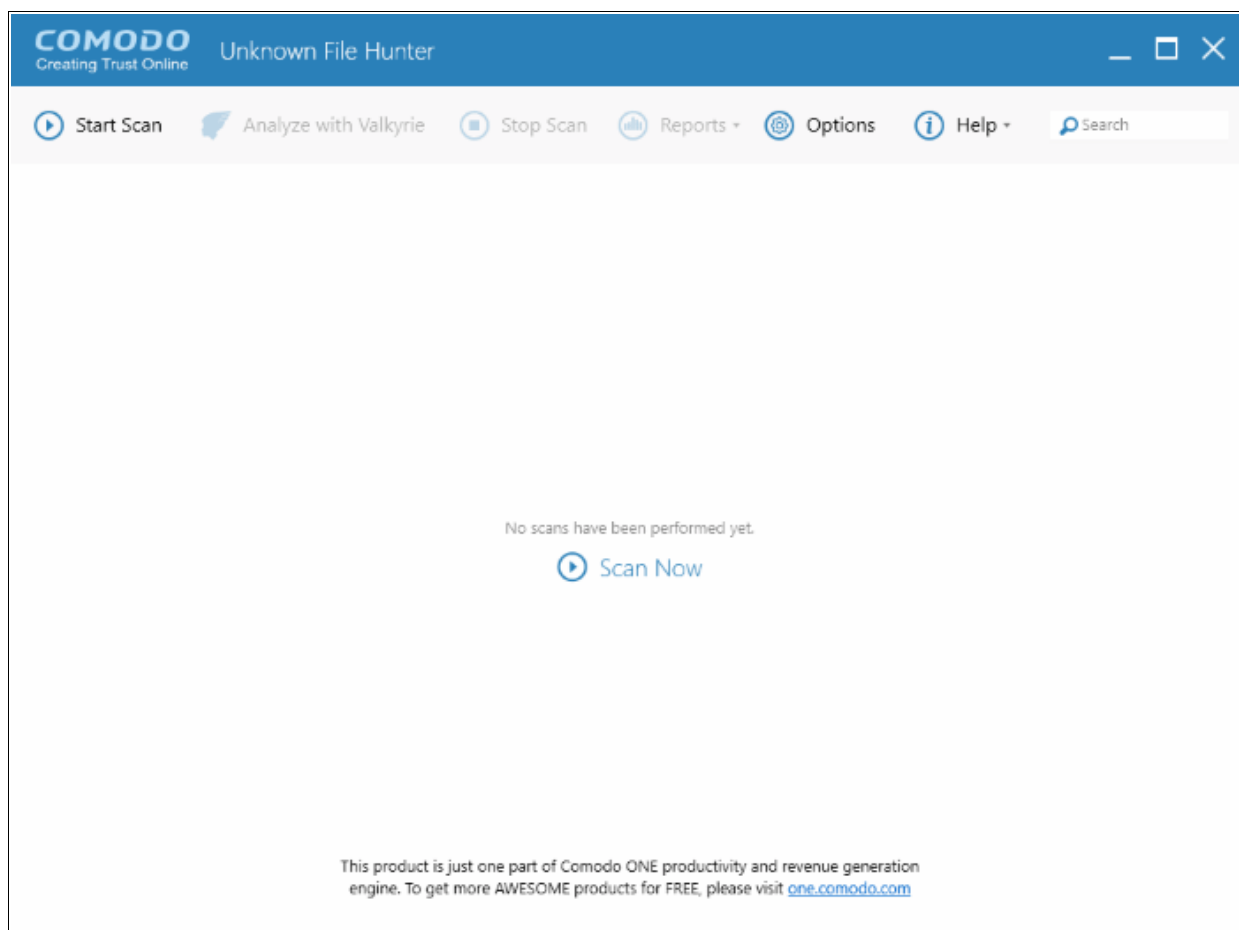
2 Running Unknown File Hunter

Comodo Unknown File Hunter can be downloaded from https://valkyrie.comodo.com/apt_tool/download/UnknownFileHunter.exe.

After saving the application to your computer, you can launch the tool by double-clicking on the application icon:



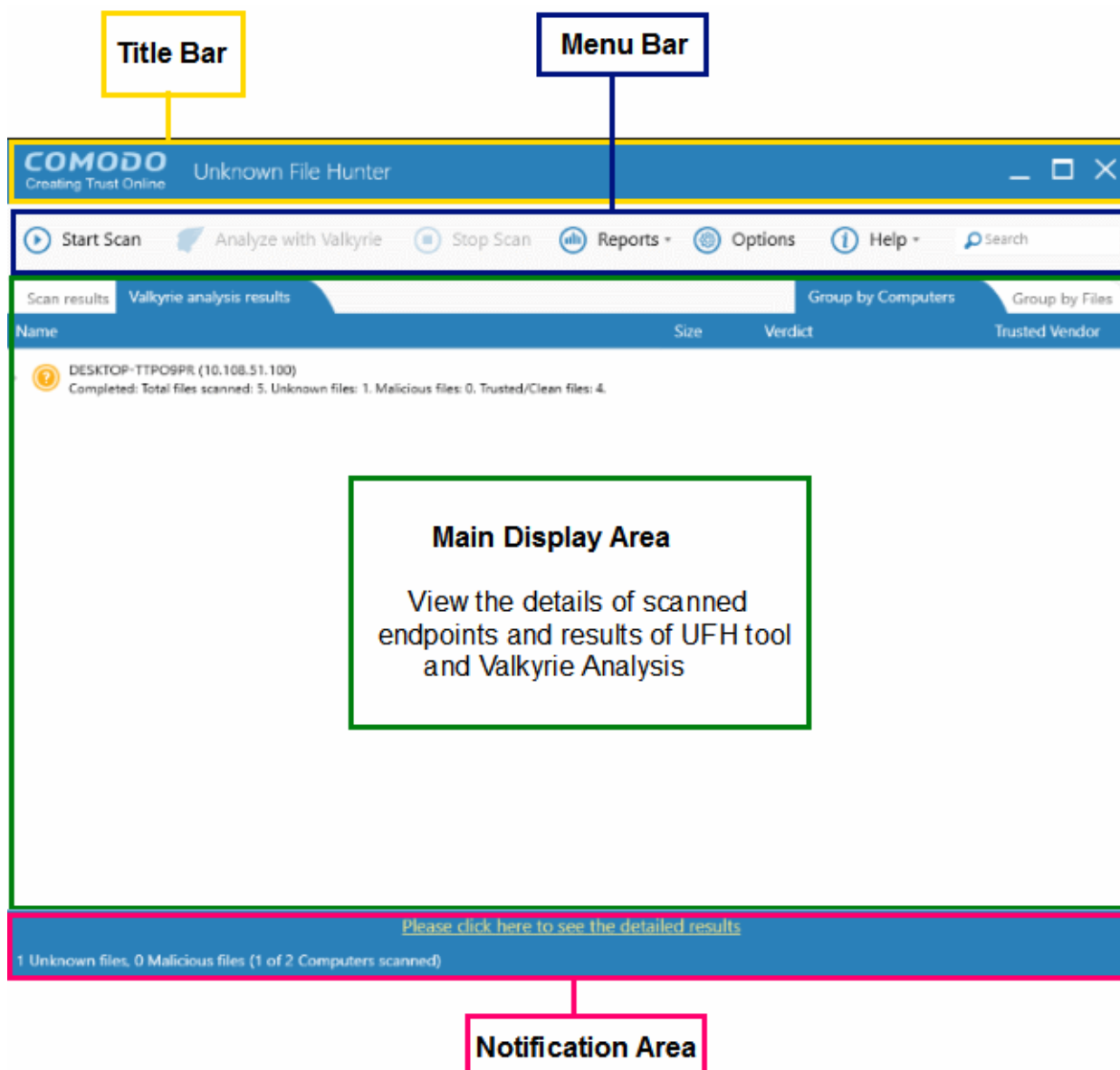
The Main Interface will be displayed.



Refer to the next section '**The Main Interface**' for more details about the features.

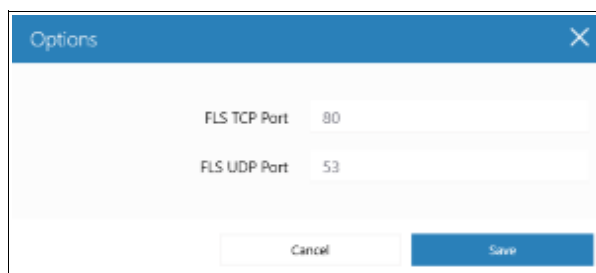
2.1 The Main Interface

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.
 - **Start Scan** - Scan target computers to identify unknown files. You can add computers via Active Directory, Workgroup or Network Addresses. Refer to the section '**Scanning Computers**' for more details.
 - **Stop Scan** - Allows you to cancel the scanning process.
 - **Options** - Displays the port numbers that CUFH 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.

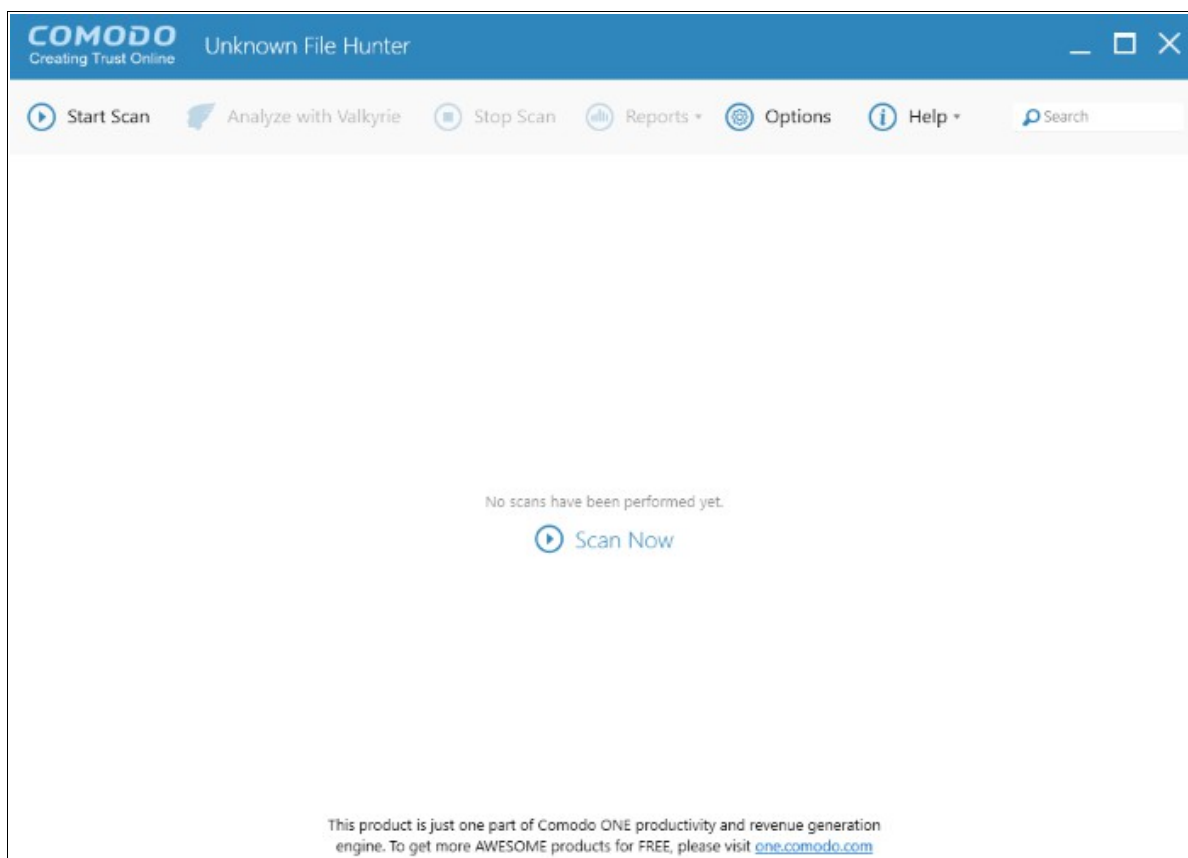


- **Reports** - Allows administrators to view reports generated by the UFH tool and Valkyrie. Refer to the section '**Reports**' for more details.
- **Help** - The 'About' menu entry shows product and version information. Refer to '**About Comodo Unknown File Hunter**' for more details. The 'Agent Requirements' 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 the details of scanned endpoints and the results from UFH and Valkyrie. Refer to the sections '**Scanning Computers**' and '**Scan Results**' for more details.
- **Notification Area** - Displays real-time information about unknown and malicious files detected, and number of endpoints scanned.

3 Scanning Computers

The Comodo UFH tool allows administrators to add computers for scanning in multiple ways. The scanning will be performed by the UFH tool and results displayed. If you want further analysis of the detected files, then you can submit the results to Valkyrie.

- **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 work group for scanning
- **Network Address** - Specify host names, IP addresses or IP ranges of computers which need to be scanned.
- **This Computer** – Allows you to run a scan on your local device.



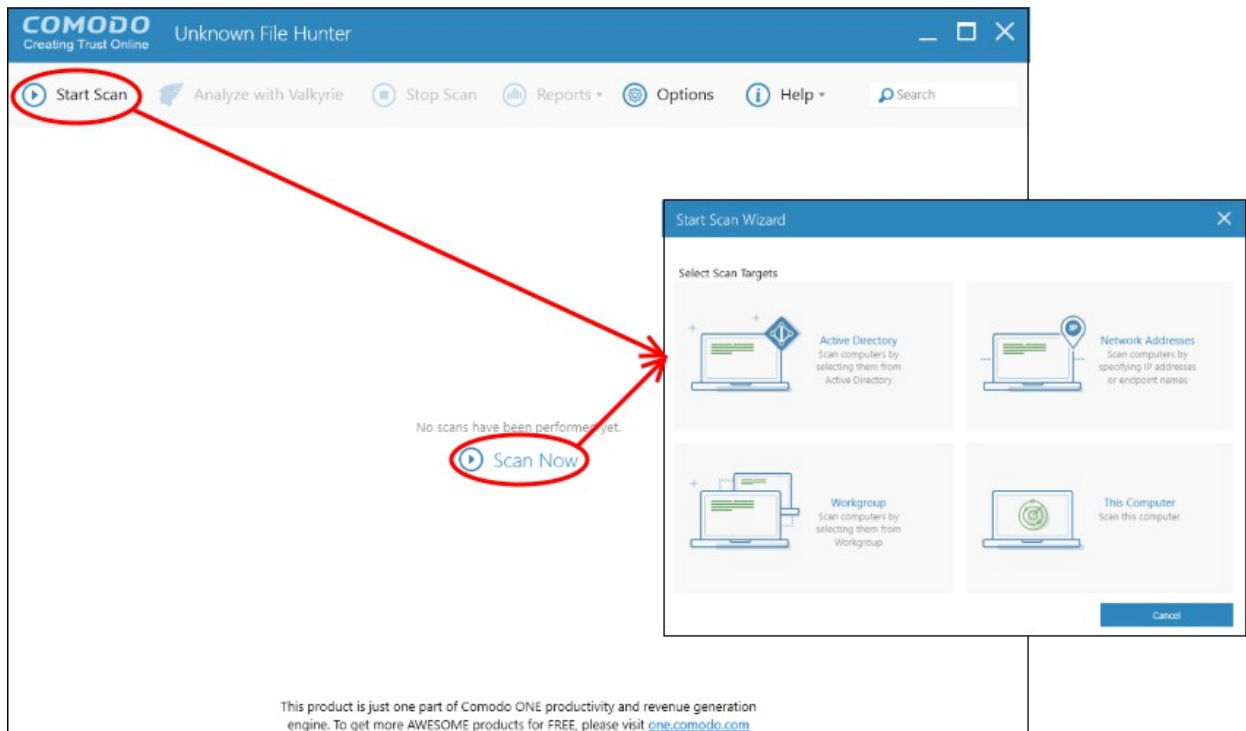
Refer to the following sections for more details:

- **Scanning Computers using Active Directory**
- **Scanning Computers using Workgroup**
- **Scanning Computers by Network Addresses**
- **Scanning Computers by Custom Scan**

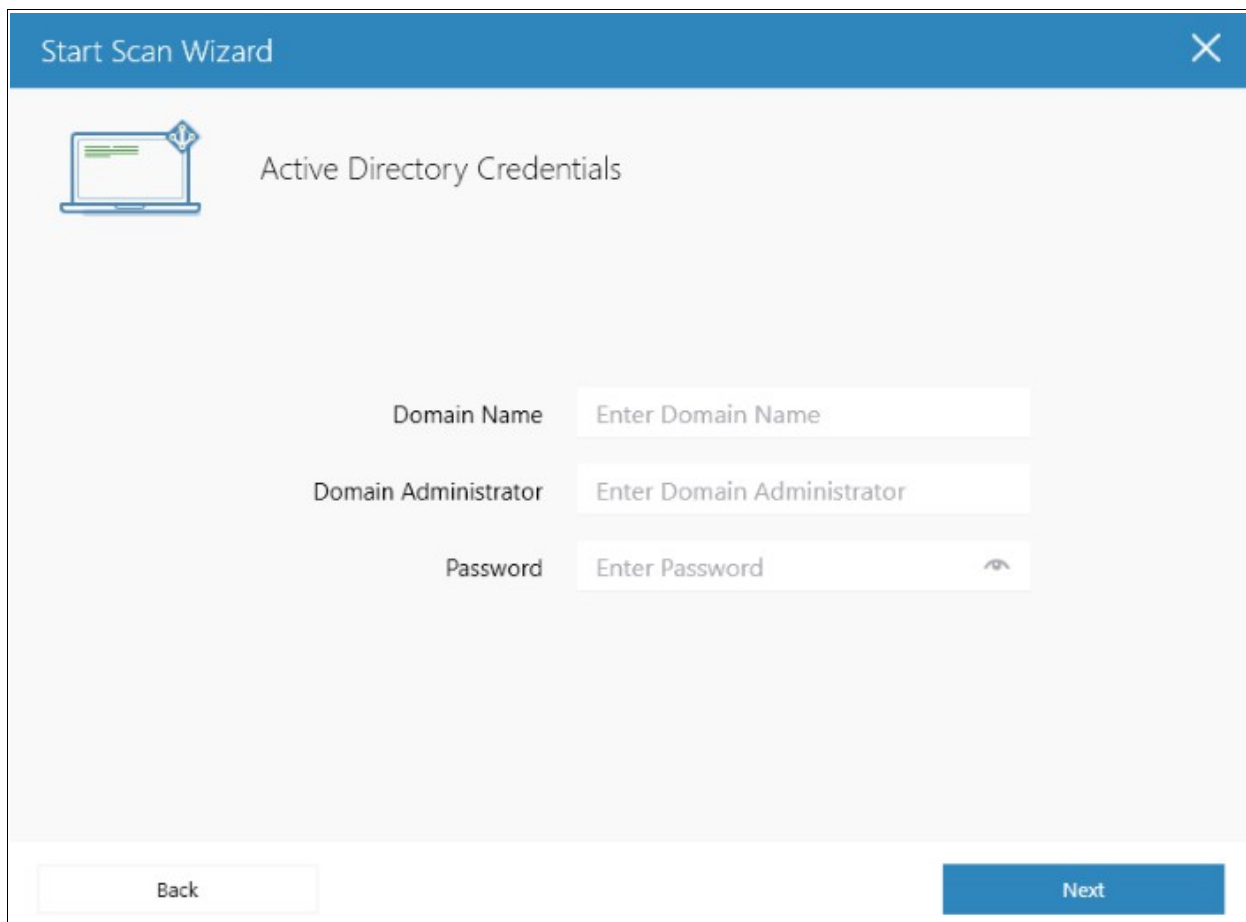
3.1 Scanning Computers using Active Directory

The Active Directory method of adding computers allows administrators to include a number of endpoints in a domain for scanning.

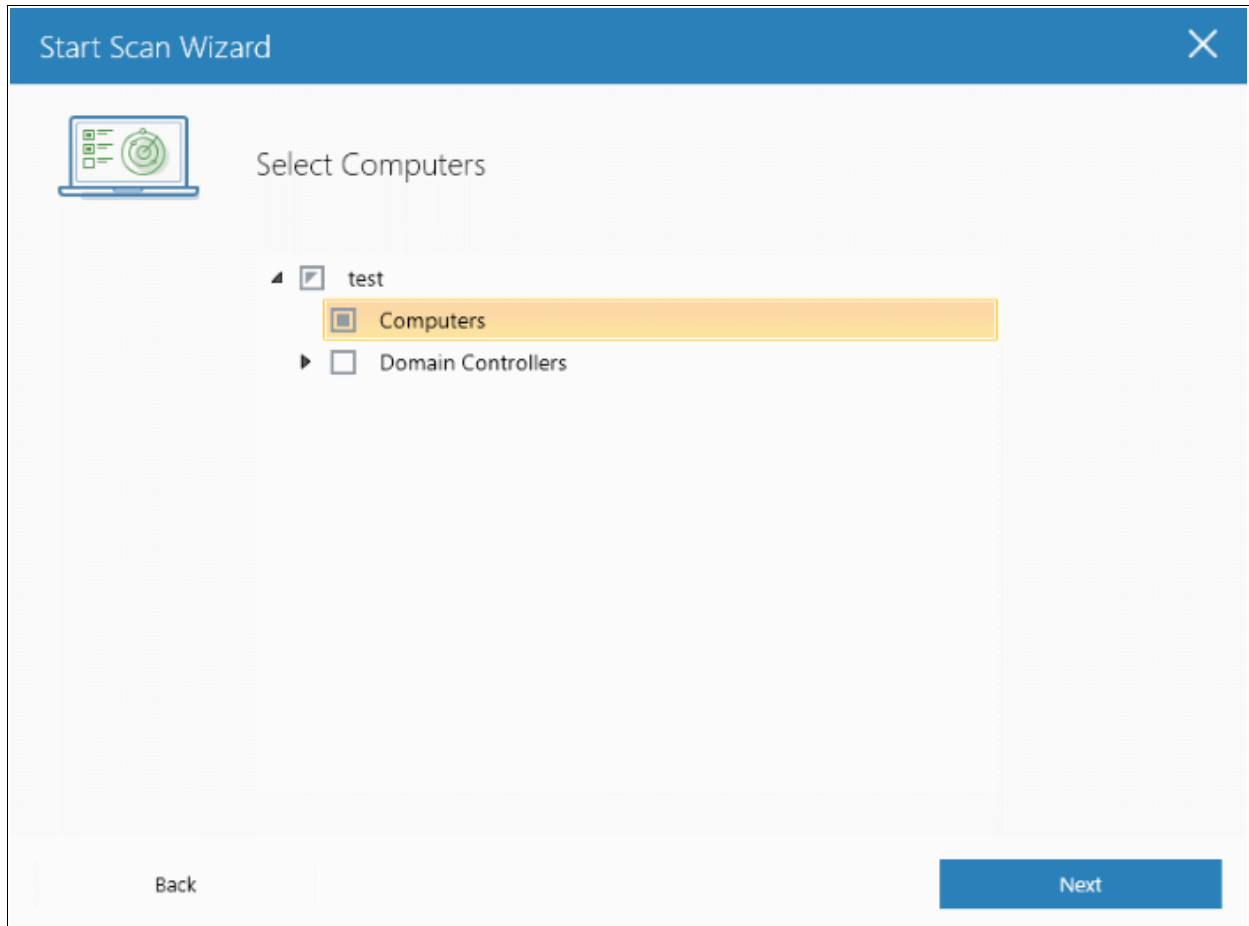
- To open the 'Start Scan Wizard', click the 'Start Scan' button at top-left or the 'Scan Now!' link in the main display area.



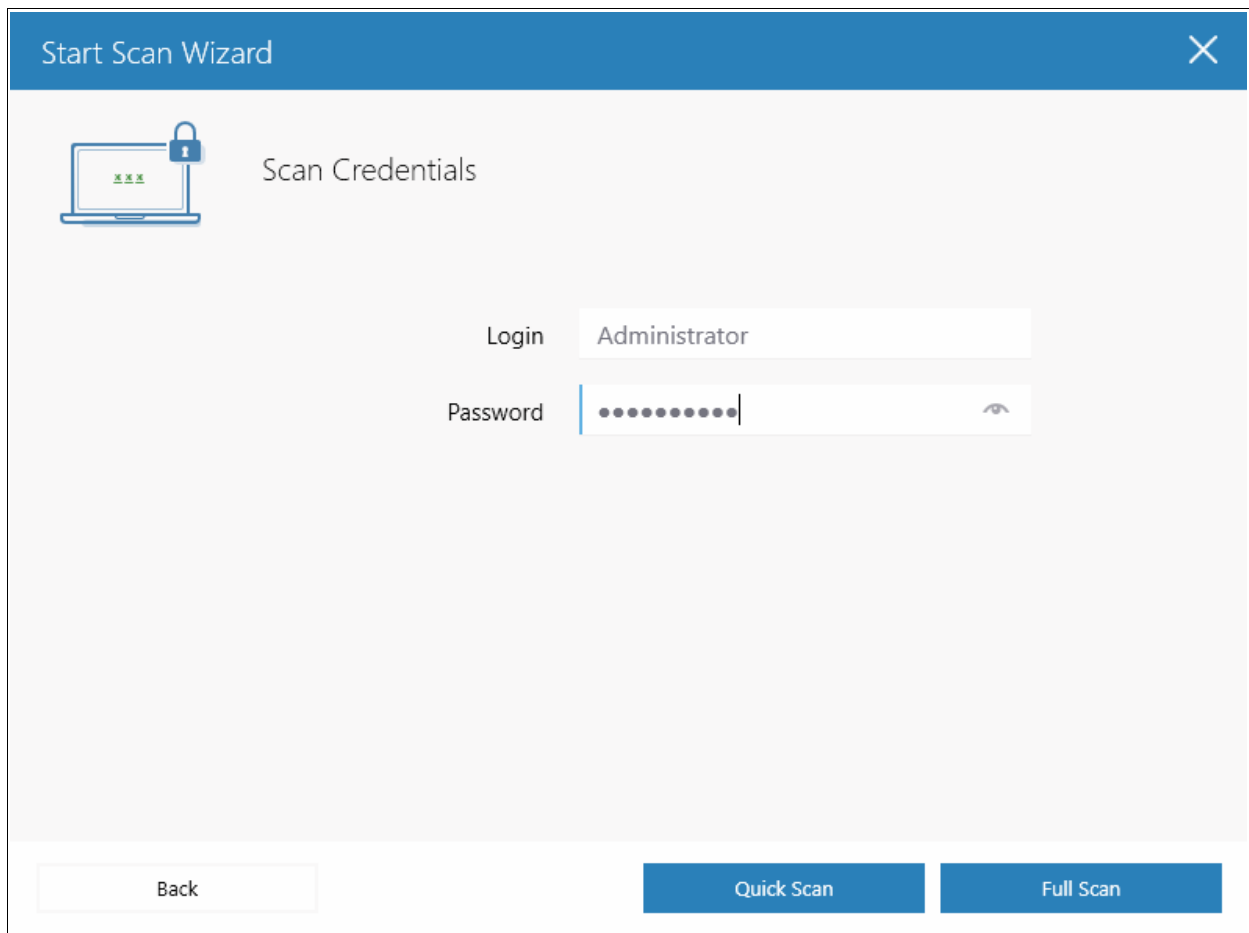
- Select 'Active Directory' to open the AD configuration screen:



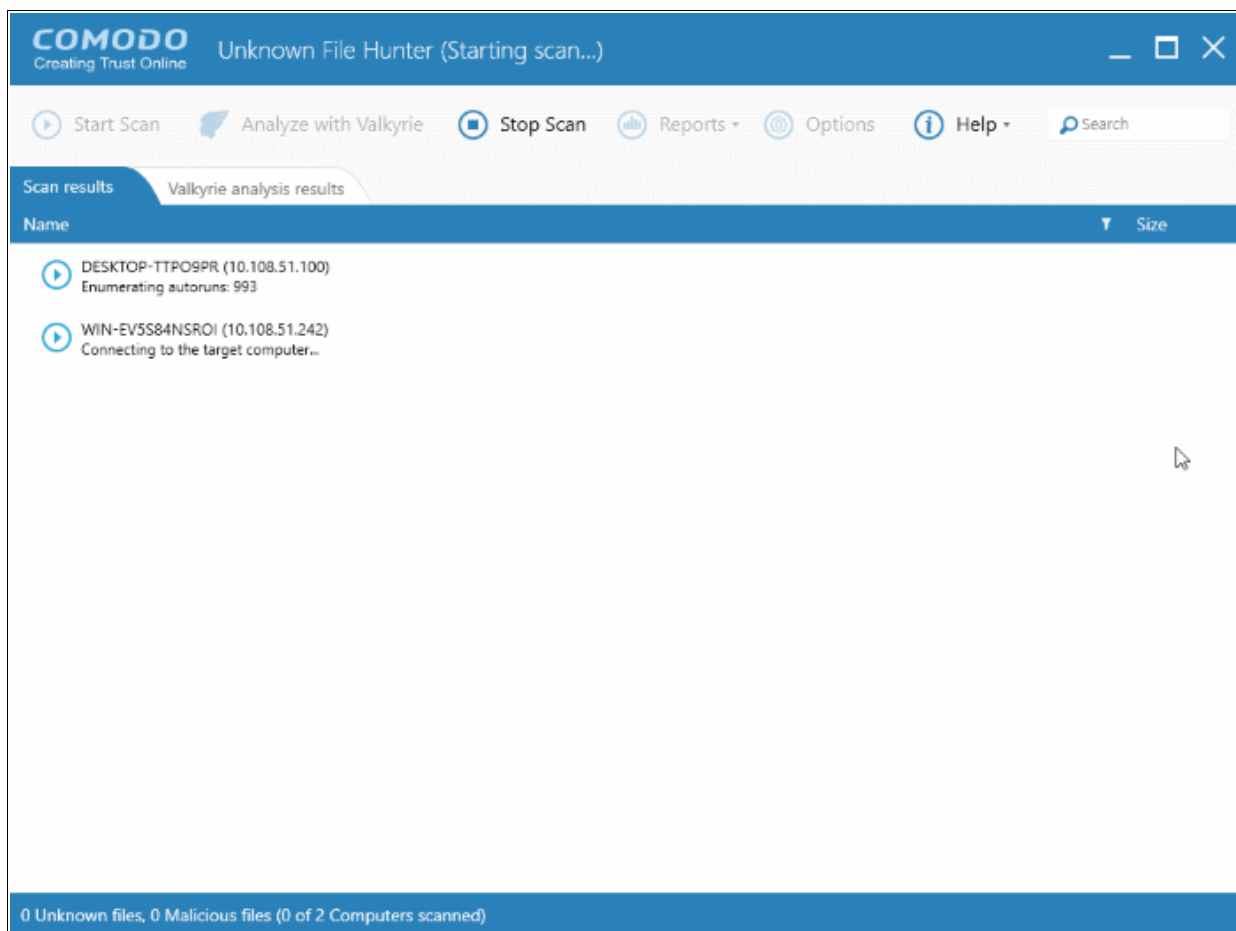
- Enter the domain name and administrator details of your Active Directory.



After successful authentication of the domain details, the 'Select Computers' screen will be displayed.



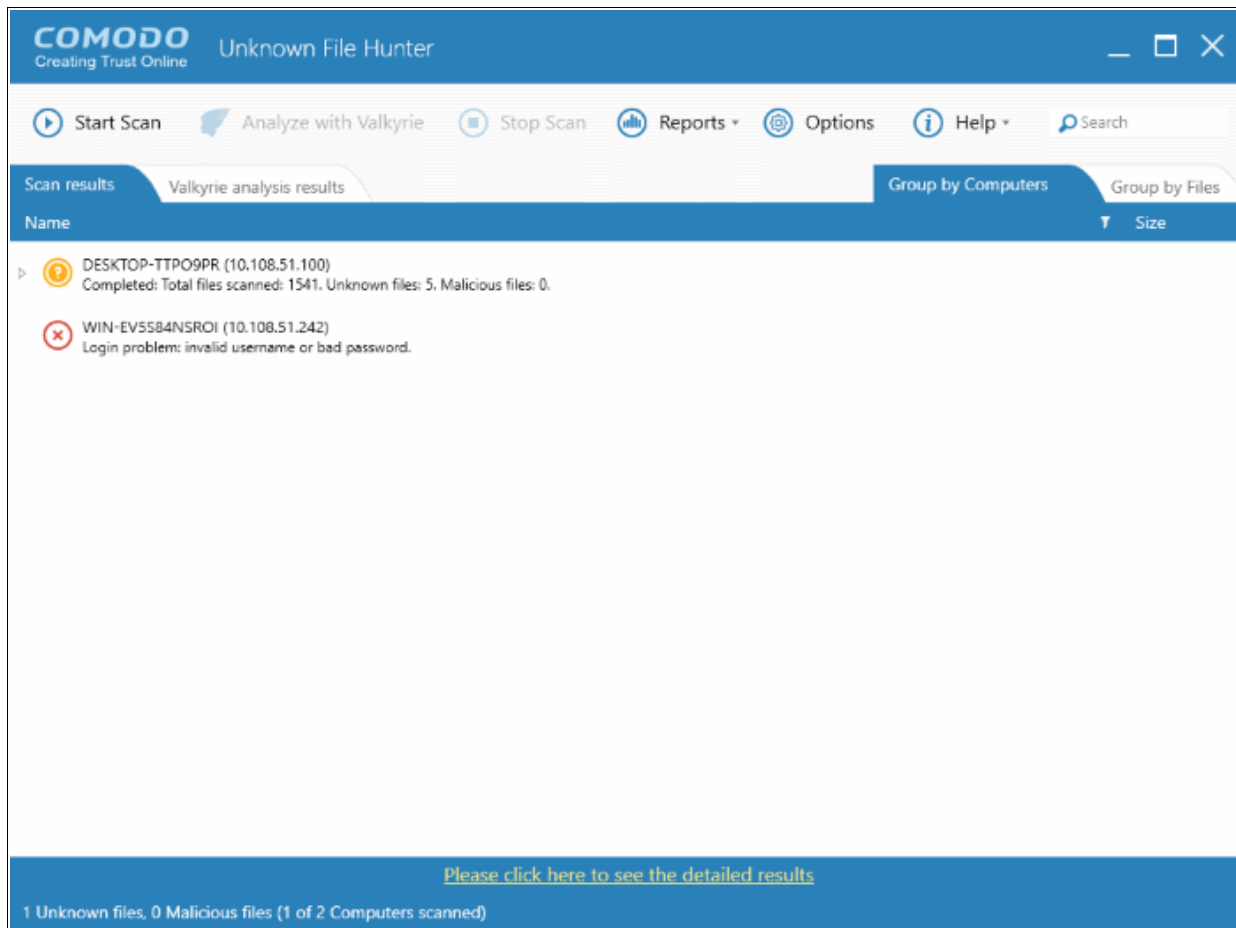
- Select the endpoints that you want to scan and choose one of the following scan types:
Quick Scan: Scans critical and commonly infected areas of target endpoints
Full Scan: Scans all files and folders on target endpoints.



The progress of the scan will be displayed for each computer on the respective rows and the total scanning progress on the title bar.

- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.

The notification bar at the bottom displays the number of unknown and malware programs detected including the number of endpoints being scanned. After the scanning process is completed, the results will be displayed including the option to analyze the results with Valkyrie.

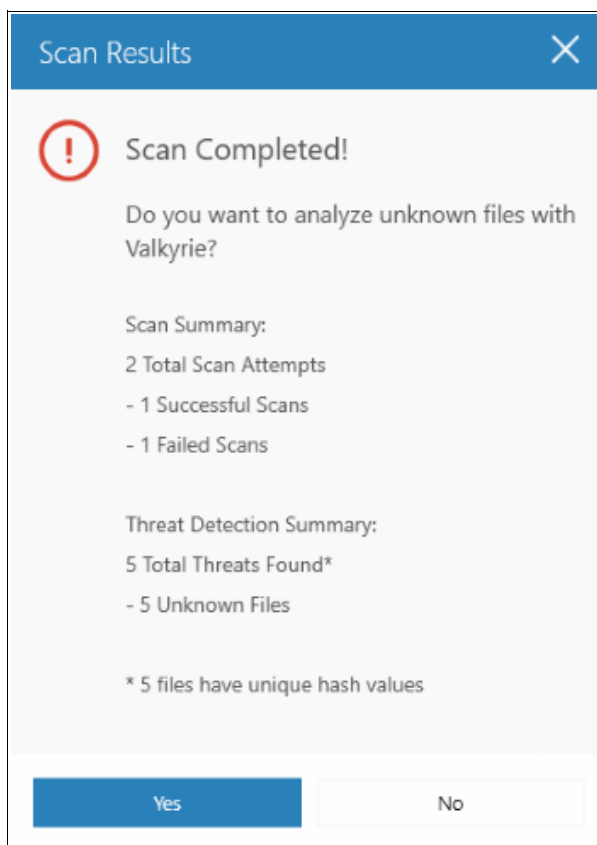


The details of results will be displayed in the respective endpoint rows, providing information such as the number of unknown files, number of malware found, the accessibility to the computers, scan progress and more.

There are results will be displayed in two ways:

Group by Computer: The scan results will display total number of computers scanned and the number of unknown files found in those computers.

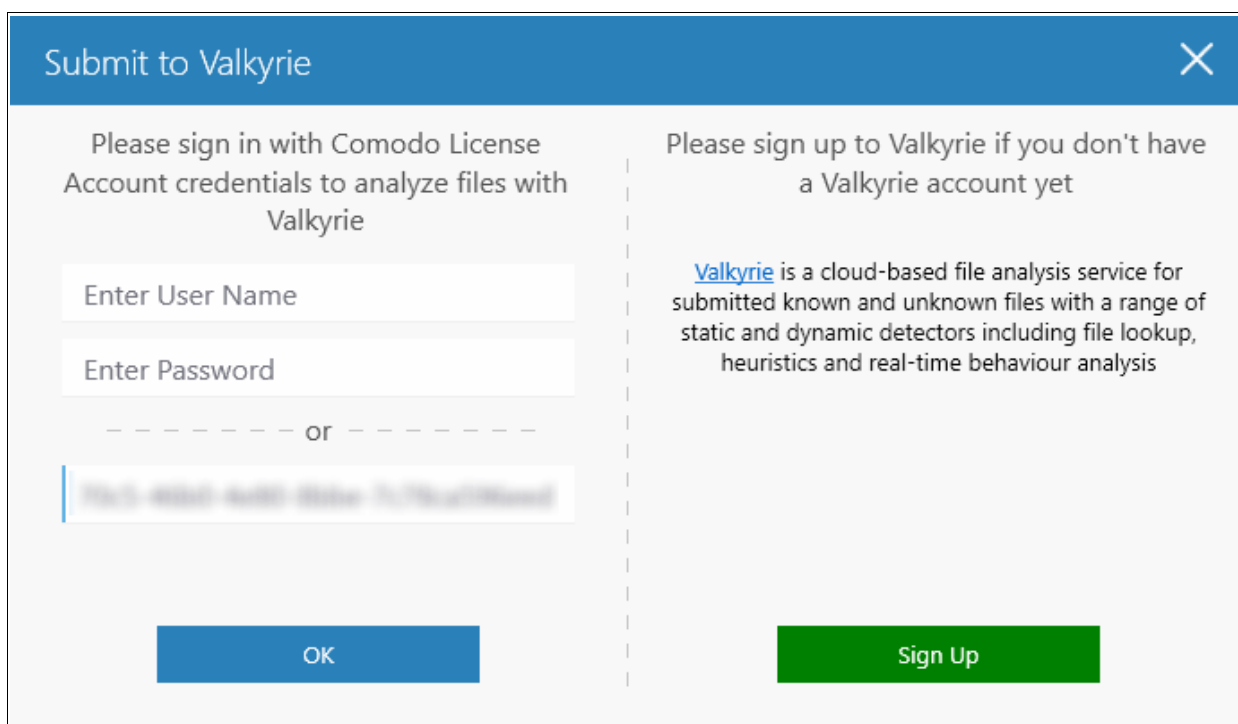
Group by File: The scan results will display the name and number of instances of unknown files identified. The option dialog to analyze the results with Valkyrie will also be displayed:



Valkyrie is an online file verdict service which analyzes the behavior of unknown files with a range of static and dynamic tests. Clicking 'OK' opens the 'Activate Valkyrie' screen. Existing users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Get Valkyrie' to create a free account.



You can also Click 'Analyze with Valkyrie' button to submit to Valkyrie for further analysis



Valkyrie results will be displayed in the Unknown File Hunter interface and, in more detail, in the Valkyrie portal:

Valkyrie

Valkyrie is a file verdict system. Different from traditional signature based malware detection techniques Valkyrie conducts several analysis using run-time behavior and hundreds of features from a file and based on analysis results can warn users against malwares undetected by classic Anti-Virus products.

[DOWNLOAD UNKNOWN FILE HUNTER](#)

LATEST FILE UPLOADS

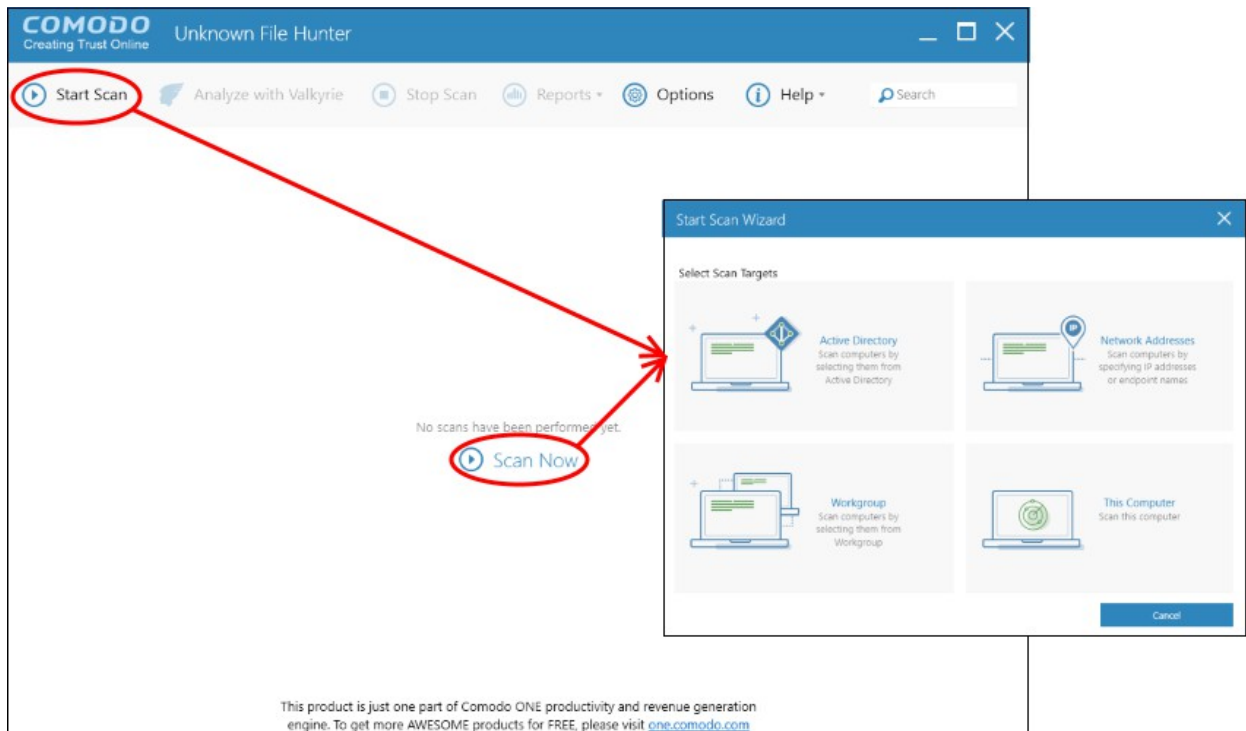
SHA1	File Name	Source	Submit Date	Final Verdict	Human Expert Verdict	Human Expert Analysis Status
545e3297ed5f6324f261921bb5f00776c7bf6bc	VLC_Media_Player_Setup.exe	Upload	2016-12-19 18:48:35	PUA	PUA	Completed
4476e9dc1b397f89fa2e1ec5256fced6dcaff686	be25	Upload	2016-12-19 12:48:16	Malware	Malware	Completed
bc46a374f8215e5a0b35ff0ce11af1ed8a292e9b	Driver_9291.exe	Upload	2016-12-19 11:29:00	PUA	PUA	Completed
c23d29666c5e67b90a5782d71729edffcc43991b	8550bd85bd1f774ab87cb86...	Upload	2016-12-19 11:24:58	PUA	PUA	Completed
60904de5d6f45714fd9d8d1dc91528b04448d7d1	Adobe_Flash_Player_xetapp....	Upload	2016-12-19 11:24:27	Malware	Malware	Completed

Refer to the section '[Analyzing Files with Valkyrie](#)' and '[Scan Results](#)' for more details.

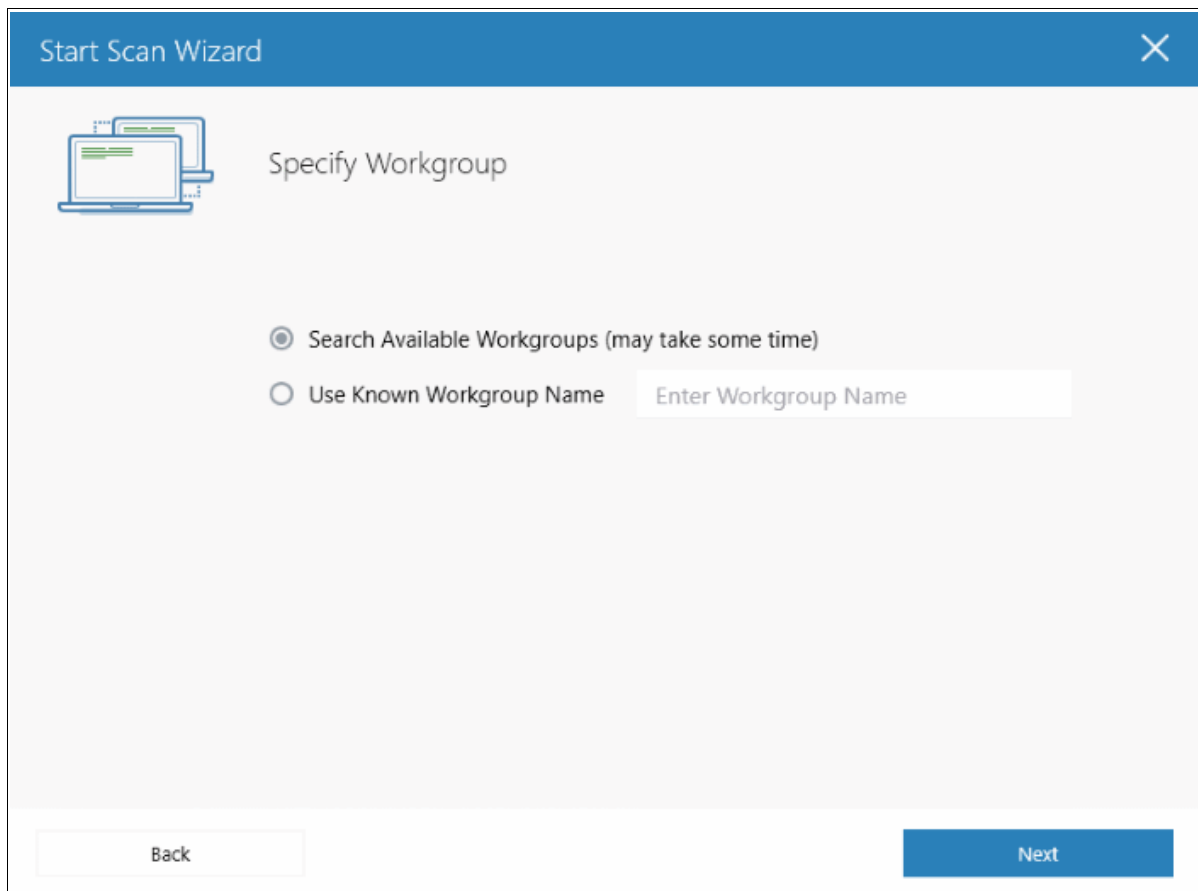
3.2 Scanning Computers using Workgroup

The Comodo UFH tool allows administrators to run a scan on computers that are available within a Workgroup.

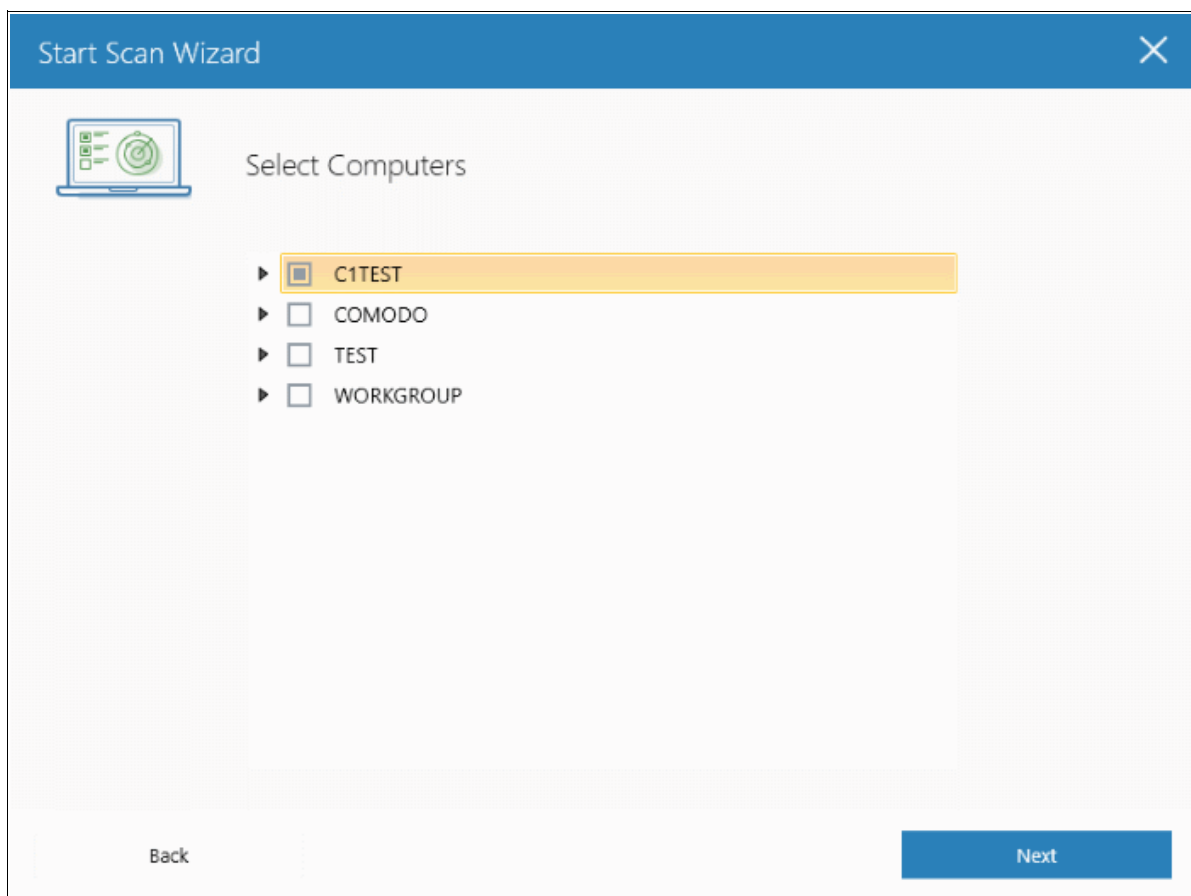
To open the 'Start Scan Wizard' screen, click the 'Start Scan' button at the top-left or the 'Scan Now!' link in the main display area.



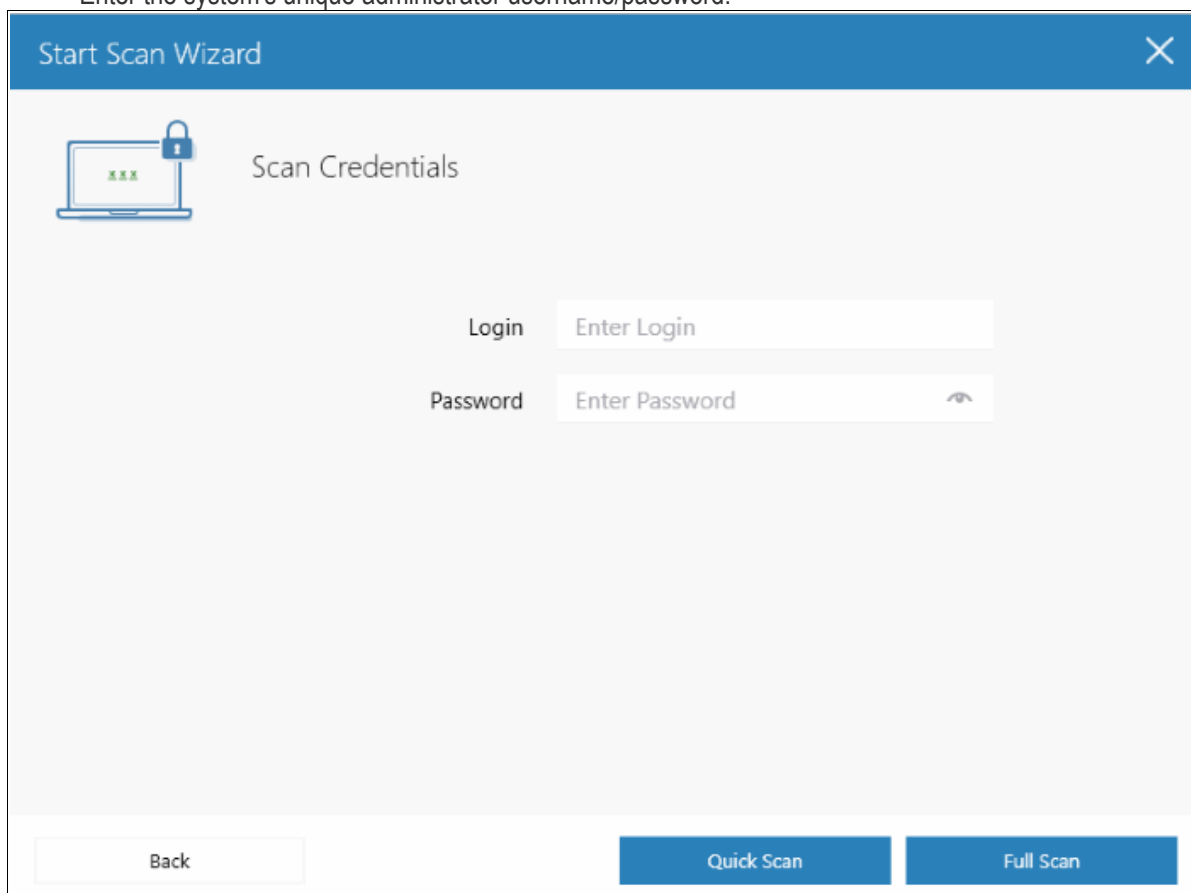
- Click 'Workgroup' and select the available workgroups or enter the domain name of your existing Workgroup



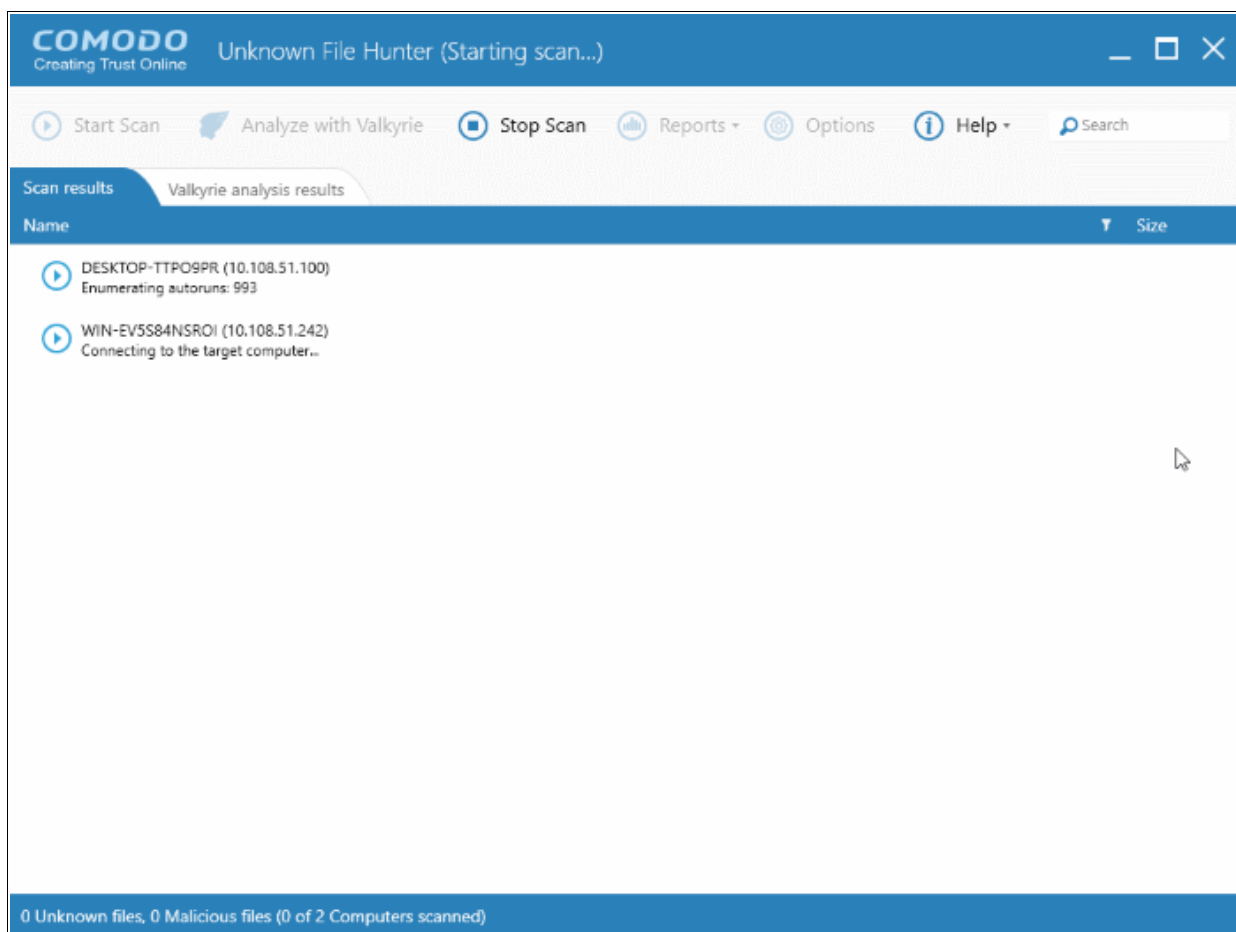
- Select the endpoints that you want to scan and choose one of the following scan types:
 - Quick Scan:** Scans critical and commonly infected areas of target endpoints
 - Full Scan:** Scans all files and folders on target endpoints.



- Enter the system's unique administrator username/password.

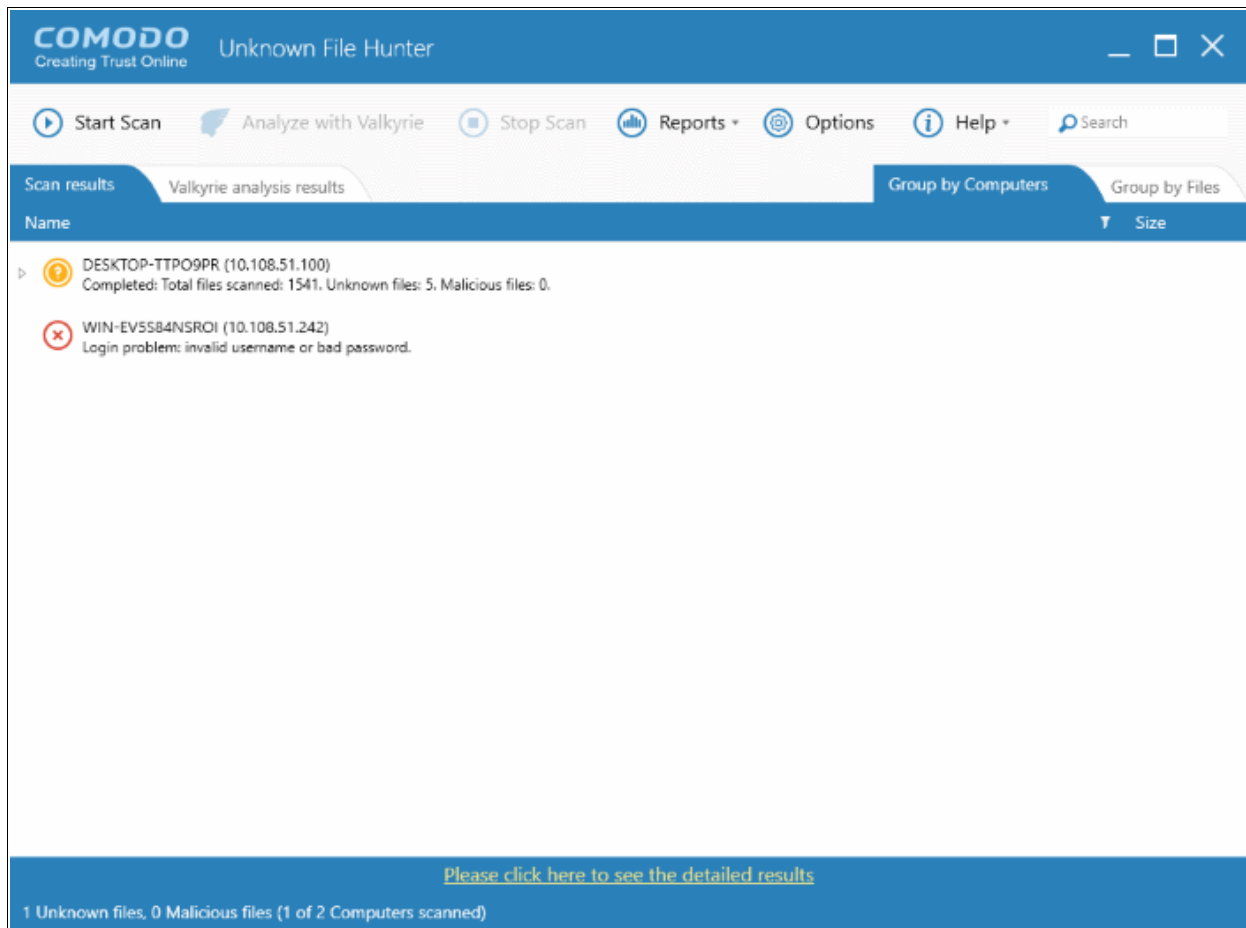


After successful authentication, the scanning of endpoints in the Workgroup will start.



- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.

The notification bar at the bottom displays the number of unknown and malware programs detected, the number of endpoints scanned, the accessibility to the computers, scan progress details and more. Full results will be displayed after the scan finishes. You will also be given the opportunity to analyze unknown files with Valkyrie:

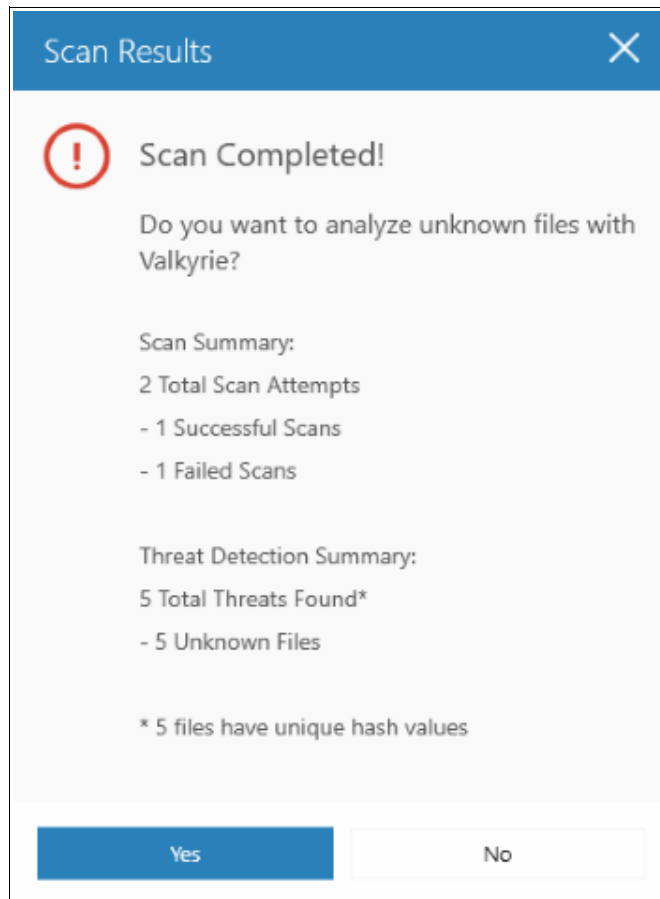


For each endpoint that was successfully scanned, you'll see total number of files scanned and the number of unknown and malware files found. Results can be viewed in two ways:

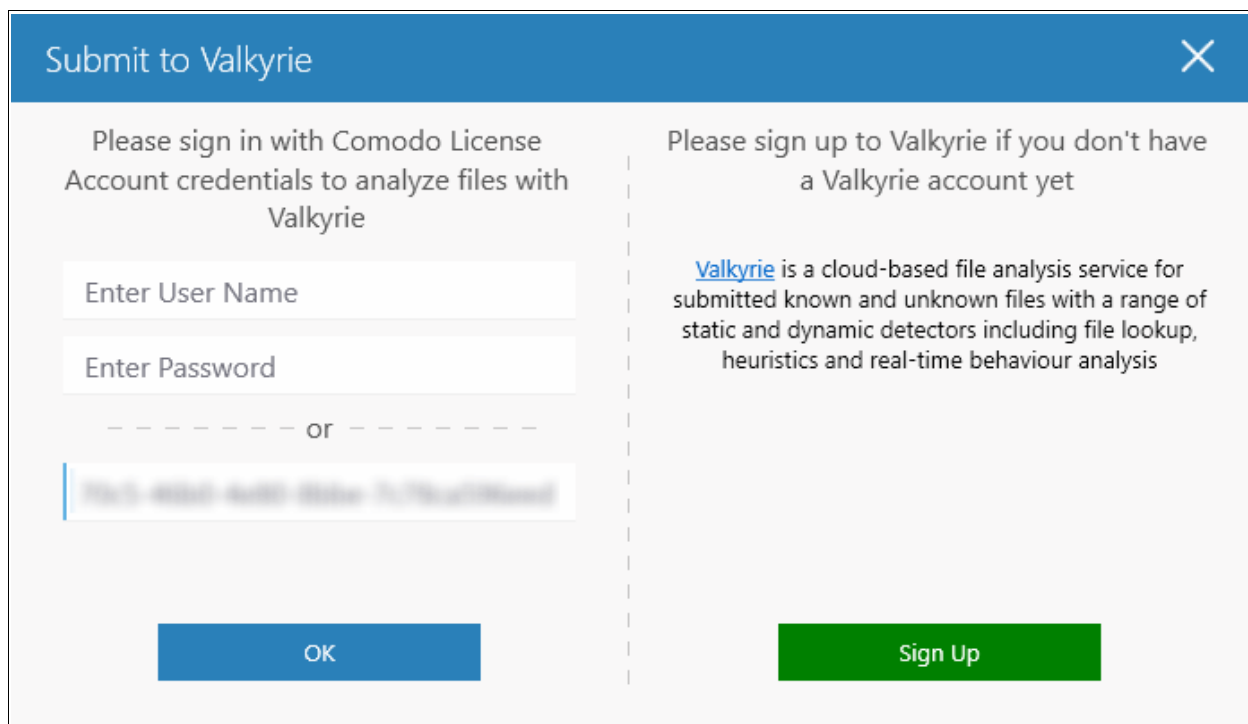
Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

Group by File: Shows the name and quantity of each unknown file.

The option to analyze the results with Valkyrie will also be displayed:



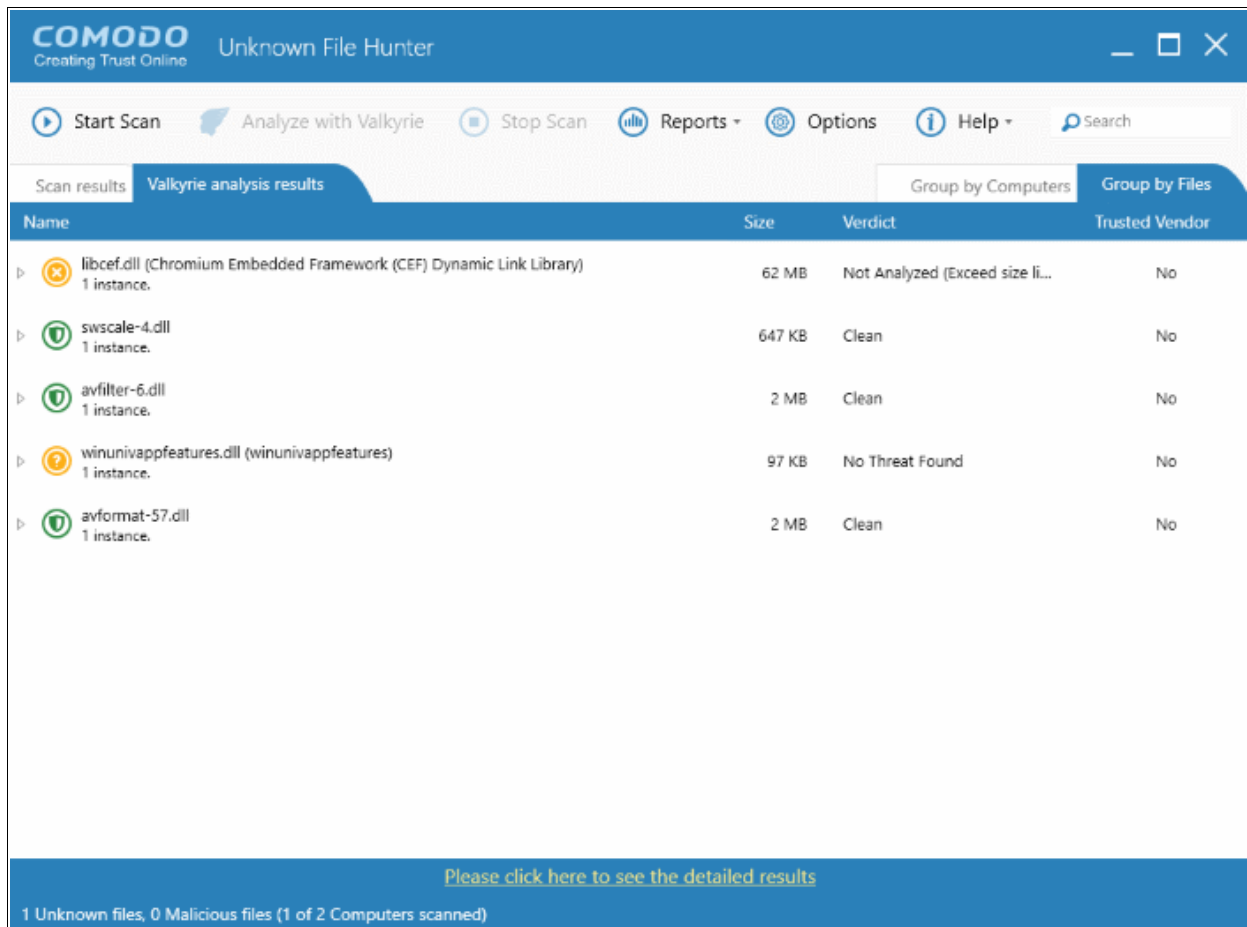
Tap 'Yes' to open the 'Submit to Valkyrie' dialog:



Existing 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.

You can also find your license key by logging in at <https://accounts.comodo.com/> and visiting <https://accounts.comodo.com/valkyrie/management>

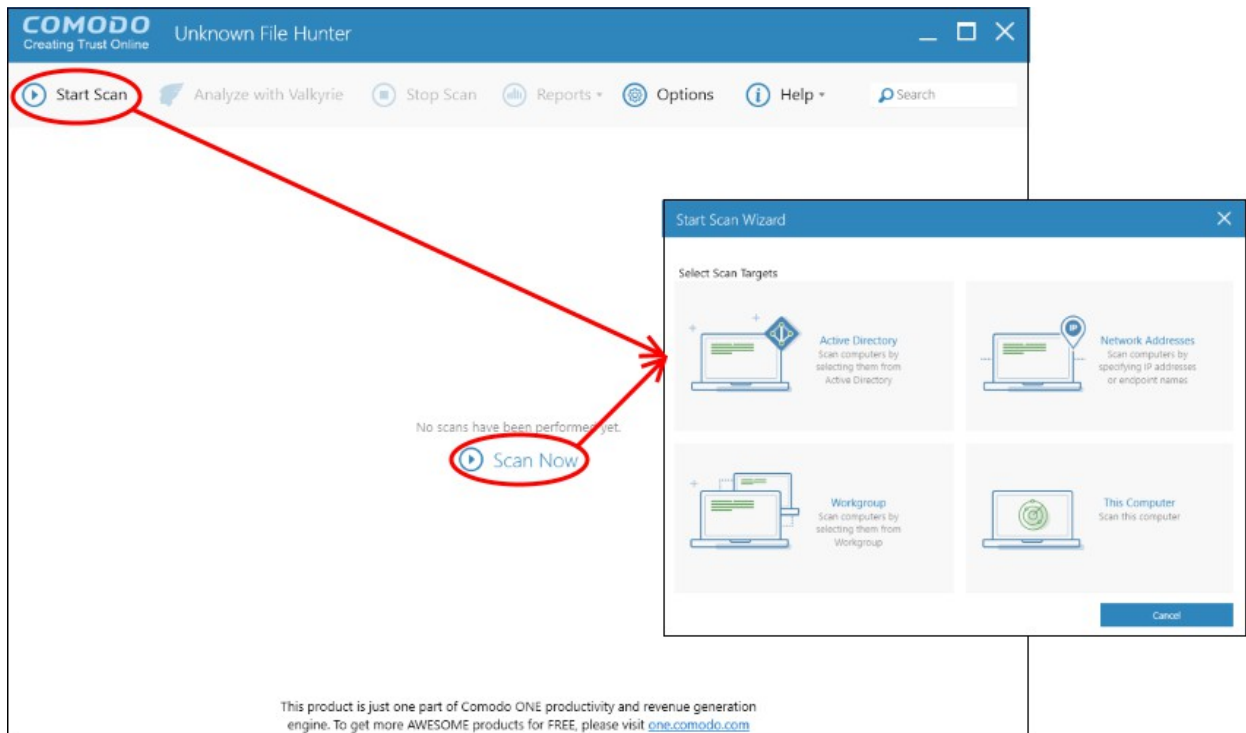
Please note that you will be able to view results in 'Valkyrie analysis results' only after the tool provides a verdict on scan results.



Refer to the section '[Analyzing Files with Valkyrie](#)' and '[Scan Results](#)' for more details.

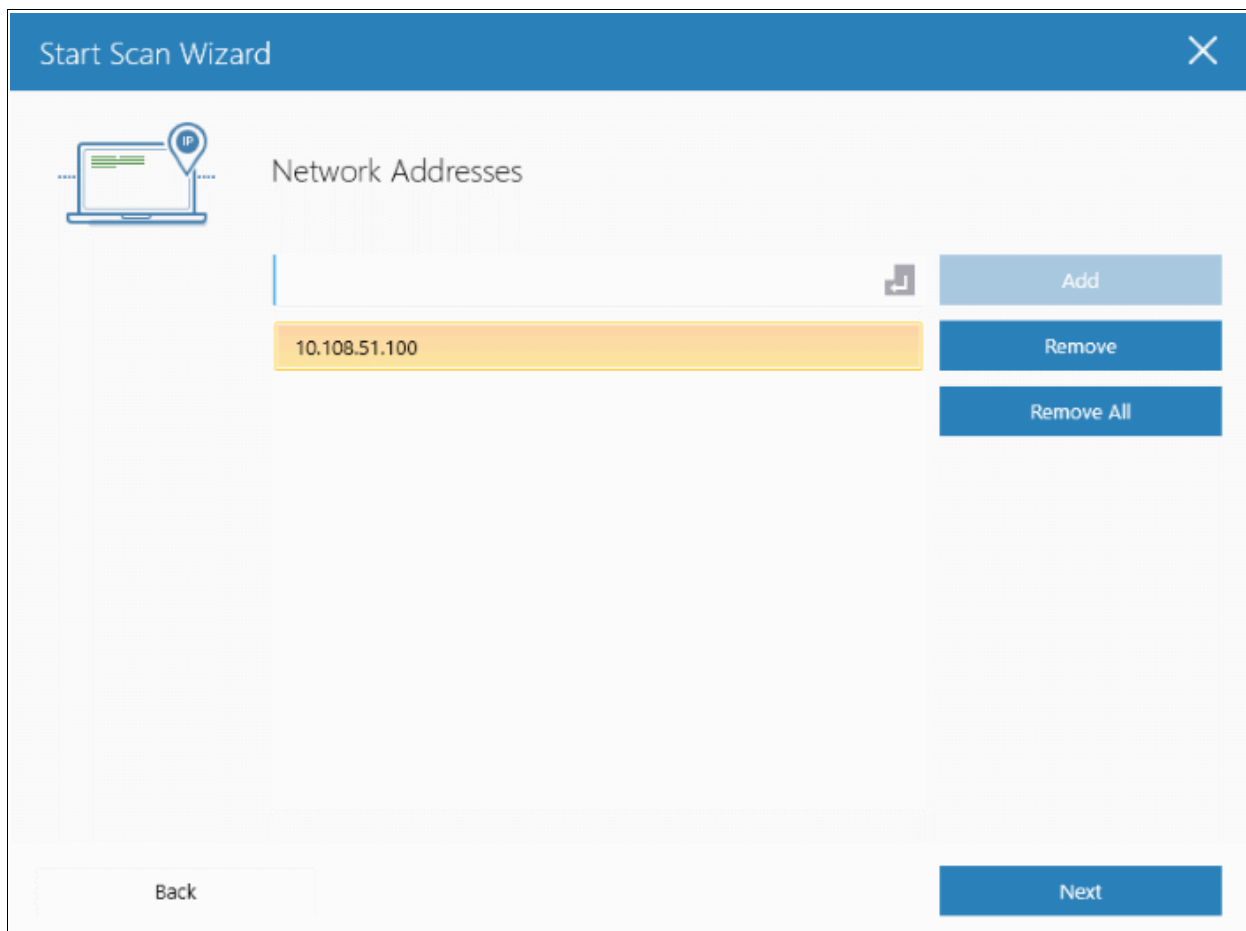
3.3 Scanning Computers by Network Addresses

Comodo UFH allows administrators to scan computers by specifying their IP address or hostname.



To open the 'Start Scan Wizard', click the 'Start Scan' button at the top-left or the 'Scan Now!' link in the main display area.

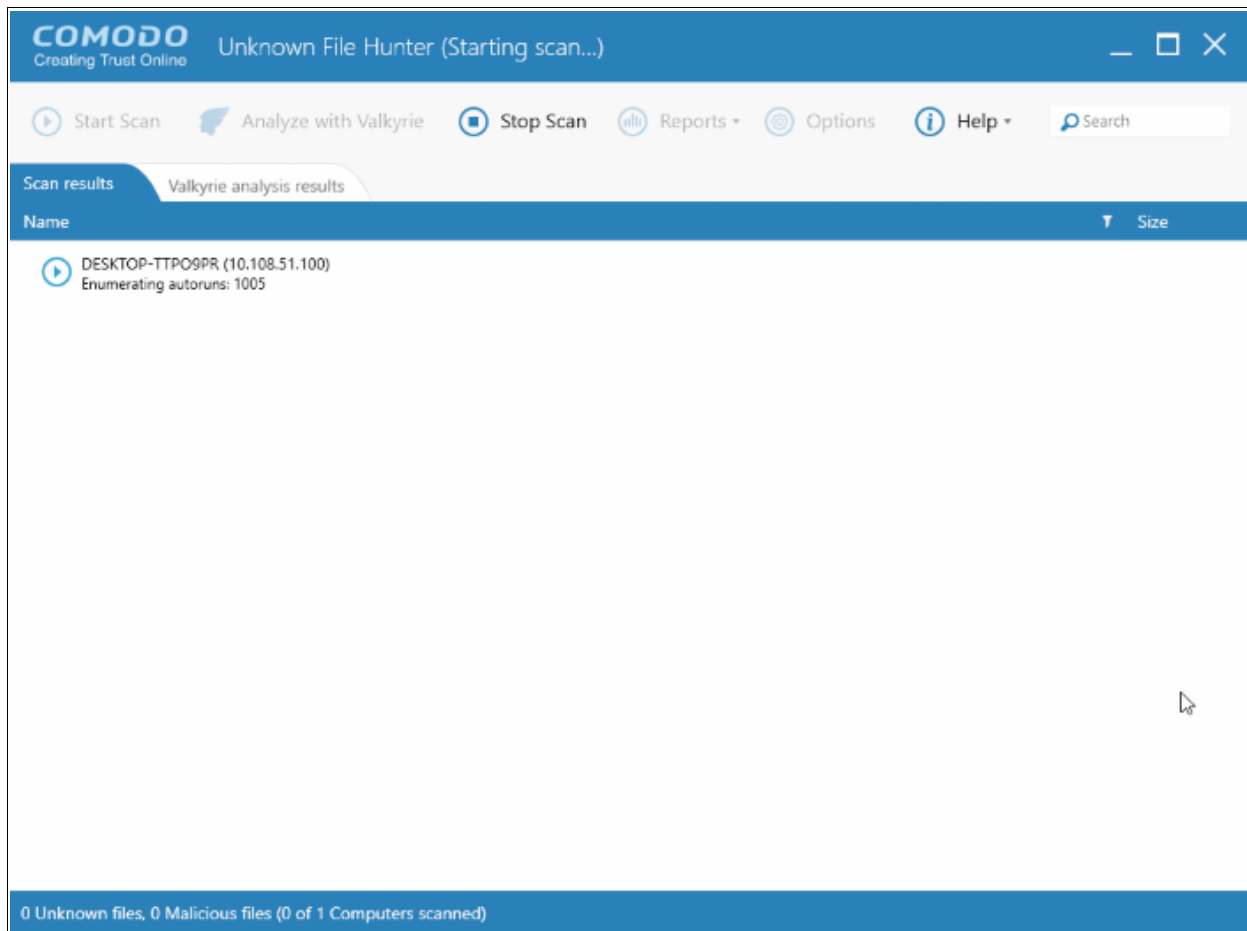
- Click 'Network Addresses'



- 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 with custom credentials.
- Next, click either the 'Quick Scan' or 'Full Scan' button to start the scan.
 - **Quick Scan:** Scans critical and commonly infected areas of target endpoints
 - **Full Scan:** Scans all files and folders on target endpoints.



- The scan will begin after UFH successfully connects to the device.
- Click the 'Stop Scan' button if you want to discontinue the scanning process.

The notification bar at the bottom displays the number of unknown and malware programs detected, the number of endpoints scanned, the accessibility to the computers, scan progress details and more. Full results will be displayed after the scan finishes.

COMODO Unknown File Hunter

Start Scan Analyze with Valkyrie Stop Scan Reports Options Help Search

Scan results Valkyrie analysis results Group by Computers Group by Files

Name	Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	
c:\program files\freedownloadmanager.org\free download manager\qt5qml.dll	2 MB
C:\Program Files (x86)\OpenOffice 4\program\unopkg.exe	11 KB
c:\program files\freedownloadmanager.org\free download manager\common.dll	416 KB
c:\program files\freedownloadmanager.org\free download manager\imageformats\jpeg.dll	234 KB
c:\program files\freedownloadmanager.org\free download manager\libcef.dll	62 MB
c:\program files\freedownloadmanager.org\free download manager\swscale-4.dll	647 KB
c:\program files\freedownloadmanager.org\free download manager\avfilter-6.dll	2 MB
c:\program files\freedownloadmanager.org\free download manager\winwfpmonitorexe	829 KB
c:\program files\freedownloadmanager.org\free download manager\sqldrivers\sqlite.dll	866 KB

Please click here to see the detailed results

1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)

You will also be given the opportunity to analyze unknown files with Valkyrie.

COMODO Unknown File Hunter

Start Scan Analyze with Valkyrie Stop Scan Reports Options Help Search

Scan results Valkyrie analysis results Group by Computers Group by Files

Name	Size	Verdict	Trusted Vendor
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 4. Unknown files: 1. Malicious files: 0. Trusted/Clean files: 3.			

Please click here to see the detailed results

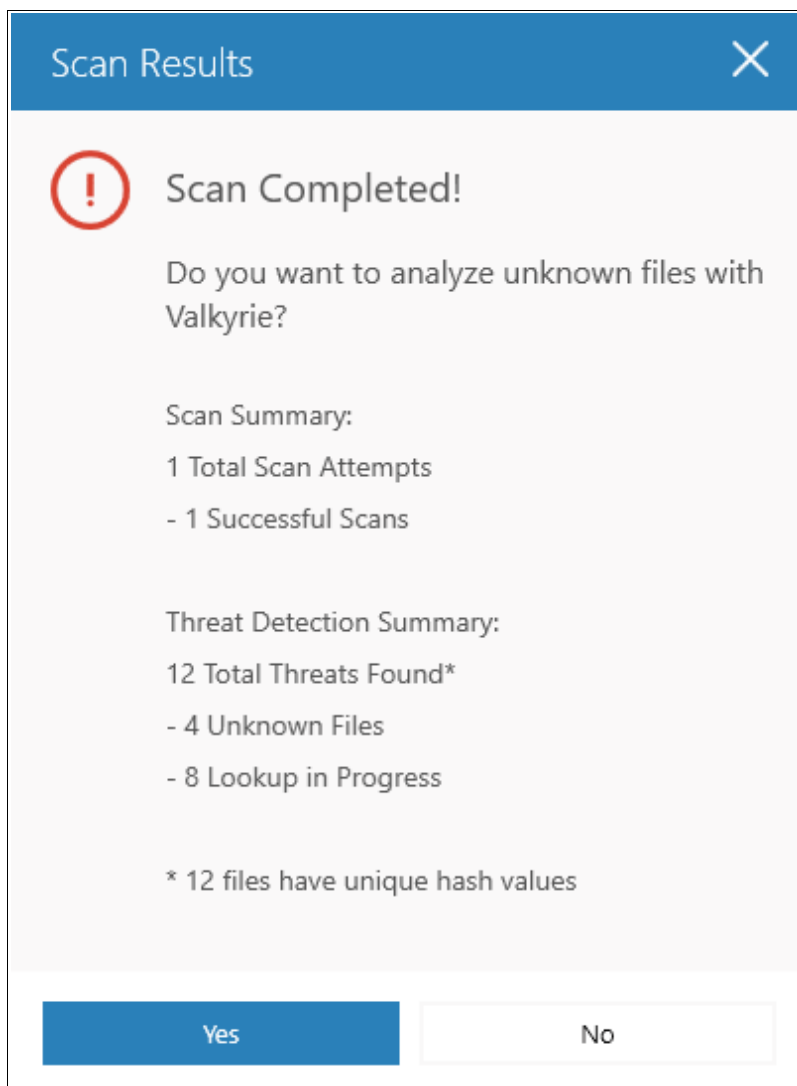
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)

For each endpoint that was successfully scanned, you'll see total number of files scanned and the number of unknown and malware files found. Results can be viewed in two ways:

Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

Group by File: Shows the name and quantity of each unknown file.

The option to analyze the results with Valkyrie will also be displayed:



Click 'Yes' to open the Valkyrie options dialog.

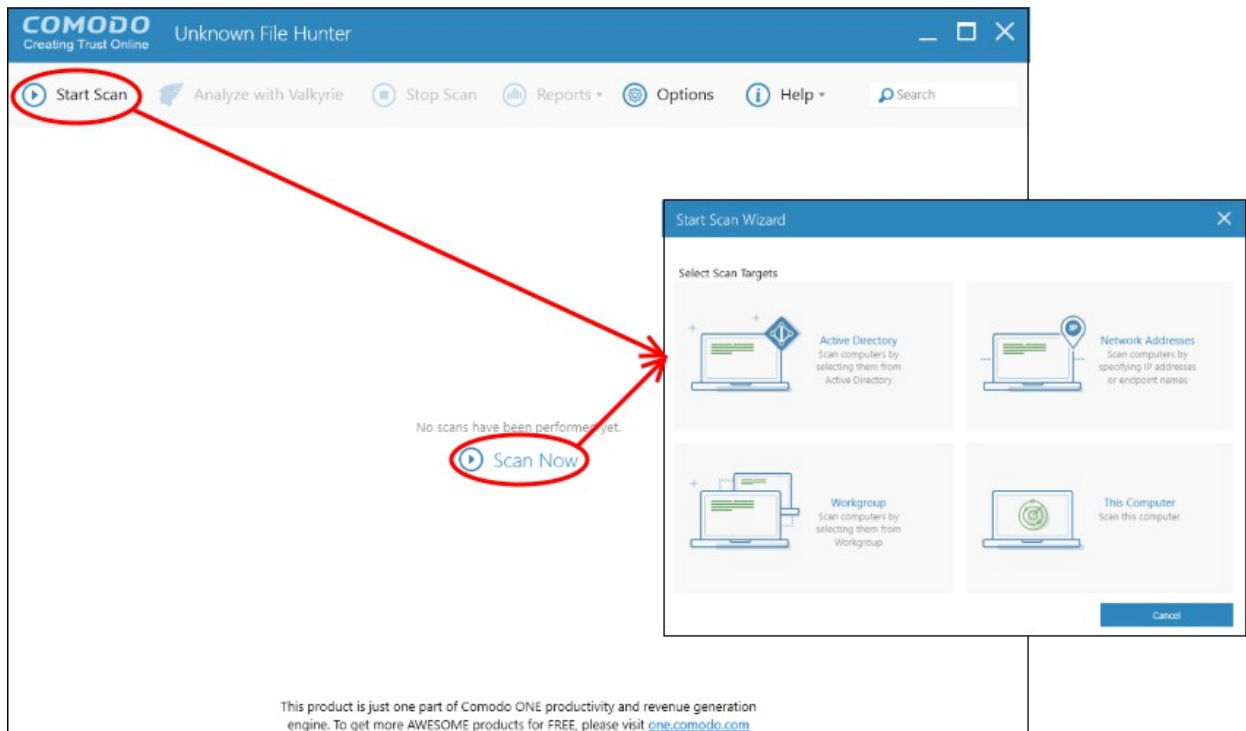
Existing users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

You can also find your license key by logging in at <https://accounts.comodo.com/> .and visiting <https://accounts.comodo.com/valkyrie/management>

Refer to the section '[Analyzing Files with Valkyrie](#)' and '[Scan Results](#)' for more details.

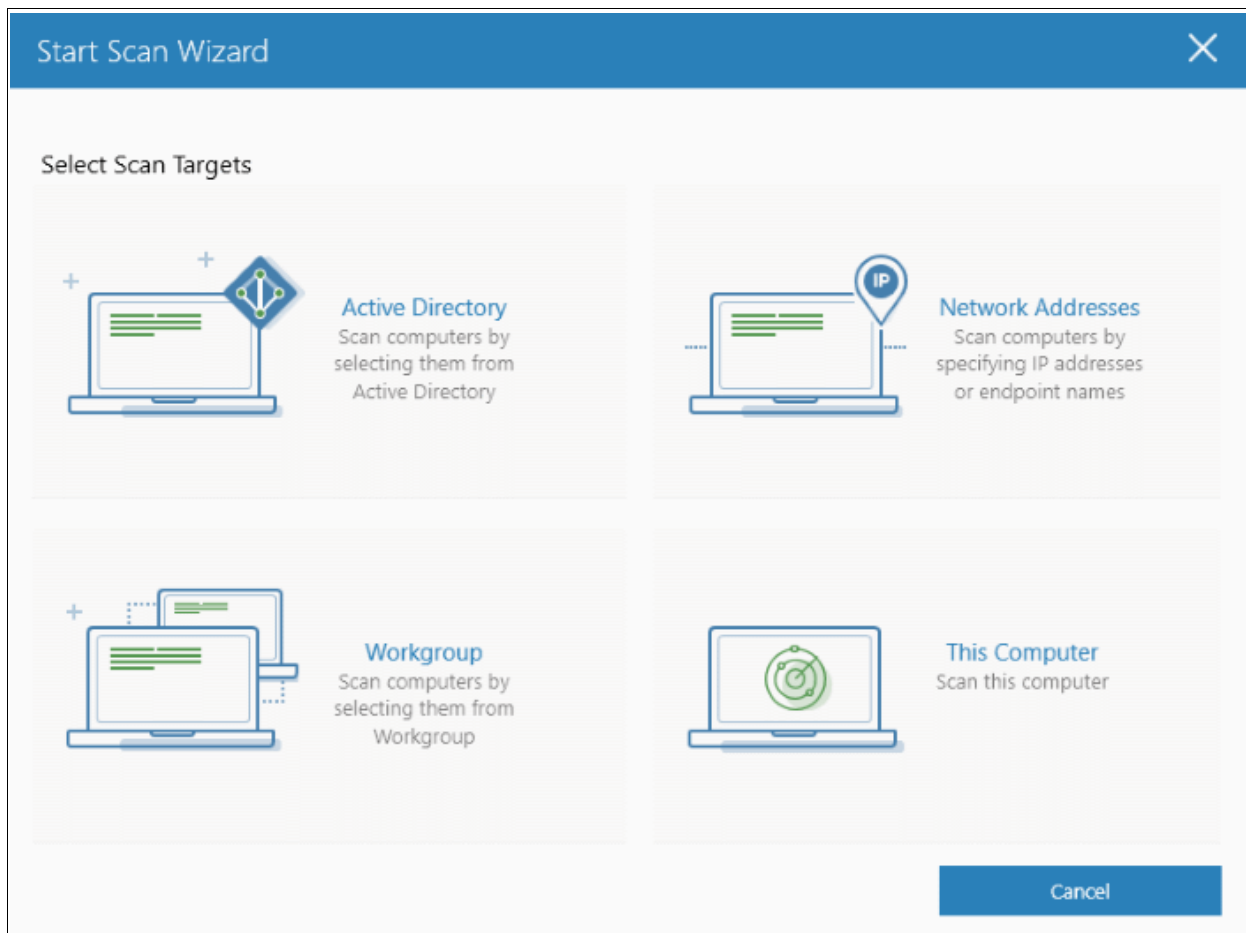
3.4 Scanning Local Computer

Comodo UFH allows you to scan your local device for unknown files. You can scan your device with a quick scan, full scan or custom scan.

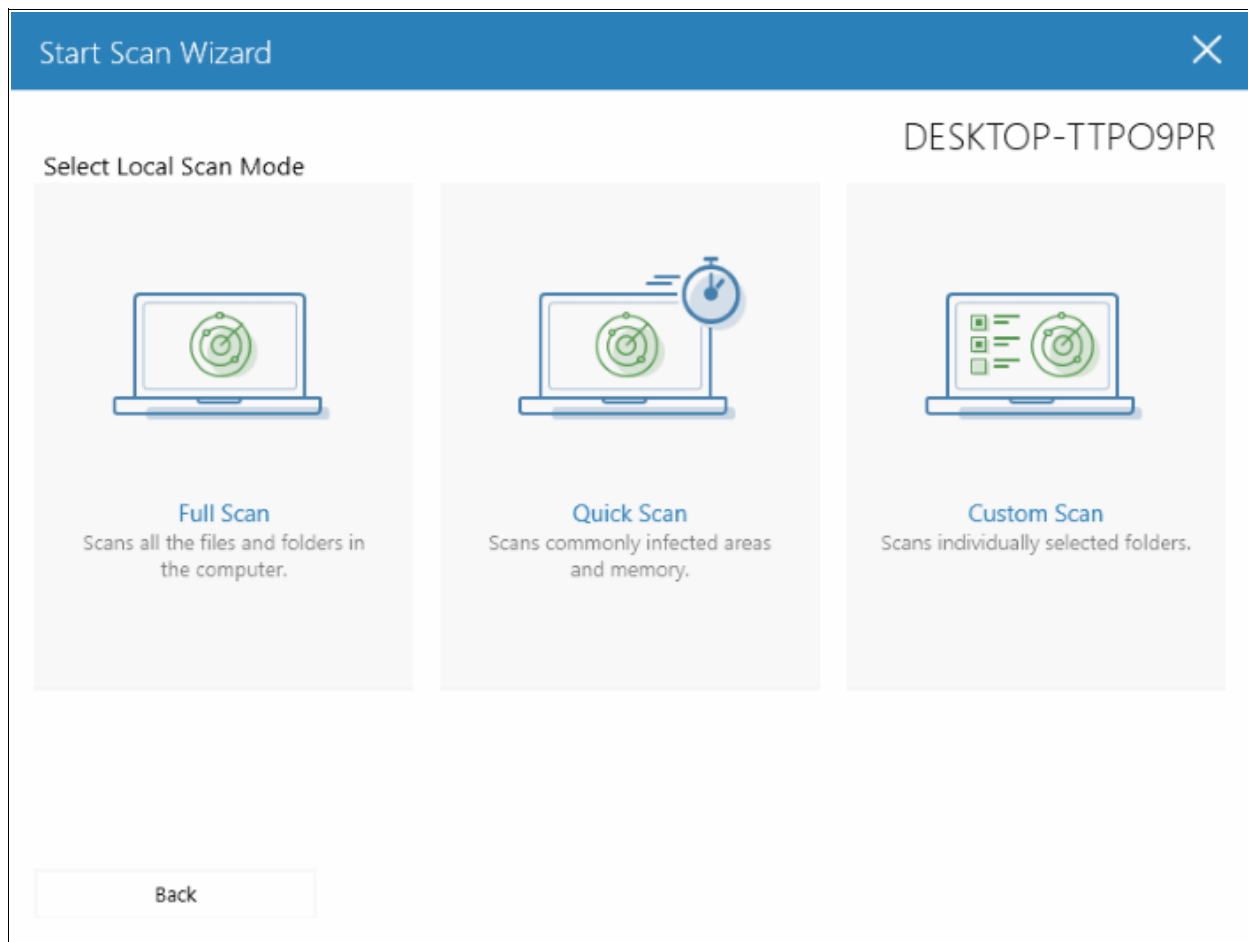


To open the 'Start Scan Wizard', click the 'Start Scan' button at the top-left or the 'Scan Now!' link in the main display area.

- Click 'This Computer'

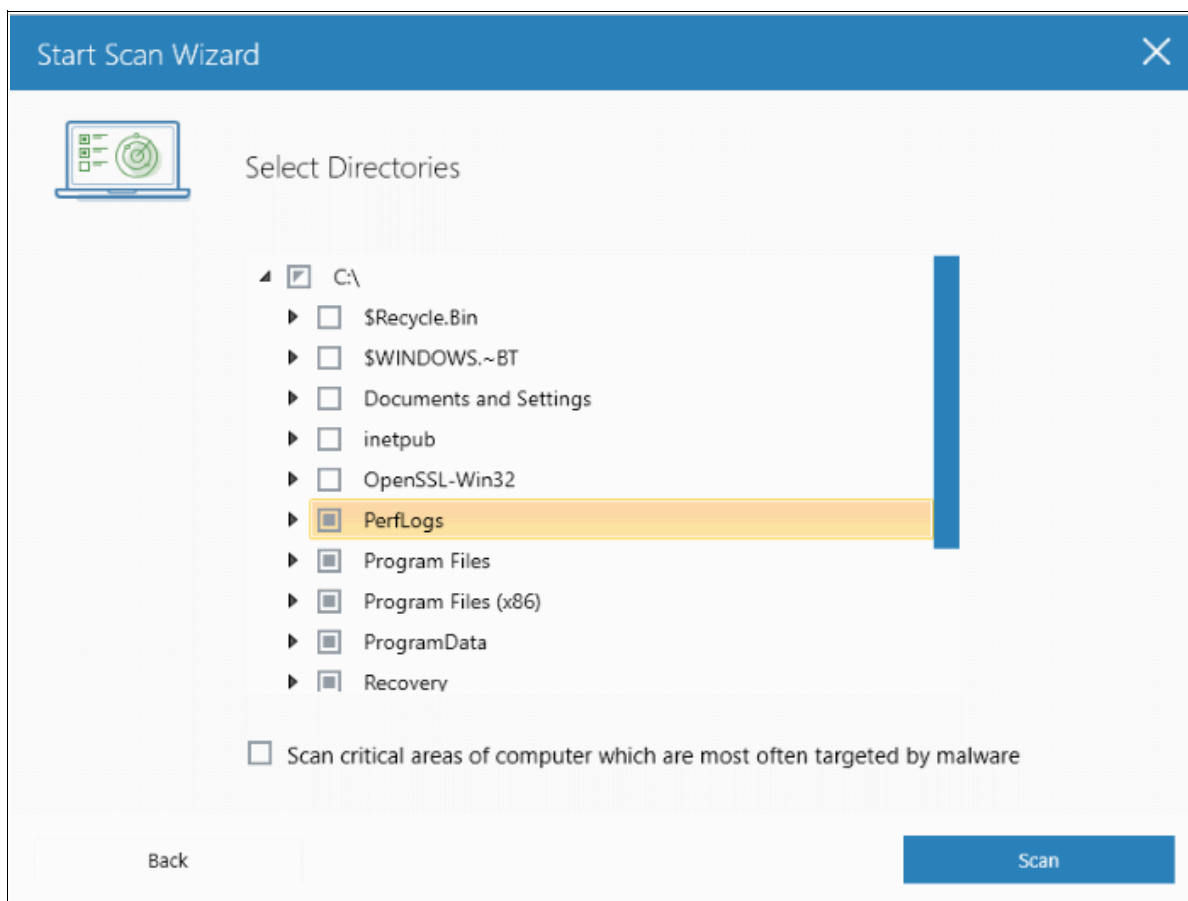


The three scan types will open.

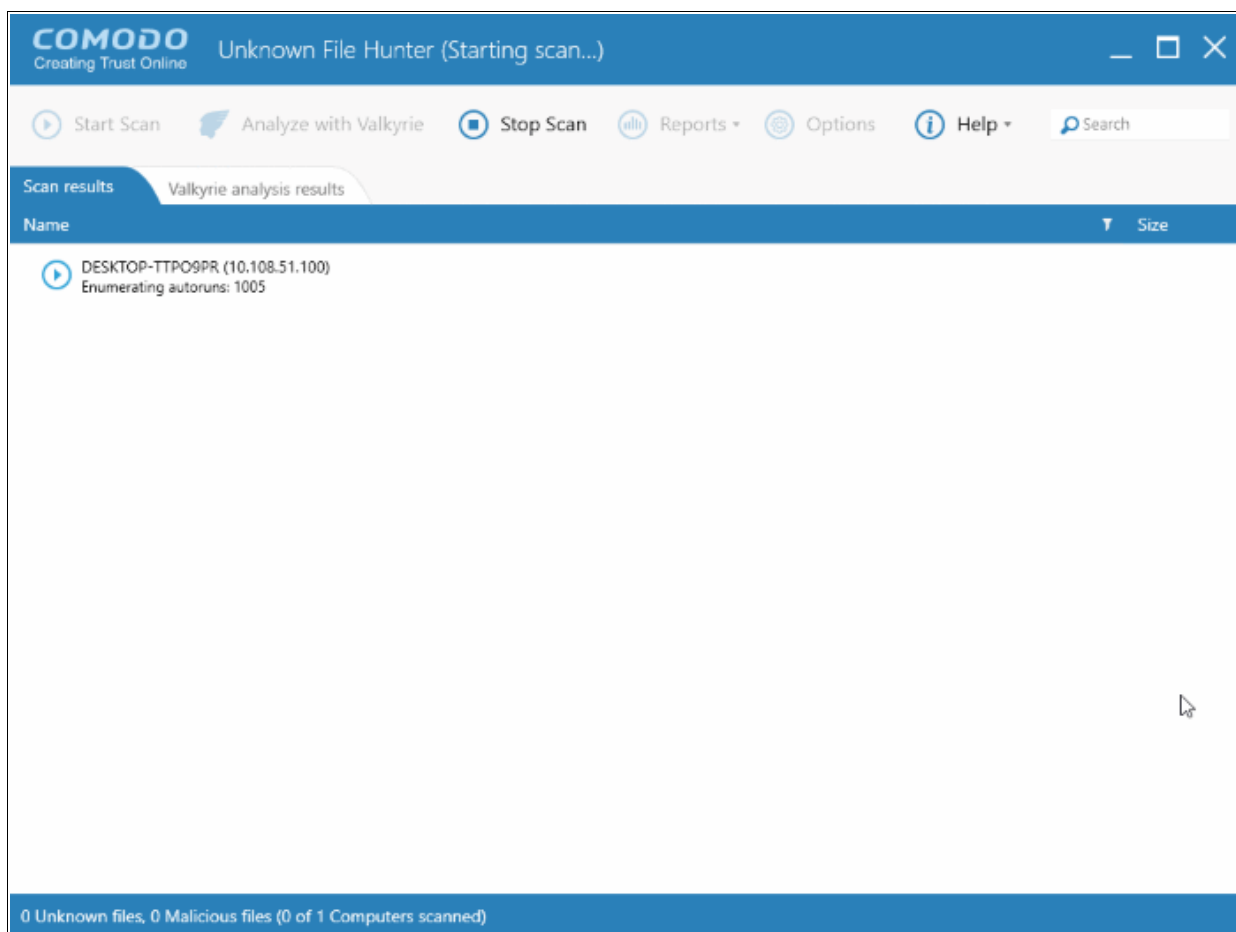


-
- Select the endpoints that you want to scan and choose one of the following scan types:
 - Quick Scan:** Scans critical and commonly infected areas of target endpoints
 - Full Scan:** Scans all files and folders on target endpoints.
 - Custom Scan:** Scans selected files or folders.

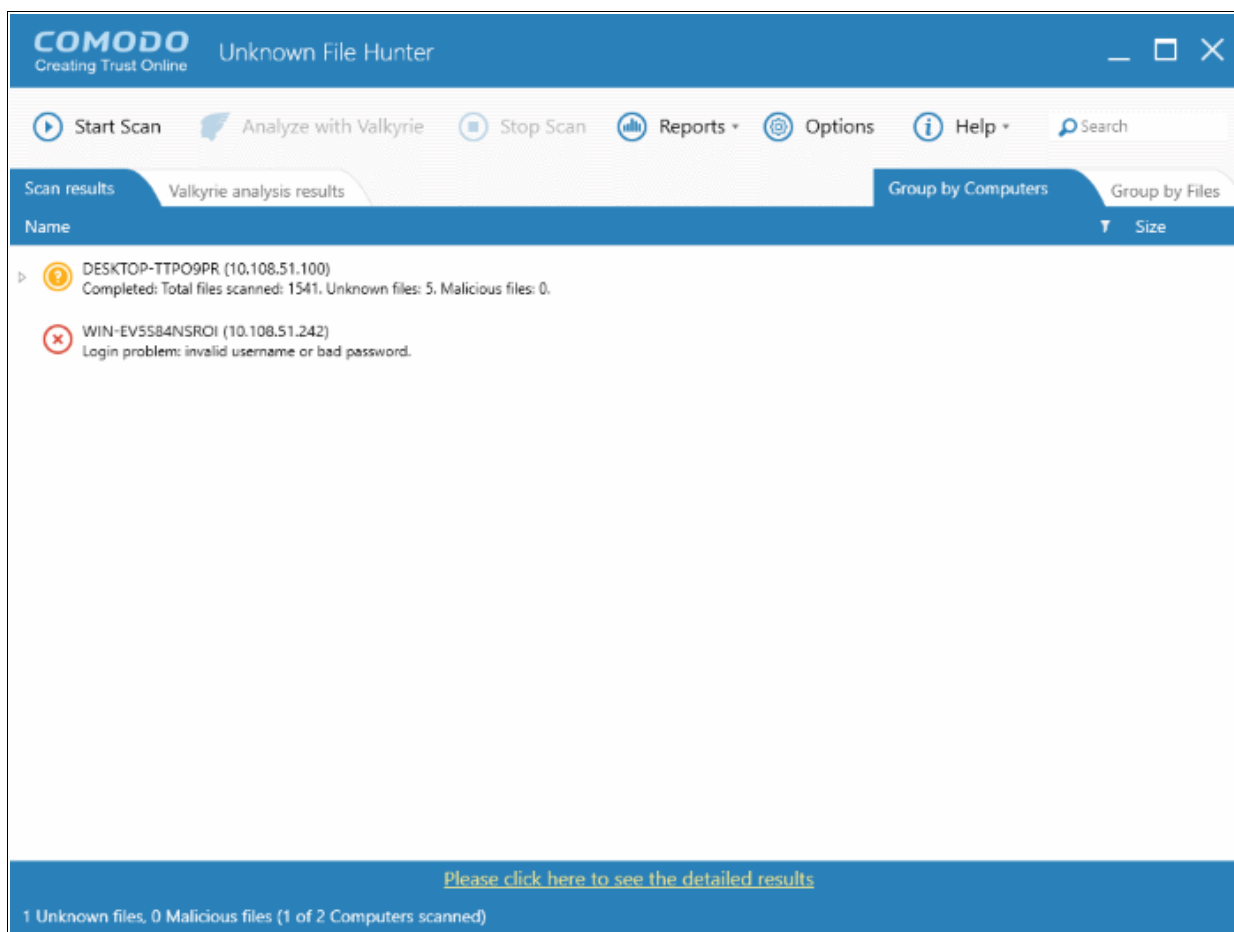
If you choose the 'Quick' or 'Full Scan' options then the scan will begin immediately. If you select 'Custom Scan', then you should next choose the directories and files you wish to scan in the 'Select Directories' screen:



- 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 scanning of endpoint(s) will start.
- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.
- The notification bar at the bottom displays the number of unknown and malware programs detected, the number of endpoints scanned, the accessibility to the computers, scan progress and more. Full results will be displayed after the scan finishes. You will also be given the opportunity to analyze unknown files with Valkyrie.



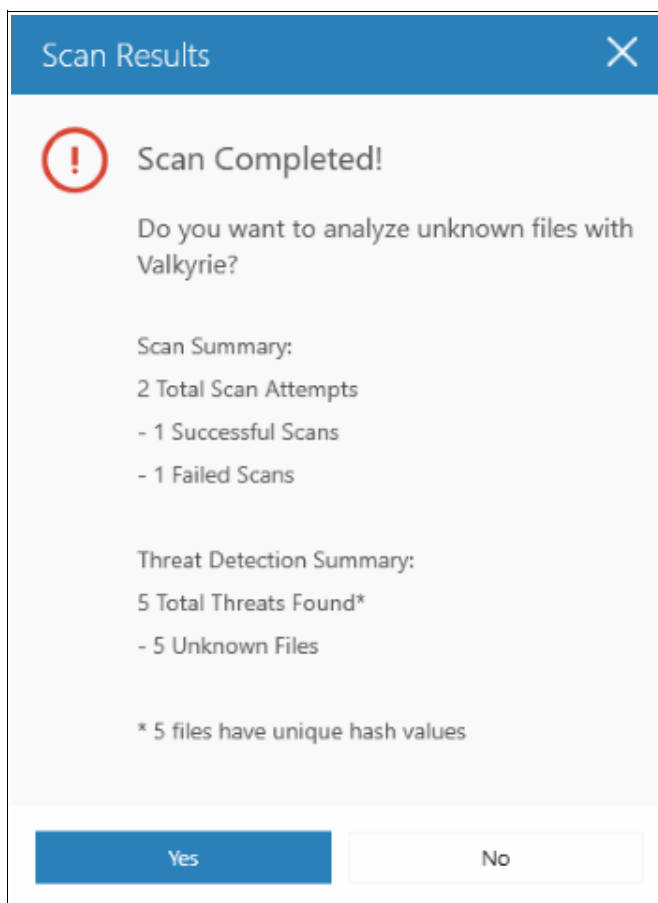
The details of results will be displayed in the respective endpoint rows, providing information such as the total number of programs scanned, number of unknown files, number of malware found and number of files that are failed to analyzed. There are results will be displayed in two ways:

For each endpoint that was successfully scanned, you'll see total number of files scanned and the number of unknown and malware files found. Results can be viewed in two ways:

Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

Group by File: Shows the name and quantity of each unknown file.

The option to analyze the results with Valkyrie will also be displayed:



Existing 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.

The screenshot displays the Comodo Unknown File Hunter web interface. The top navigation bar includes buttons for 'Start Scan', 'Analyze with Valkyrie', 'Stop Scan', 'Reports', 'Options', and 'Help', along with a search field. Below the navigation, there are tabs for 'Scan results' and 'Valkyrie analysis results'. The main content area shows a table of analysis results with columns for Name, Size, Verdict, and Trusted Vendor. The table lists five files: libcef.dll (62 MB, Not Analyzed), swscale-4.dll (647 KB, Clean), avfilter-6.dll (2 MB, Clean), winunivappfeatures.dll (97 KB, No Threat Found), and avformat-57.dll (2 MB, Clean). A footer bar contains a link to view detailed results and a summary: '1 Unknown files, 0 Malicious files (1 of 2 Computers scanned)'.

Name	Size	Verdict	Trusted Vendor
libcef.dll (Chromium Embedded Framework (CEF) Dynamic Link Library) 1 instance.	62 MB	Not Analyzed (Exceed size li...	No
swscale-4.dll 1 instance.	647 KB	Clean	No
avfilter-6.dll 1 instance.	2 MB	Clean	No
winunivappfeatures.dll (winunivappfeatures) 1 instance.	97 KB	No Threat Found	No
avformat-57.dll 1 instance.	2 MB	Clean	No

Please click here to see the detailed results

1 Unknown files, 0 Malicious files (1 of 2 Computers scanned)

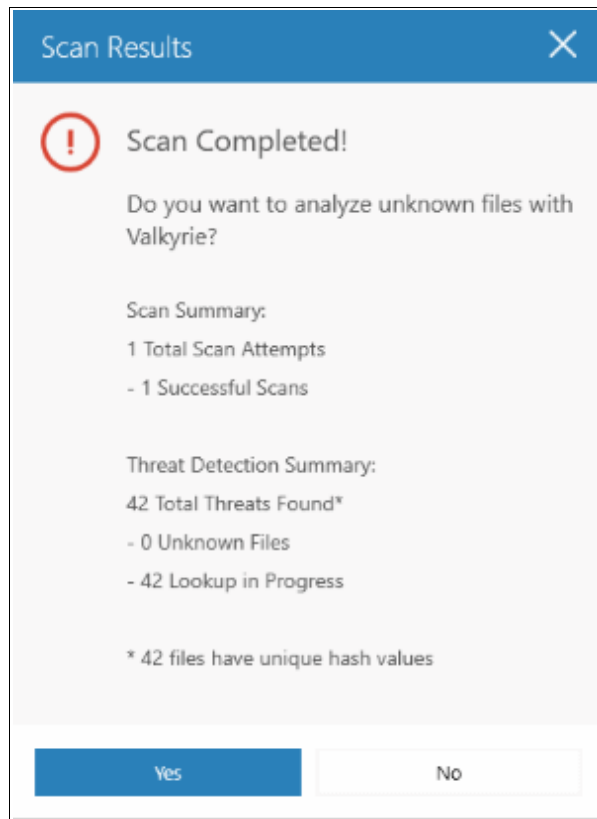
You can also find your license key by logging in at <https://accounts.comodo.com/> and visiting <https://accounts.comodo.com/valkyrie/management>

3.5 Analyzing Files with Valkyrie

Valkyrie is a cloud based file analysis system that is completely different from the conventional signature based malware detection technique. The uploaded files are analyzed dynamically and statically. The dynamic process includes the run-time behavior and static process includes analyzing the file's binary properties extracted from it such as its sections, entropy, packer type and many more. Any deviation from the expected values in these features provides the clue about the nature of the file.

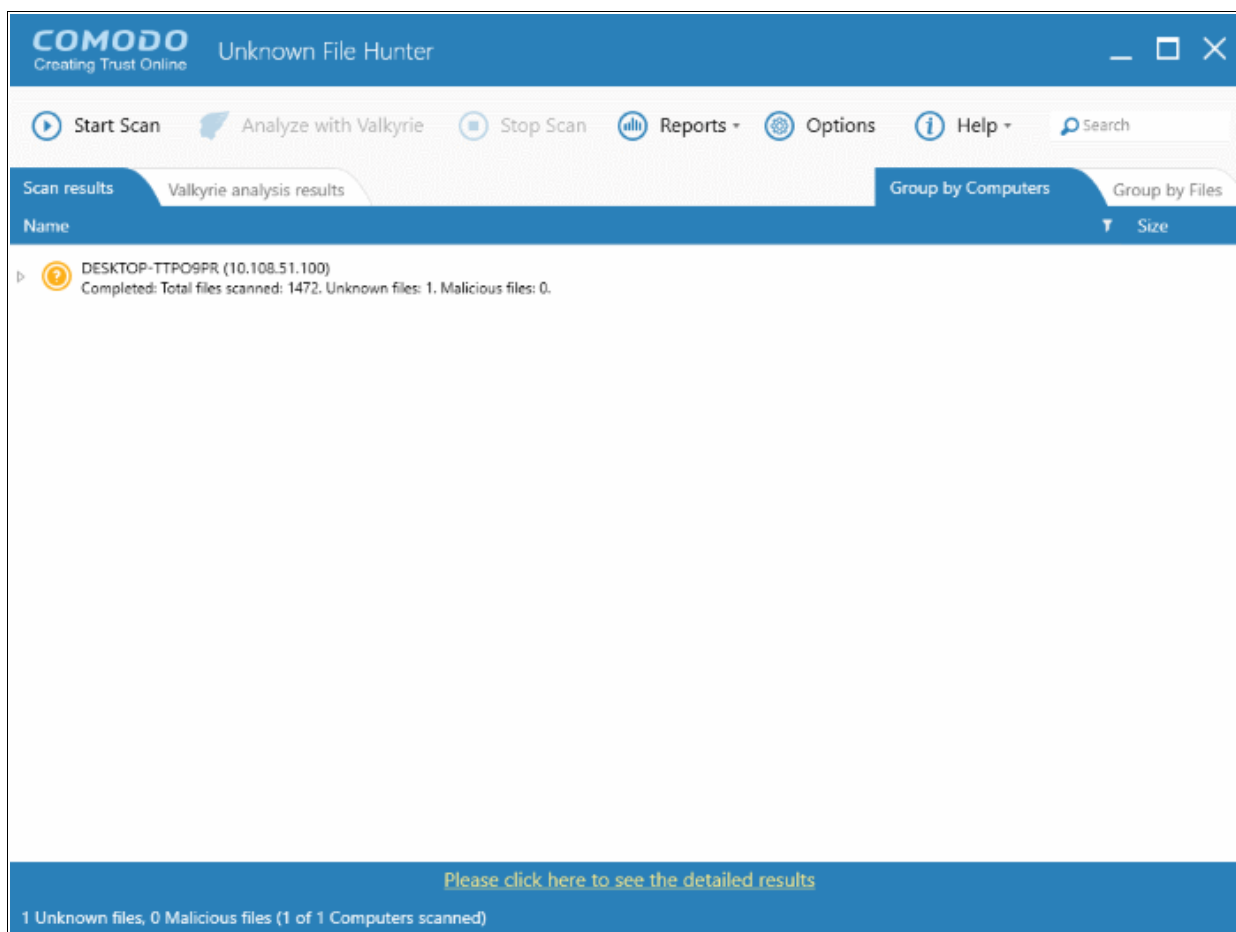
The UFH uses the Comodo's file look up service to identify files with its huge database of blacklisted and whitelisted files. If the files analyzed by the UFH tool is not available in either of these blacklist or whitelist, then they are categorized as 'Unknowns'. The administrator then has the option to submit the UFH tool detected unknown files with Valkyrie for an in-depth analysis including run-time behavior of the submitted files.

To submit the UFH tool detected unknown files with Valkyrie for analysis, click 'Yes' in the 'Scan Completed! Do you want to analyze files Valkyrie?'. This dialog appears after a scan is completed and displays the details of the scan including the number of malware and unknown files detected.



The detected files will be submitted to Valkyrie for an in-depth analysis and the progress will be displayed. The main interface will now have two tabs - one showing the results of UFH tool analysis and the the other for Valkyrie.

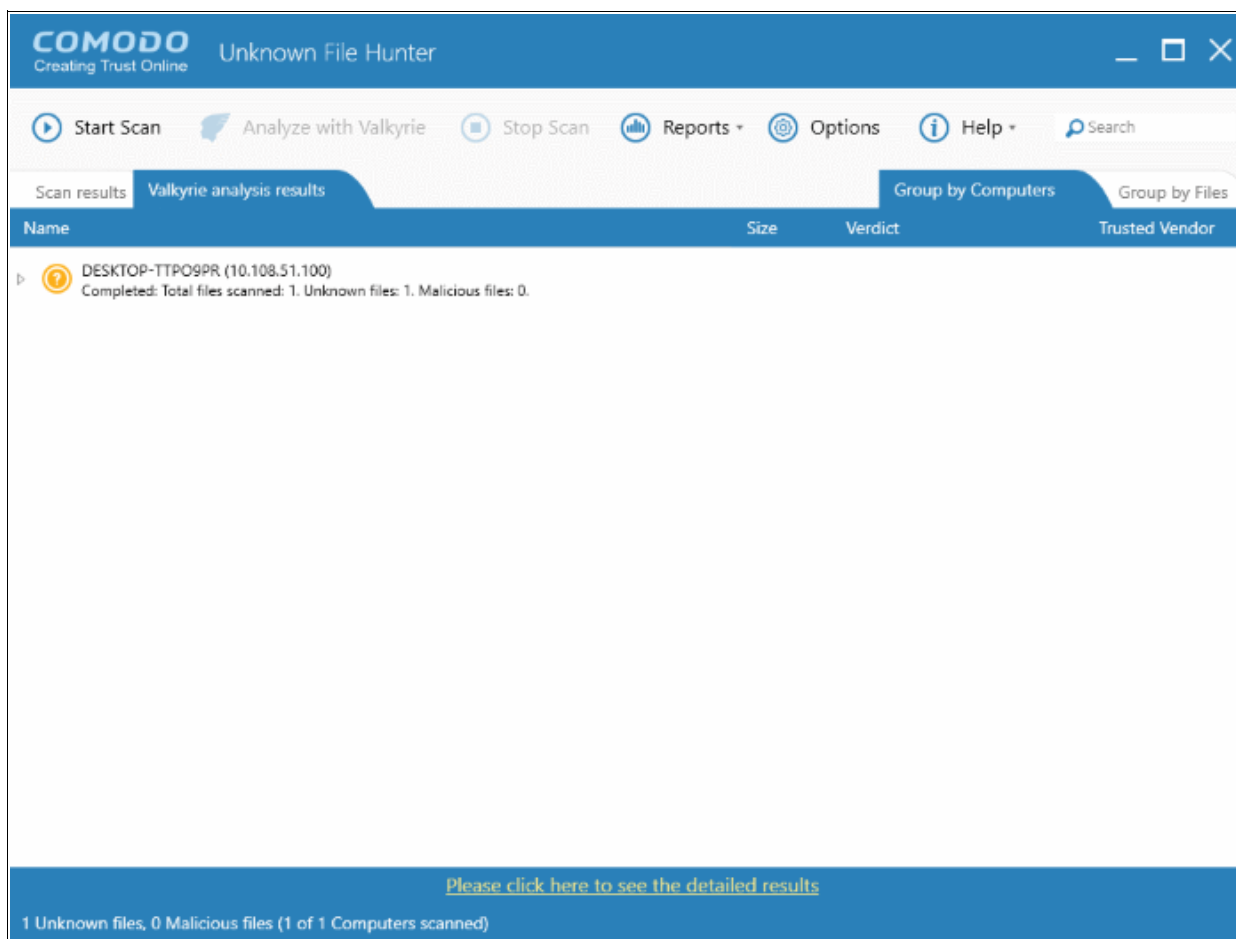
After the analysis is completed the results are displayed under the 'Valkyrie analysis results' tab.



Both results can be displayed in two ways:

Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

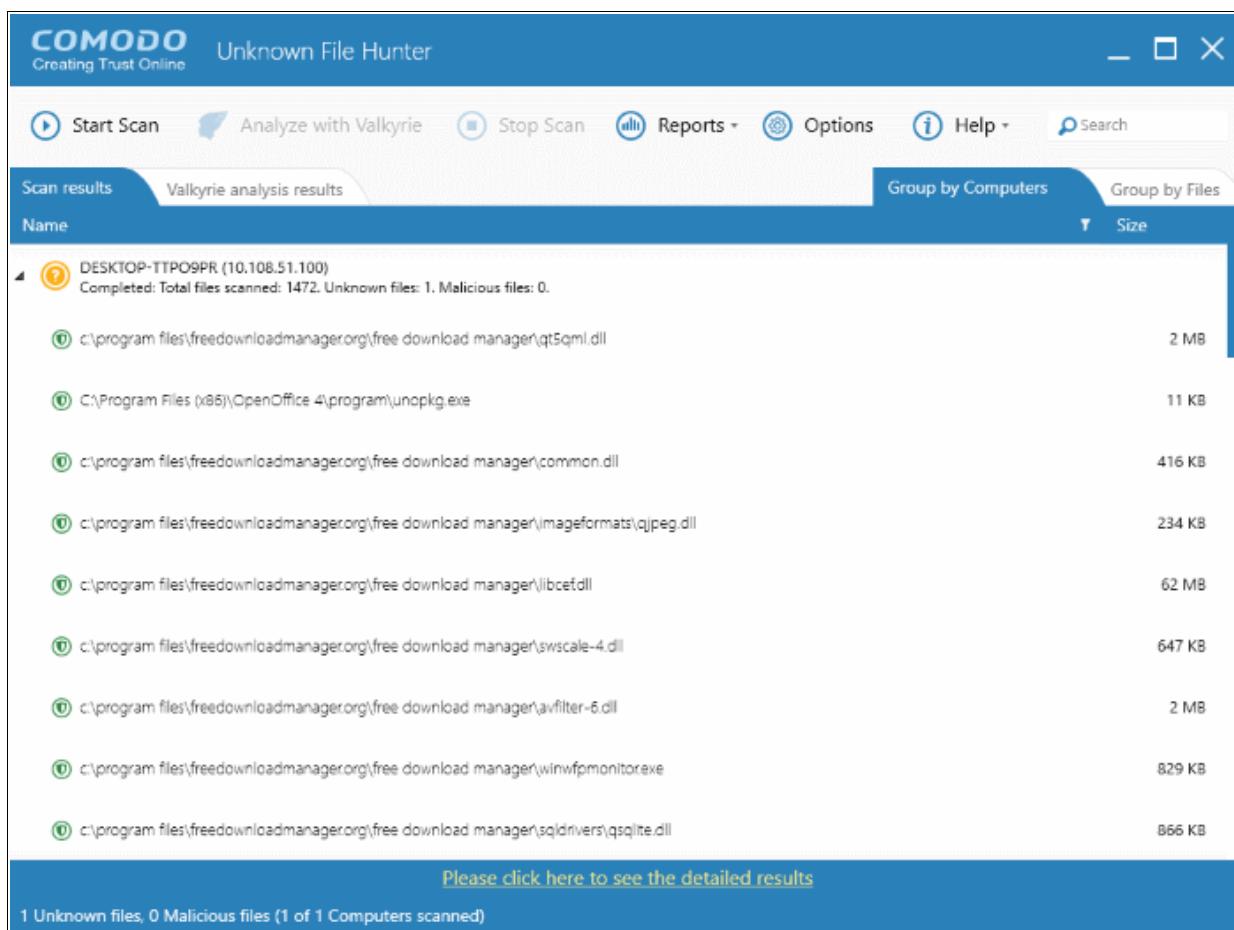
Group by File: Shows the name and quantity of each unknown file.



The results displays the details such as the name of the file, its size, the scanning verdict and more. Refer to the section '**Valkyrie Analysis Results**' for more details.

4 Scan Results

After the scanning process is completed, the results will be displayed in the main interface. The unknown files detected by the UFH tool are displayed under the 'Scanning results' tab. If the files are submitted to Valkyrie, then its results will be displayed under the 'Valkyrie analysis results' tab.



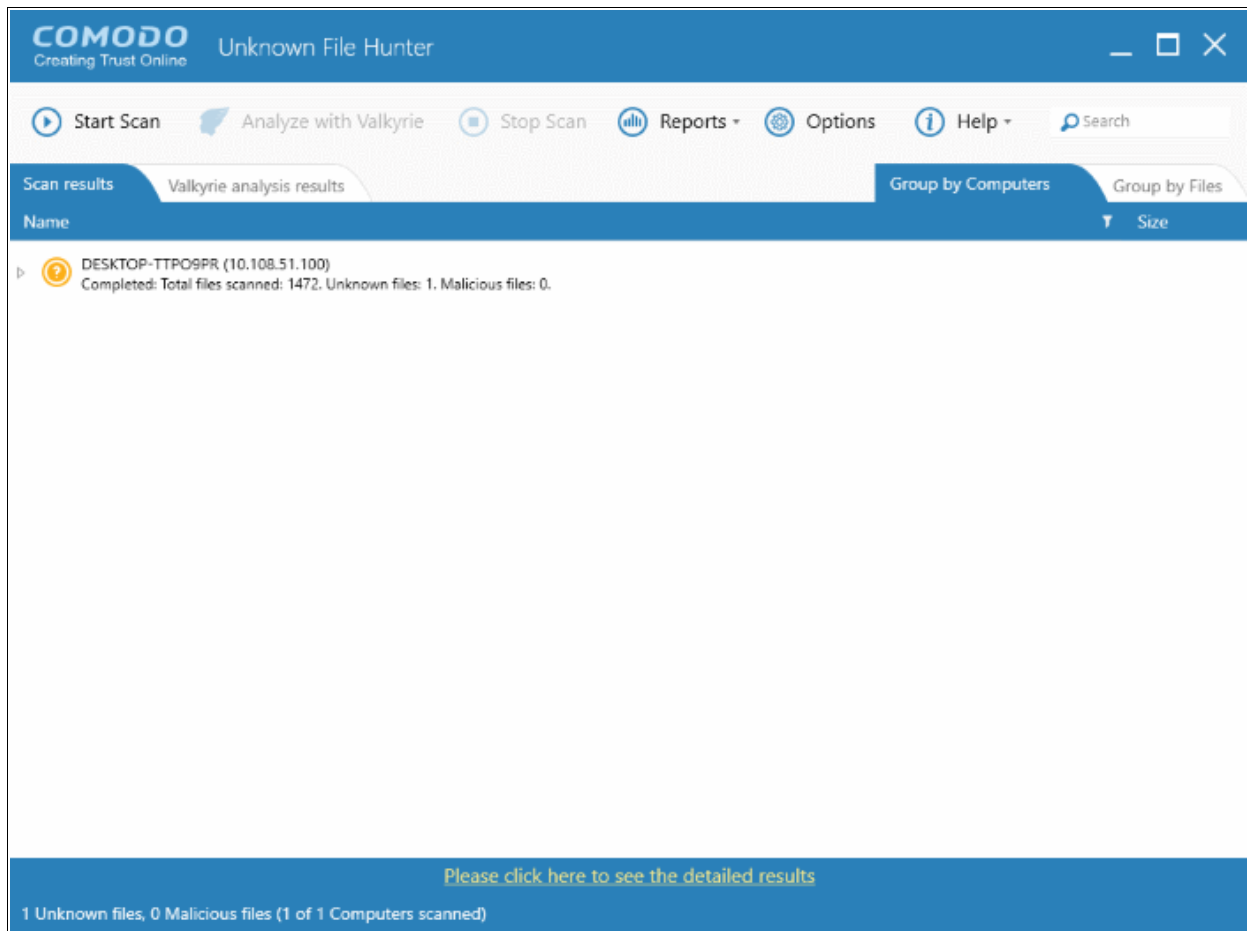
Refer to the following sections for more details:

- [Comodo Unknown File Hunter Scan Results](#)
- [Valkyrie Analysis Results](#)

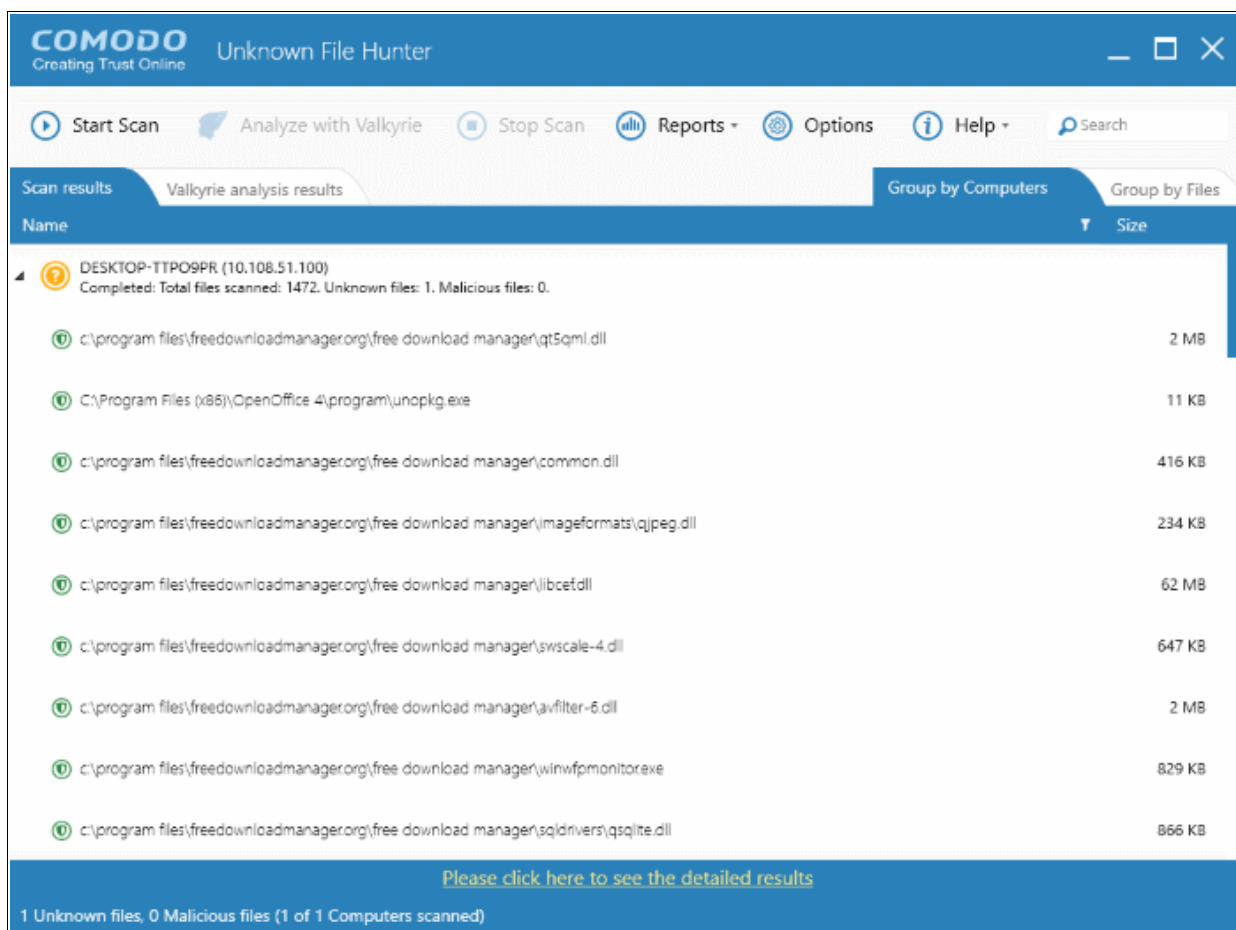
4.1 Comodo Unknown File Hunter Scan Results

The results of the Comodo UFH tool scan will be displayed in the 'Scanning results' tab in the main display area. The scan results are provided for each computer that the UFH tool has scanned including the name of the computer and the name of the detected files in them.

To view the UFH tool scan results, click the 'Scanning files' tab



- Click on the arrow beside each endpoint to expand and view the details of detected files in it such as the location, its name and so on.

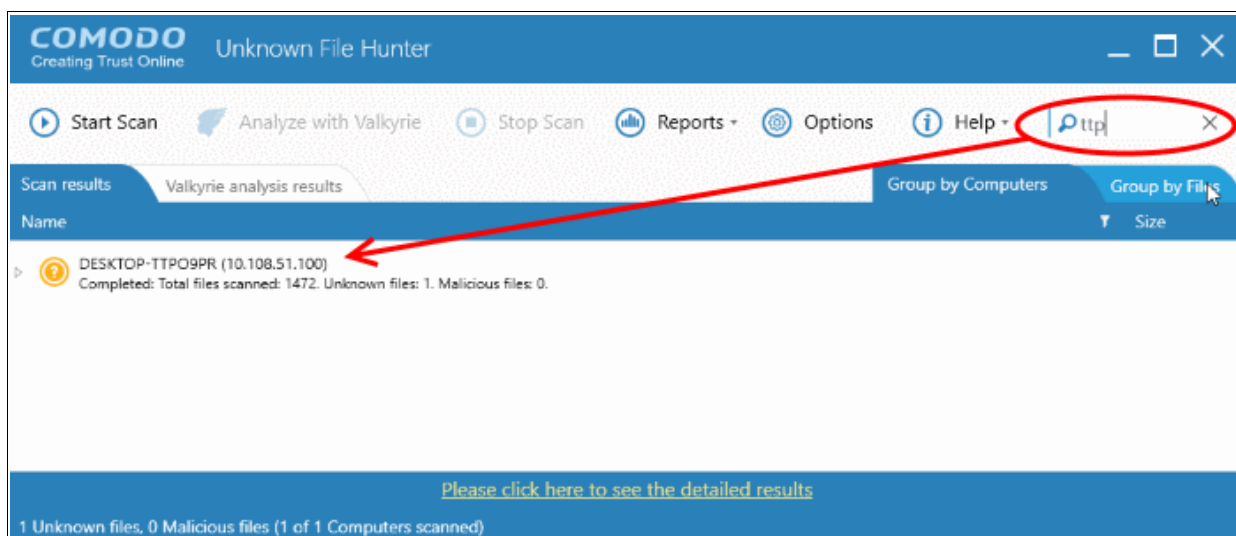


Searching, sorting and filtering Options

Searching Option

- To search for a particular endpoint, enter its name or IP address partially or fully in the 'Search' box at the top right

The items that match the search criteria will be displayed.



- To display all the endpoints again, clear the search box.

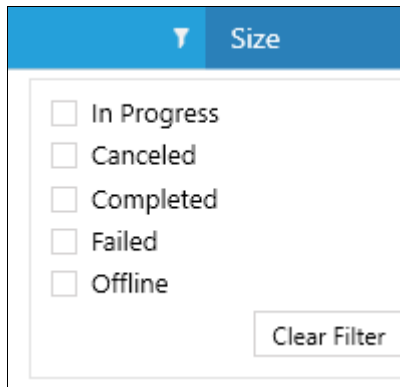
Sorting Option


- Click on the 'Name' column header to sort the endpoints in ascending/descending order

- To sort the files in ascending/descending order according to its name and size, expand the endpoints to display the detected files and click on the 'Name' and 'Size' column headers

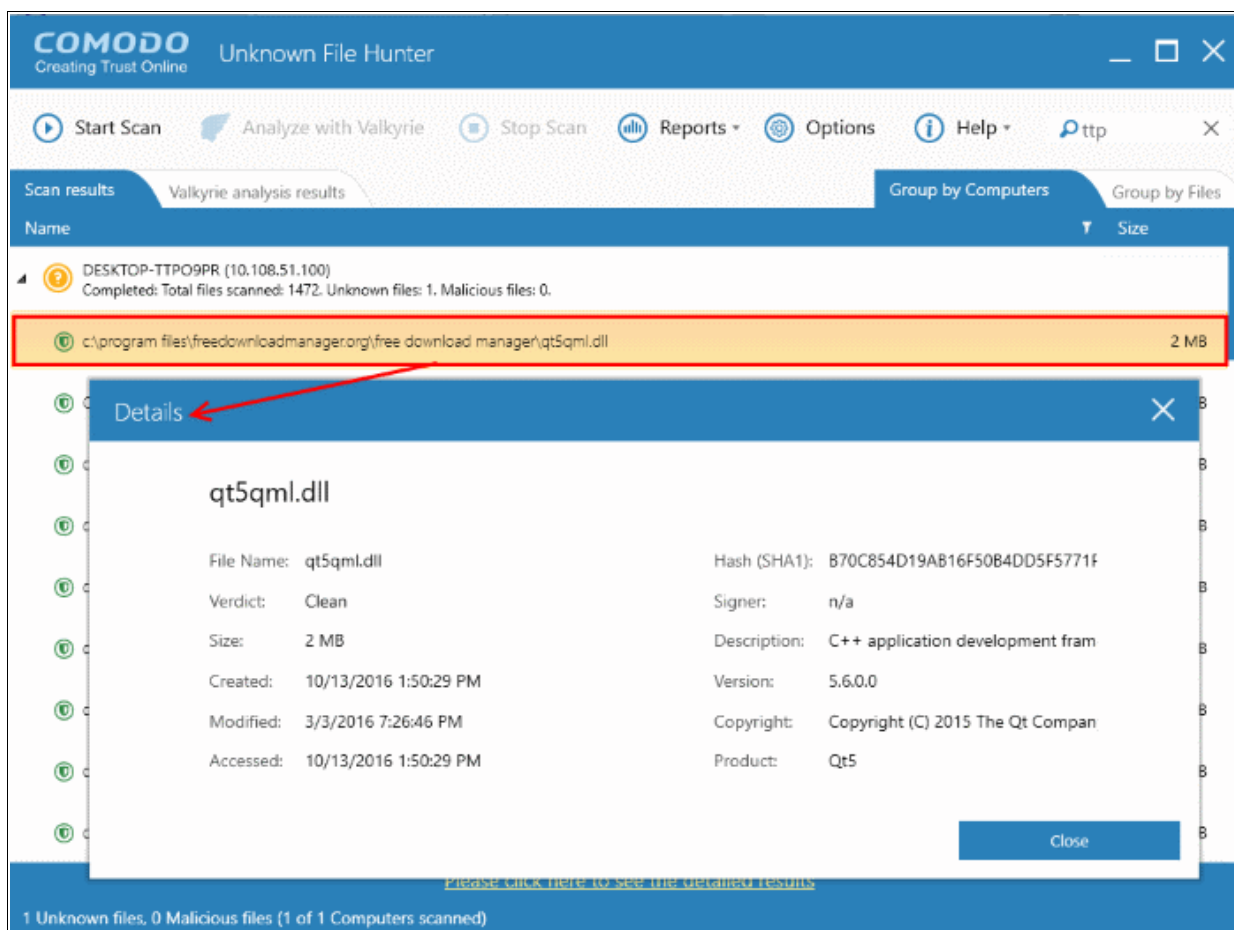
Filtering Option

- Click the funnel icon  at the end of 'Name' column



- Select the filter criteria from the options
 - In Progress - Displays the endpoints in which the scanning is in progress
 - Canceled - Displays the endpoints for which the scanning was canceled
 - Completed - Displays the endpoints for which the scanning was completed
 - Failed - Displays the endpoints for which the scanning failed
 - Offline - Displays the endpoints that have gone offline during the scanning process
- If the filter icon is in blue color , it indicates filter(s) are applied
- To display all the endpoints again, click 'Clear Filter'

To view the details of file, double click on the file from the list.



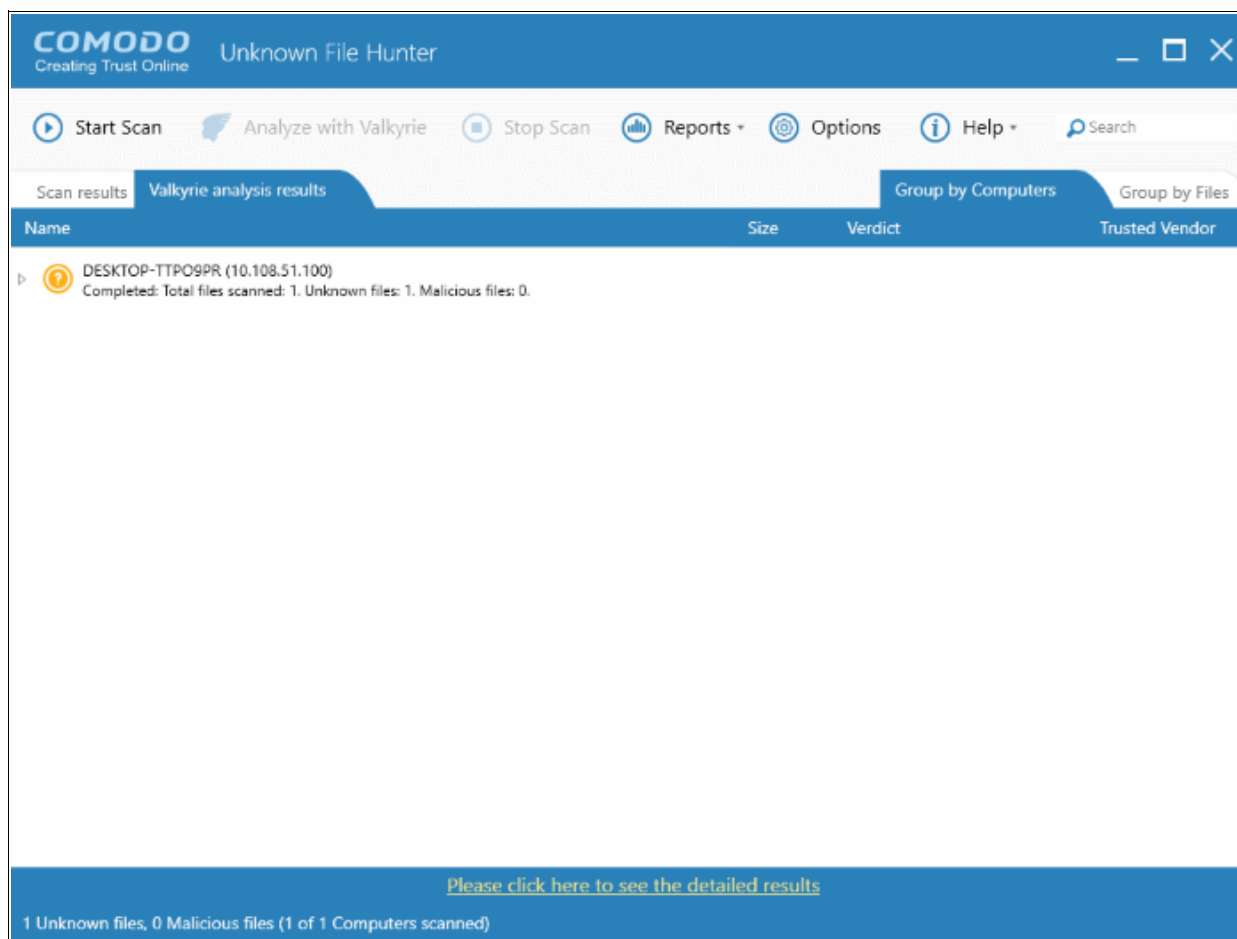
The details of the file include SHA1 hash value, file name, its size, version no and so on.

- Click the 'Close' button to return to the scan results screen.

4.2 Valkyrie Analysis Results

The 'Valkyrie analysis results' tab will be available only if the administrator has opted to submit unknown files to Valkyrie for in-depth analysis. Refer to the sections '**Scanning Computers**' and '**Analyzing Files with Valkyrie**' for more details about scanning endpoints and about Valkyrie.

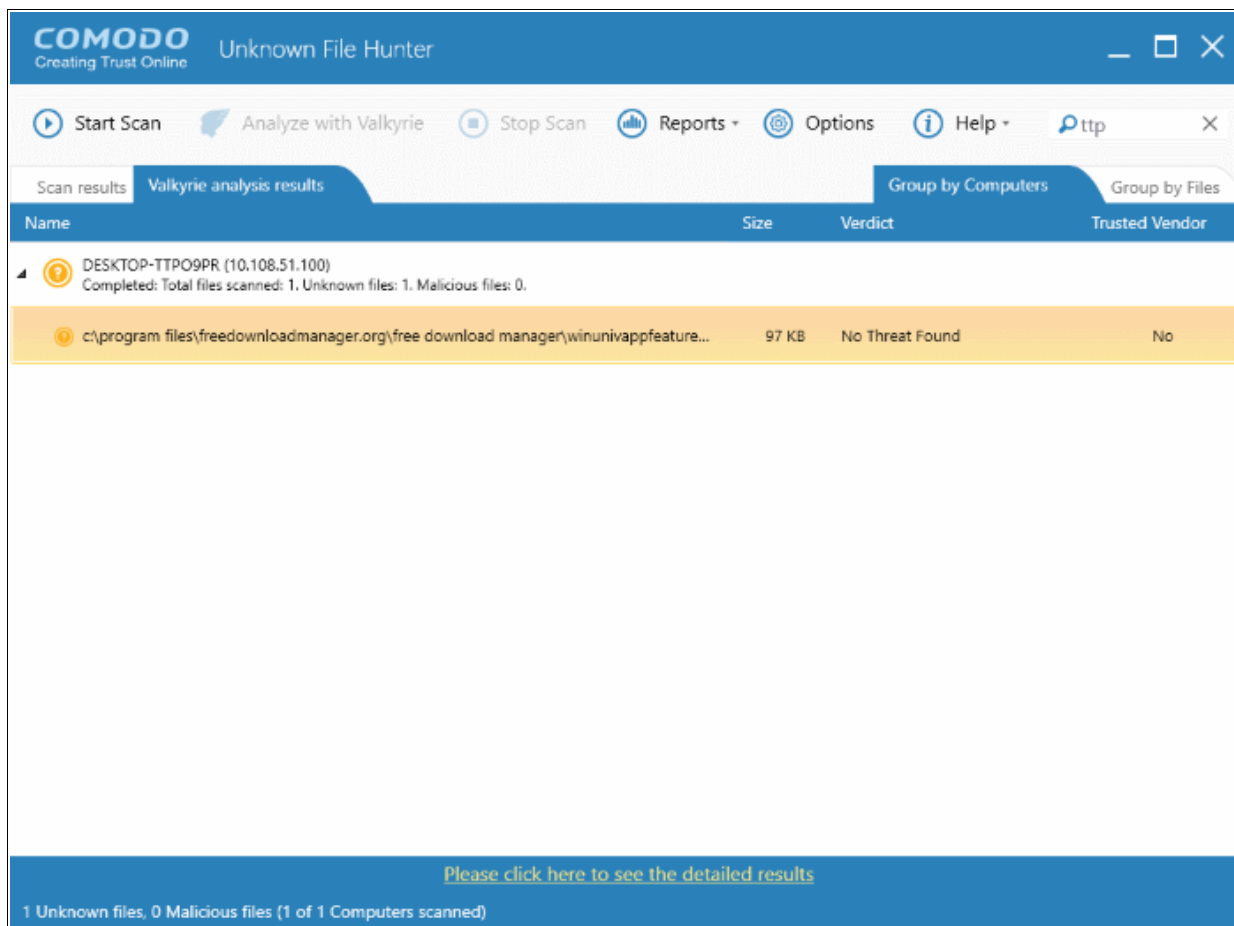
To view the Valkyrie scan results, click the 'Valkyrie analysis results' tab.




Sorting option

- Click on a column header to sort the results in ascending/descending order

The details of computer(s) that is affected by a file and its location can be viewed by clicking the arrow beside each file.



Valkyrie Analysis Results - Table of Column Descriptions

Column Header	Description
Name	The name of the file. The icon  beside a file indicates a malware file.
Size	The size of the analyzed file
Verdict	The result of Valkyrie analysis of a file. Indicates if the file is a malware or safe.
Status	The file has been successfully analyzed by Valkyrie
White Listed	Indicates whether the file has been whitelisted after the manual review . Even if a program is marked as whitelisted, it will be detected again during the next scan but shown as whitelisted.

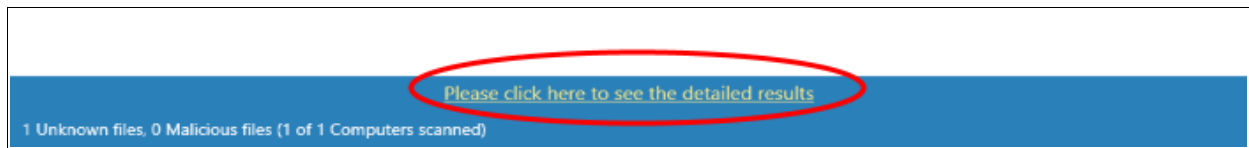
The bottom of the Valkyrie results page shows a short summary of the unknown programs and malware discovered by the scan. It also shows the number of computers scanned.

The 'Valkyrie' website at <https://valkyrie.comodo.com> provides detailed results for the scans that are run and includes the following options:

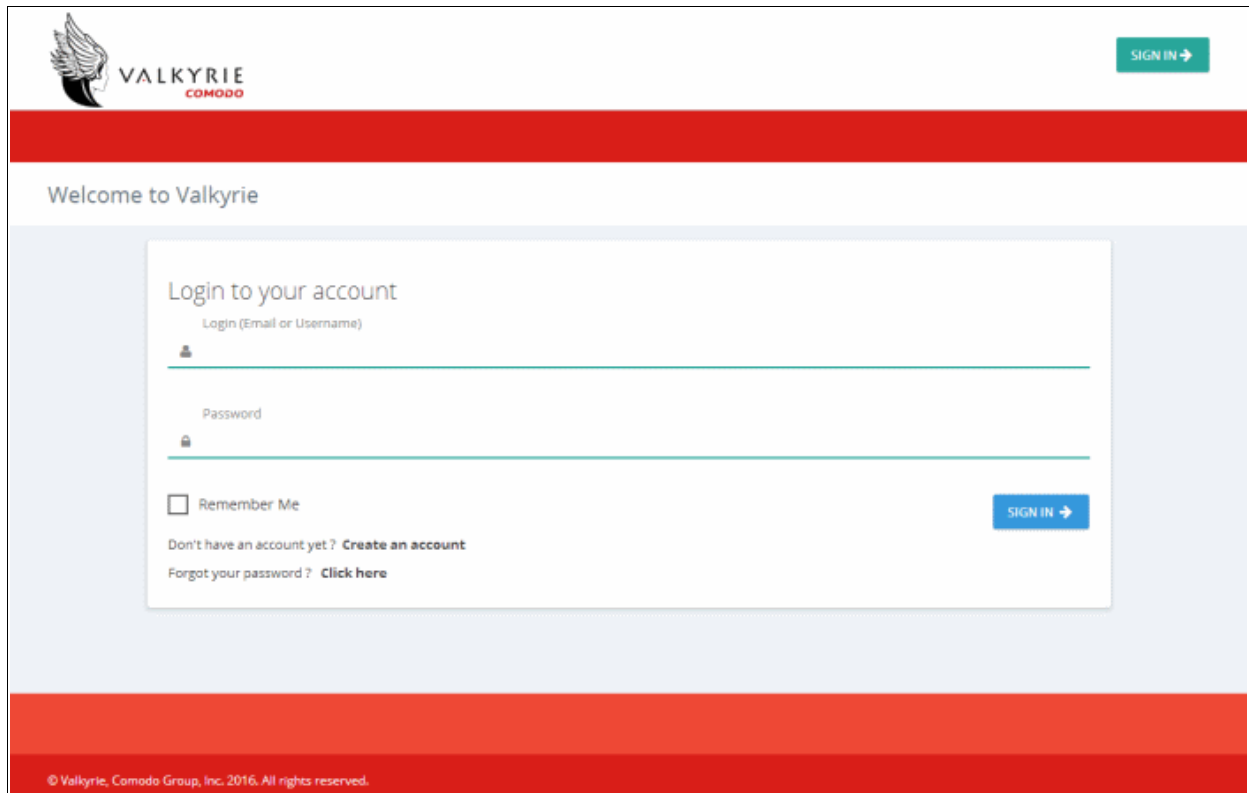
- Submit the files for manual analysis
- View detailed information about each file
- Download the result for each in PDF format
- View detailed information about each detected file from VirusTotal.com website

To view the detailed results, click the 'Please click here to see the detailed results' link at the bottom of the results

interface.

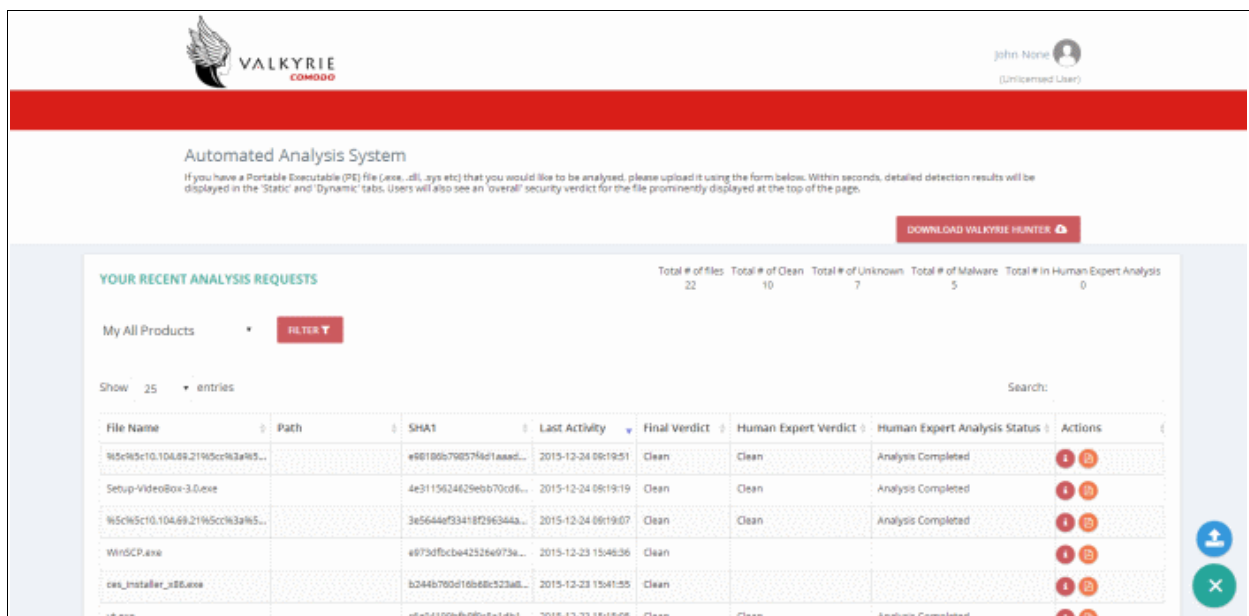


You will be navigated to the Valkyrie website login page at <https://valkyrie.comodo.com>

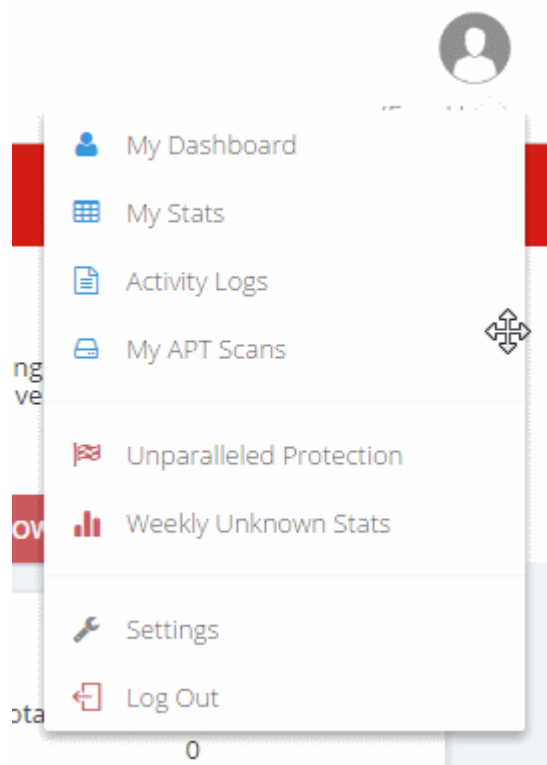


- If you do not have an account, click the 'Create an account' link, provide the required details and sign up for an account, which is free.
- If you already have a Valkyrie account, enter the credentials and click the 'Sign In' button.

The 'Dashboard' page will be displayed by default.



You can navigate to different pages of the website by clicking your account name on the top right side of the page.



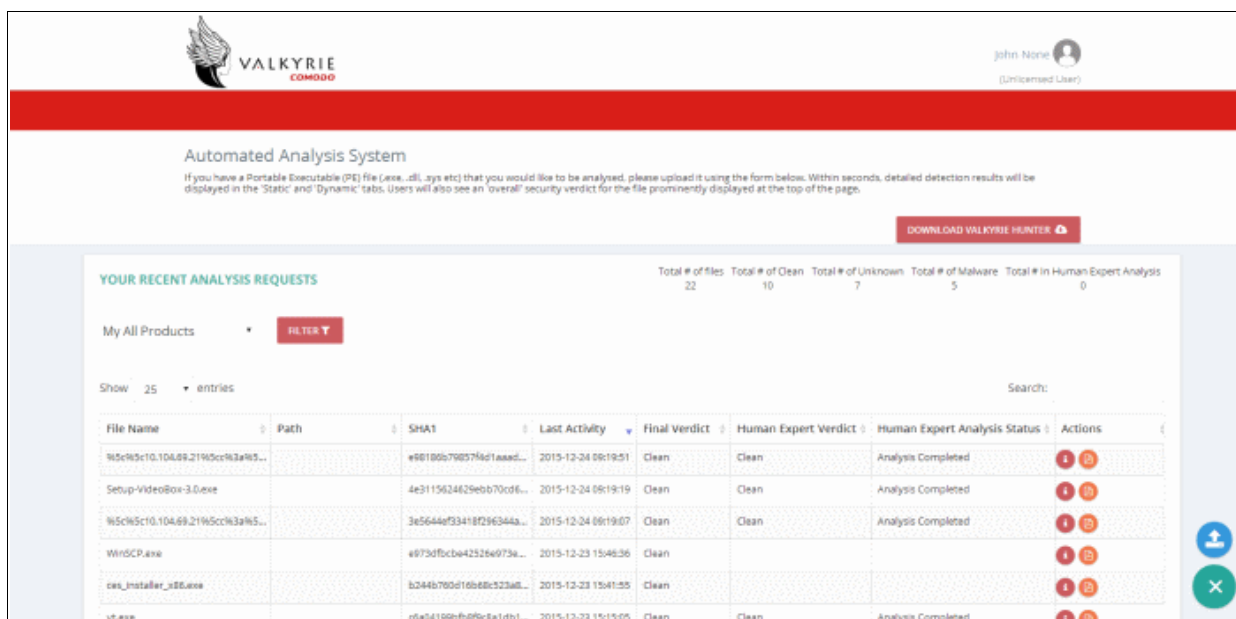
- **My Dashboard** - Provides details of each file that was submitted to Valkyrie for analysis, including its SHA1 signature, submitted date and more. Refer to the section '**Dashboard**' for more details.
- **My Stats** - Provides the summary of files analyzed by Valkyrie for your account. Refer to the section '**Valkyrie Usage Statistics**' for more details.
- **Activity Logs** - Provides the Valkyrie account usage details such as date and time of login, the source IP of the computer used to login and more. Refer to the section '**Activity Logs**' for more details.
- **My APT Scans** - The scan start and end date, number of files scanned, queried files, uploaded files, cleaned files and malware files and the actions that can be performed for each scan information.
- **Unparalleled Protection** – Provides statistics with monthly details of total number of malware files that were not detected by previous vendor and AV industry.
- **Weekly Unknown Stats** – Provides graphical representation of Malware and unknown files.
- **Settings** - This option displays the details of the user and portal.
- **Log Out** - Allows you to log out of your account.

Dashboard

The 'Dashboard' page of Valkyrie displays the details of analysis for the files submitted. From this page, you can view the download auto analysis report, view details of static analysis, view details of dynamic analysis and more.

- Click 'My Dashboard'

The details of each analyzed file will be displayed in the table. The number of items to be displayed on each page can be selected from the 'Show entries' option on the left.



The summary of analysis requests and results are displayed at the top of the table.

Sort and search options





Sorting the entries

- You can sort the items in ascending/descending order by clicking on the column headers.

Searching for particular item(s)

- Enter the details partially or fully in the search field on the top right side. You can search for items based on all columns except the 'Actions' column.
- To display all the entries again, clear the search field.

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: <ul style="list-style-type: none"> Clean - The file is 99.9% 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: <ul style="list-style-type: none"> 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

<p>Human Expert Analysis Status</p>	<p>Indicates the status of files submitted for Human Expert analysis. The statuses are:</p> <ul style="list-style-type: none"> • 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.
<p>Actions</p>	<p>The available actions are:</p> <ul style="list-style-type: none">  - View Info - You can view the complete details of the results for the file such as summary, static analysis, dynamic analysis and file details. Refer to 'File Analysis Results' for more details.  - Download Automatic Analysis Report - Allows you to download the report in PDF format. Refer to 'Download Automatic Analysis Report' for more details.  - View Virus Total Result - Takes you to the Virus Total website that displays its results for the file. Refer to 'View Virus Total Results for the File' for more details.  - Send to Manual Analysis - Allows you to submit the file for manual analysis by Comodo technicians. Refer to 'Send the File for Manual Analysis' for more details.

File Analysis Results

- Click the 'View Info' icon  under the 'Actions' column for a file to view its detailed results

A new web page will open displaying the detailed results for the file.

- Click the 'Summary' tab

The screenshot shows the 'Summary' tab of the Valkyrie interface. At the top, the file name is 'agent.rv.watcher.service.exe' and the file type is 'PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows'. A 'Valkyrie Final Verdict' of 'CLEAN' is displayed with a green checkmark icon. Below this, the 'Analysis Summary' table provides a detailed overview of the analysis results.

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2015-09-17 20:56:10	No Match
Static Analysis Overall Verdict	2015-09-17 20:56:10	Highly Suspicious
Human Expert Analysis Overall Verdict	2015-09-17 20:56:10	Clean
File Certificate Validation	2016-04-04 17:36:33	Not Applicable

Summary - The top section shows file details such as name, file type, and more. At the top right, the 'Valkyrie Final Verdict' is displayed. The details under 'Analysis Summary' displays the summary of the file analysis such as signature based detected, static analysis overall verdict and dynamic overall verdict for the file.

- To view the detailed results of static analysis of the file, click the 'Static Analysis' tab

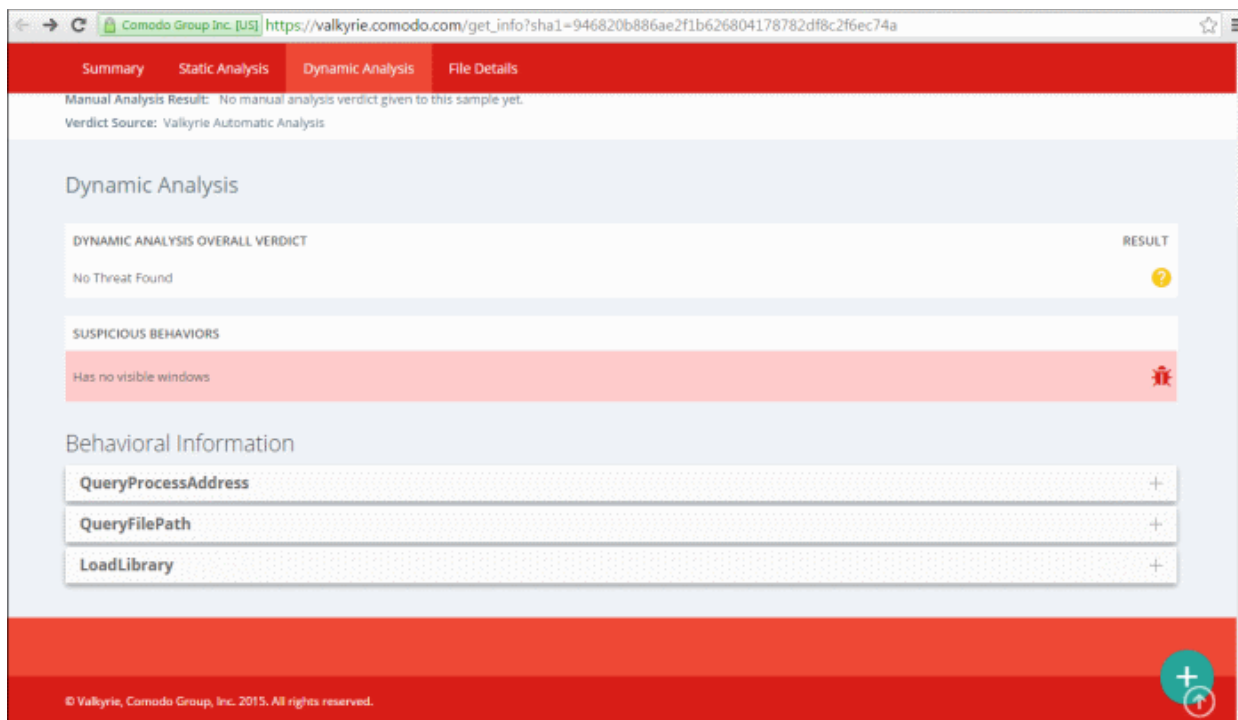
The screenshot shows the 'Static Analysis' tab of the Valkyrie interface. It displays the 'STATIC ANALYSIS OVERALL VERDICT' as 'Highly Suspicious' with a red bug icon. Below this, a table lists specific detectors and their results.

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional header	Clean

Static Analysis - Static process includes analyzing the file's binary properties extracted from it such as its sections, entropy, packer type and many more. Any deviation from the expected values in these features provides the clue about the nature of the file.

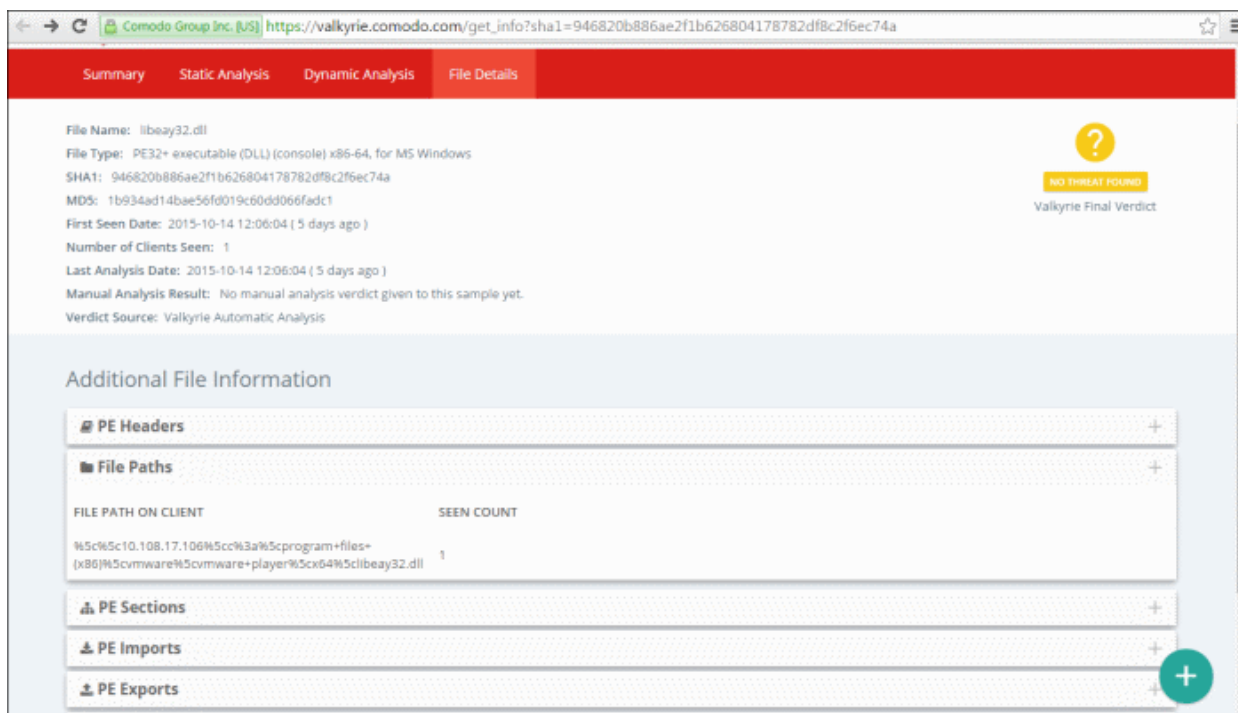
Scroll down the page to view static analysis overall verdict for the file as well as detailed result for each of the parameter checked for the file.

- To view the detailed results of dynamic analysis of the file, click the 'Dynamic Analysis' tab



Dynamic Analysis - The dynamic process includes the run-time behavior of the file in a test environment. The page provides the dynamic analysis overall verdict and behavioral information for the file. Scroll down the page to view the detailed behavioral information for the file.

- To view the more details about the file, click the 'File Details' tab





File Details - Provides additional file information such as the file path on the client machine, PE headers, PE sections and more. Scroll down the page to view the details file information.

Download Automatic Analysis Report

- Click the 'Download Automatic Analysis Report' icon  under the 'Actions' column for a file to download the report in PDF format

A new web page will open displaying the detailed results for the file.





File Name: agent.rv.watcherservice.exe
 File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
 SHA1: e98186b79857f4d1aaadc16a3c762ed5bd03b4cb
 MDS: be50979384a5161da0955772205fa12f
 First Seen Date: 2015-09-17 15:26:10 UTC
 Number of Clients Seen: 5
 Last Analysis Date: 2015-09-17 15:26:10 UTC
 Manual Analysis Result: No manual analysis verdict given to this sample yet.
 Verdict Source: Valkyrie Automatic Analysis

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2015-09-17 15:26:10 UTC	No Match	?
Static Analysis Overall Verdict	2015-09-17 15:26:10 UTC	Malware	🚫
Dynamic Analysis Overall Verdict	2015-09-17 15:26:10 UTC	No Threat Found	?

Static Analysis


STATIC ANALYSIS OVERALL VERDICT	RESULT
Malware	🚫

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	✔️
Non-ascii or empty section names detected	Clean	✔️
Illegal size of optional Header	Clean	✔️
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Clean	✔️

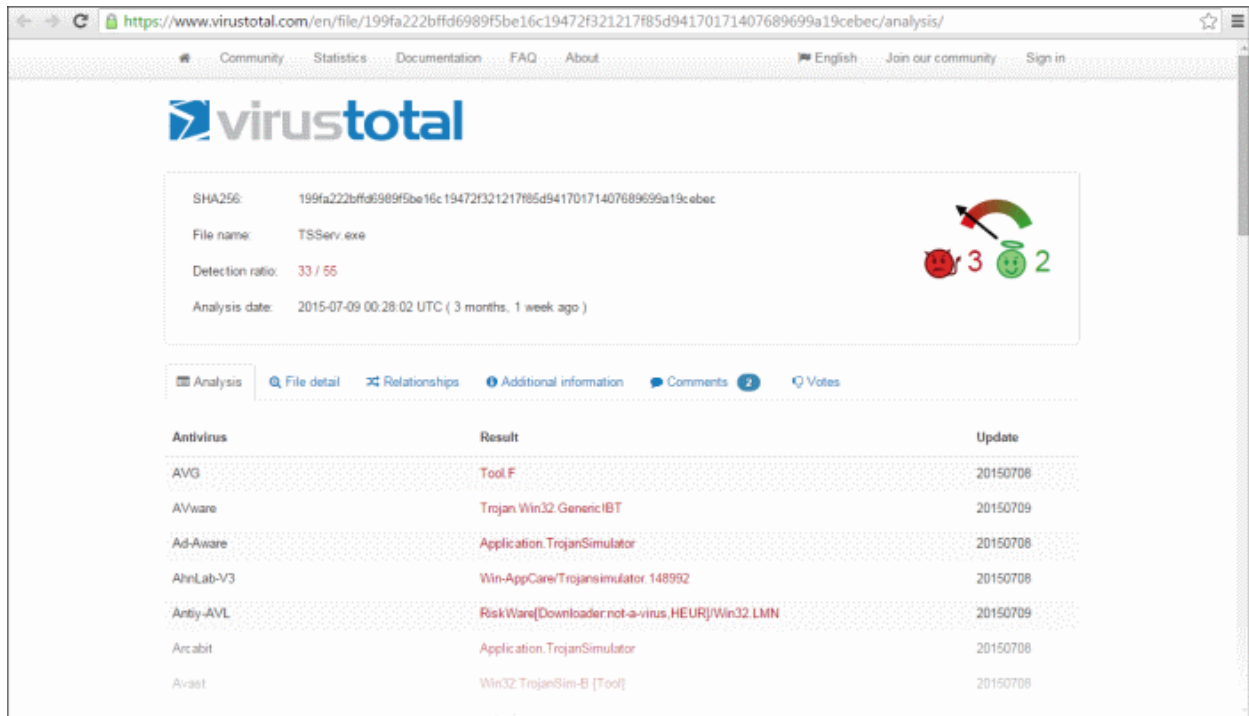
The report contains the compiled results of the automatic analysis explained in the **File Analysis Results** section. Scroll down the page to view the full report and save it.

View Virus Total Results for the File

Virus Total, a subsidiary of Google, is a information aggregation website and one of its function is to aggregate output data of different antivirus engines, website scanners and so on. Valkyrie allows to get the details of the file from this website.

- Click the 'View Virus Total Results' icon  under the 'Actions' column for a file to view the Virus Total analysis results for the file


The 'Virus Total' web page for the selected file will be displayed with its results.



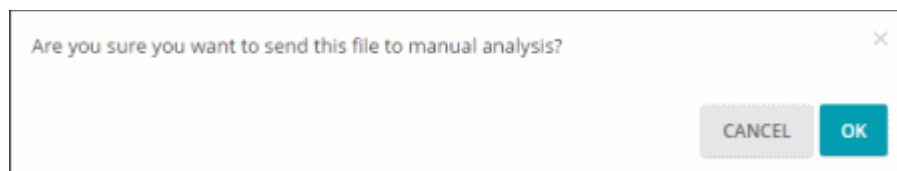
Scroll down the page to view the results for the file from different antivirus engines.

Send the File for Manual Analysis

You can also send a file for manual analysis by Comodo malware specialists for more comprehensive inspection in addition to the automated process. This is premium service and users should subscribe for the same.










- Click the 'Send to Manual Analysis' icon  under the 'Actions' column to submit a file for manual analysis by Comodo engineers

A confirmation dialog will be displayed.



- Click 'OK' to confirm

After the file is submitted for manual analysis, it will show as 'In Queue' under the 'Status' column and 'Unknown' under 'Manual Verdict'. The 'Send to Manual Analysis' icon also will not be available indicating the file is already submitted.

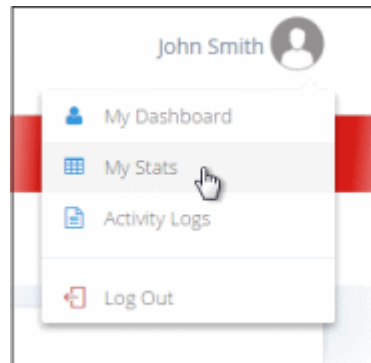
YOUR RECENT ANALYSIS REQUESTS									Total # of files	Total # of Clean	Total # of Unknown	Total # of Malware	Total # In Manual Analysis
									18	3	10	5	0
Show <input type="text" value="10"/> entries									Search: <input type="text"/>				
File Name	Path	SHA1	Source	Submit Date	Auto Verdict	Manual Verdict	Status	Actions					
jZipShell.dll	%5c%5... (x86)%6...	74e2e...	Upload	2015-10-15 11:04:56	Clean	Unknown	In Queue	  					
tsserv.exe	%5c%5...	846c1...	Upload	2015-10-14 12:48:51	Malware	Unknown	In Queue	  					
ocsinventory-deploy-tool.exe	%5c%5... (x86)%6... deploy-	e3fabf...	Upload	2015-10-14 12:06:21	No Threat Found			  					

Valkyrie Usage Statistics


The 'My Valkyrie Usage Statistics' page of Valkyrie displays how many files are submitted for your account and displays the details for:


- Today - Details of files submitted today
- This Week - Details of files submitted for this week
- This Month - Details of files submitted for month
- All Time - Total number of files submitted since account creation

To view your Valkyrie account usage statistics, click the 'My Stats' link



The usage statistics page will be displayed.






My Portal

MY VALKYRIE USAGE STATISTICS

Date	Total Files	Clean	Malware	Undetected	Automatic Analysis	Human Expert Analysis	Basic Info Req.	Full Info Req.	UI Get Info Req.
Today	1	1	0	0	0 (0)	0 (0)	0 (0)	0 (0)	1 (1)
This Week	1	1	0	0	0 (0)	0 (0)	0 (0)	0 (0)	2 (1)
This Month	1	1	0	0	0 (0)	0 (0)	0 (0)	0 (0)	2 (1)
All Time	22	10	5	7	19 (18)	6 (6)	234 (18)	0 (0)	23 (8)

*Values inside paranthesis represents unique number of files in that category.

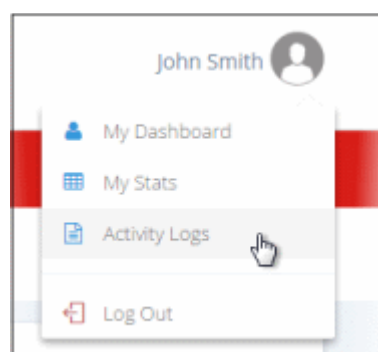
© Valkyrie, Comodo Group, Inc. 2016. All rights reserved.

My Valkyrie Usage Statistics - Table of Column Descriptions	
Column Header	Description
Date	Indicates the period of usage
Total Files	Number of files submitted for the period
Clean	Number of files found to be clean
Malware	Number of files found to be malware files submitted
Undetected	Indicates the number of files in which no threat was found
Automatic Analysis	Number of files submitted for automatic analysis
Human Expert Analysis	Number of files submitted for manual analysis
Basic Info Req.	Indicates the number of times the user has used Valkyrie REST API named fvs_basic_info, requesting basic analysis results from Valkyrie database such as if the file is uploaded before, verdict of last analysis, last analysis date, first analysis date, is the file whitelisted and so on.
Full Info Req.	This is same as Basic Info Req. but requested for greater detail. Indicates the number of times the user has used REST API named fvs_full_info, which is used to retrieve last analysis results from Valkyrie database in greater detail such as static, dynamic and manual results including behavioral and file information.
UI Get Info Req.	Indicates the number of times the user opened the detailed analysis results page from the Dashboard screen by pressing the  button or doing a search by SHA1 of a file.

Activity Logs

The 'Activity Logs' page provides the records of activities carried out in the Valkyrie account such as the activity date, user name, activity type and more.

To view your Valkyrie Activity Logs, click the 'Activity Logs' link



The activity logs page will be displayed. The number of logs to be displayed on each page can be selected from the 'Show entries' option on the left.

VALKYRIE
COMODO

John (unlicensed user)

Activity Logs

YOUR RECENT ACTIVITIES

Show 25 entries Search:

Activity Date	User Name	Email	Activity Type	Source IP	API Key	SHA1
2016-04-05 13:12:21	John		See MyStats	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	
2016-04-05 13:01:44	John		Get Info	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	e98186b79857f4d1aaadc16a...
2016-04-05 13:01:07	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	
2016-04-05 12:50:34	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	
2016-04-05 12:46:48	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	
2016-04-05 12:45:36	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	
2016-04-05 12:45:35	John		Log In	10.108.51.61		
2016-04-04 17:52:15	John		Download Auto Analysis Report	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	e98186b79857f4d1aaadc16a...
2016-04-04 17:36:33	John		Get Info	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	e98186b79857f4d1aaadc16a...
2016-04-04 16:14:30	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d...	
2016-04-04 16:14:29	John		Log In	10.108.51.61		

Sort and search options

Sorting the entries

- You can sort the items in ascending/descending order by clicking on the column headers.

Searching for particular item(s)

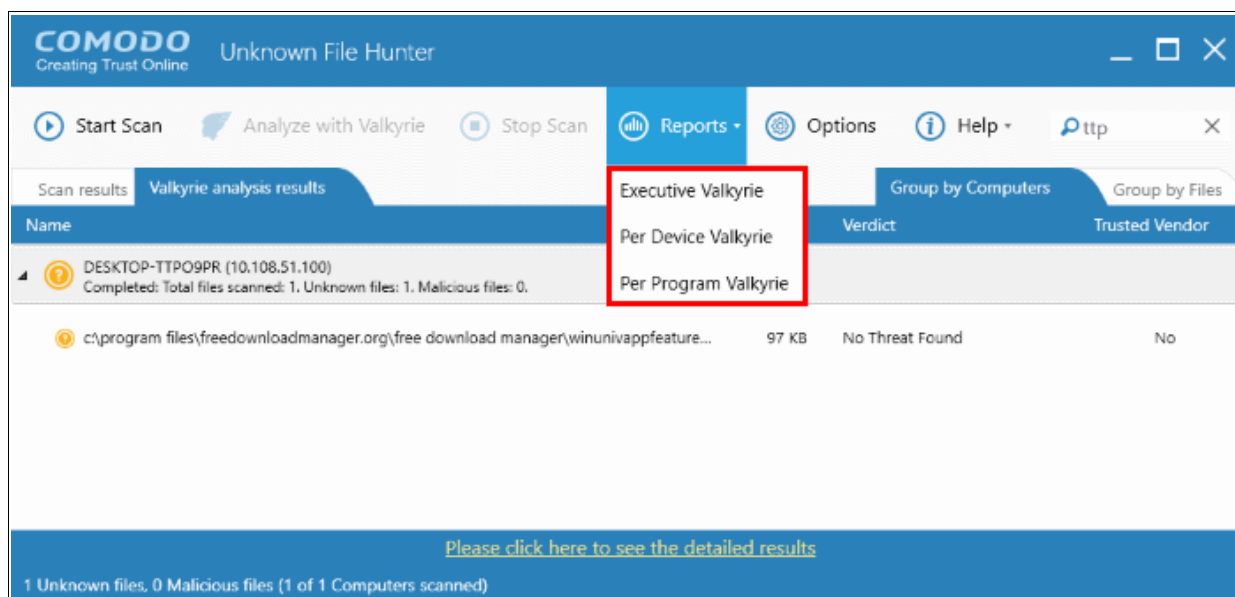
- Enter the details partially or fully in the search field on the top right side. You can search for logs based on all the columns.
- To display all the logs again, clear the search field.

Activity Logs - Table of Column Descriptions	
Column Header	Description
Activity Date	The date and time of using the Valkyrie account for a particular activity type
User Name	The logged user name for the account
Email	The email id of the Valkyrie account.
Activity Type	The name of the activity that was recorded.
Source IP	The IP of the computer from which the Valkyrie account was logged in and used
API Key	The private key of the user to use REST API
SHA1	If a file is the subject of activity then its SHA1 hash details will be displayed here.

5 Reports

After each scan is completed, the administrators can view the reports for the scan results. The reports are divided into three categories - Executive Report, Per Device Report and Per Program Report. The Executive Report is a summary of the scan providing details such as number of devices scanned, number of unknown programs found and so on. The Per Device Report is a summary of scan results providing details for each device scanned. The Per Program Report is a summary of scan results providing details of each unknown / malicious program, the devices affected by it and so on.

If the unknown files are submitted to Valkyrie for further analysis, the results reports for these scans also will also be available from the Reports drop-down as 'Executive Valkyrie', 'Per Device Valkyrie' and 'Per Program Valkyrie'. Please note that if you have not scanned with Valkyrie you can view only Executive, Per Device and Per Program Device reports and once you have scanned the files using Valkyrie analysis, you will be able to view only Valkyrie results.



Refer to the following for more details:

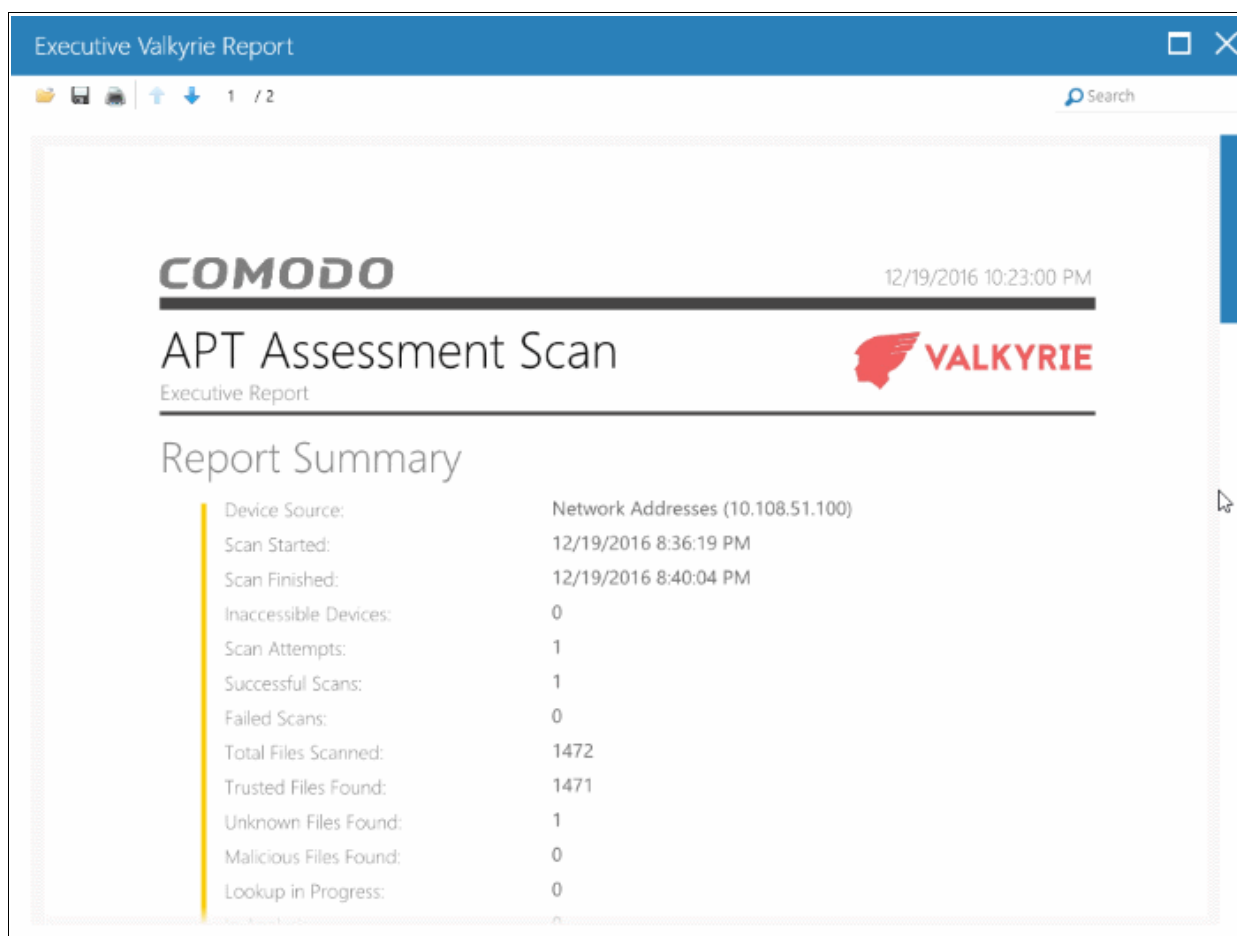
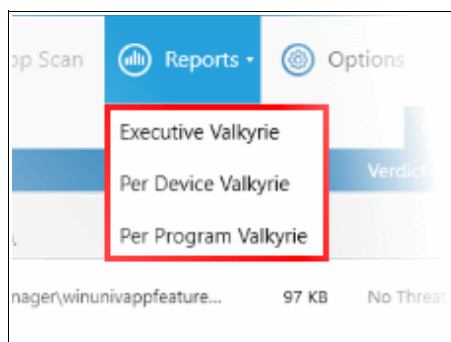
- **Executive Report**
- **Device Report**
- **Program Report**

5.1 Executive Report

The executive report is a summary of the 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 rating are also available in pie chart. If a Valkyrie scan is run, then the programs Valkyrie rating over the scanned devices is also displayed in pie chart.

To generate an 'Executive' report results, click 'Reports' and then 'Executive' or 'Executive Valkyrie'.

The report will be generated and displayed:



Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **Report Summary** - Provides the details of the scan such as number of devices scanned, date and time of the scan, number of malware found and so on.
- **Summary Charts** - Provides the details of programs found on the scanned devices and the rating of the scanned devices.
 - **Programs Rating Over Scanned Devices** - Results displayed in pie chart of the programs that were scanned on the devices. Provides the percentage of trusted programs, unknown programs and malware.
 - **Scanned Devices Rating** - The statuses of the scanned devices in pie chart providing the percentage of devices that are found safe, infected and at risk.
 - **Programs Valkyrie Rating Over Scanned Devices** - This is will be available in 'Executive Valkyrie' report only. Provides details of the Valkyrie rating of unknown files that were scanned.

5.2 Device Report

The 'Per Device Report' is a summary of scan results for a particular device. It includes details of malware found on each device, unknown files found and the path of the files. If a Valkyrie scan is run, then the Valkyrie verdict is also provided for the unknown files at the end of the report.

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

The report will be generated and displayed:

Detailed Per-Device Valkyrie Report

COMODO 12/19/2016 10:33:42 PM

APT Assessment Scan

Detailed Per-Device Report

Report Summary

Device Source:	Network Addresses (10.108.51.100)
Scan Started:	12/19/2016 8:36:19 PM
Scan Finished:	12/19/2016 8:40:04 PM
Inaccessible Devices:	0
Scan Attempts:	1
Successful Scans:	1
Failed Scans:	0
Total Files Scanned:	1472
Trusted Files Found:	1471
Unknown Files Found:	1
Malicious Files Found:	0
Lookup in Progress:	0

Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

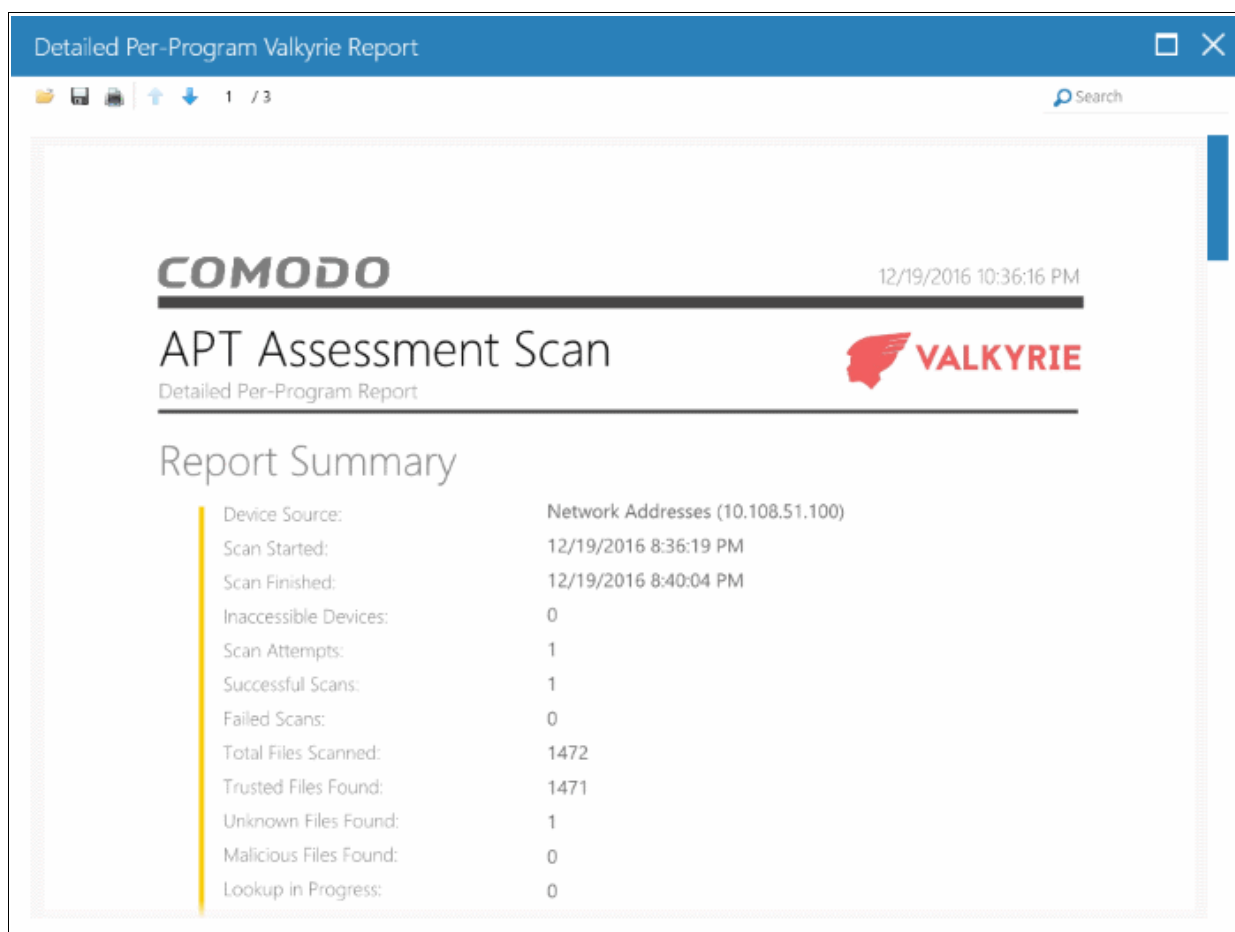
- **Report Summary** - Provides the details of the scan such as number of devices scanned, date and time of the scan, number of malware found and so on.
- **Summary Chart** - Provides the details in bar graph the top 10 endpoints that are detected with unknown/malware files.
- **Details per Device** - The details of each device including the name of the device, number of malware/unknown files in them, the path of each malware/unknown files in the affected device and more.
- **Valkyrie** - This is will be available in 'Per Device Valkyrie' report only. Provides the details of the scan report of each of the unknown file.

5.3 Program Report

The 'Per Program Report' provides scan results on a per program basis. It includes details of each malware/unknown file found, the devices on which they were found, the path of the files on the device and more. If a Valkyrie scan is run, then the Valkyrie verdict is also provided for each of the malware/unknown file.

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

The report will be generated and displayed:



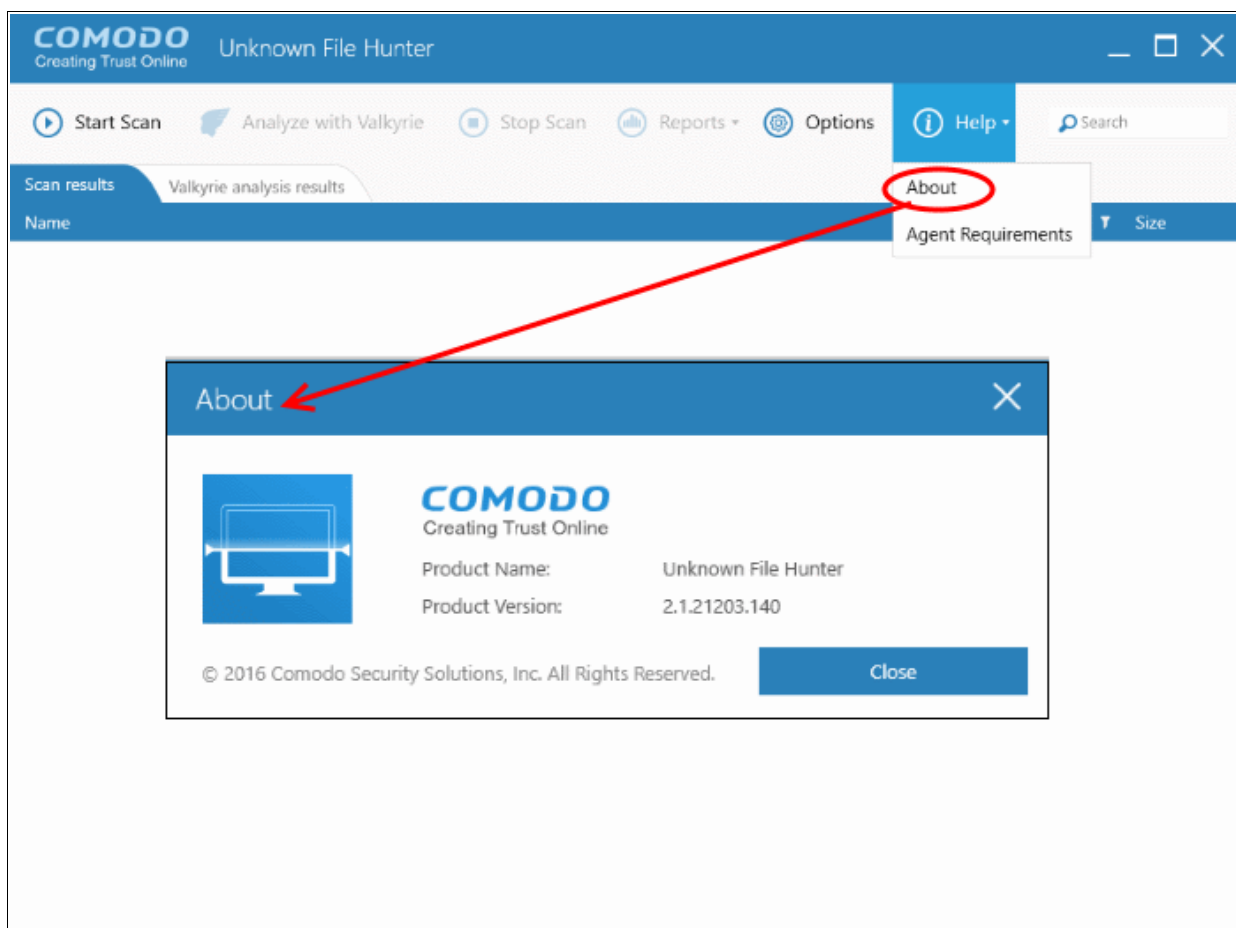
Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **Report Summary** - Provides the details of the scan such as number of devices scanned, date and time of the scan, number of malware/unknown files found and so on.
- **Summary Chart** - Provides the details of the top 10 unknown/malicious programs in bar graph.
- **Details per Program** - The details of each file including the name(s) of the device(s) it was found on, IP addresses of the devices and more. In the 'Per Program Valkyrie' report, the verdict of the Valkyrie analysis will also be provided for each program.

6 About Comodo Unknown File Hunter

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

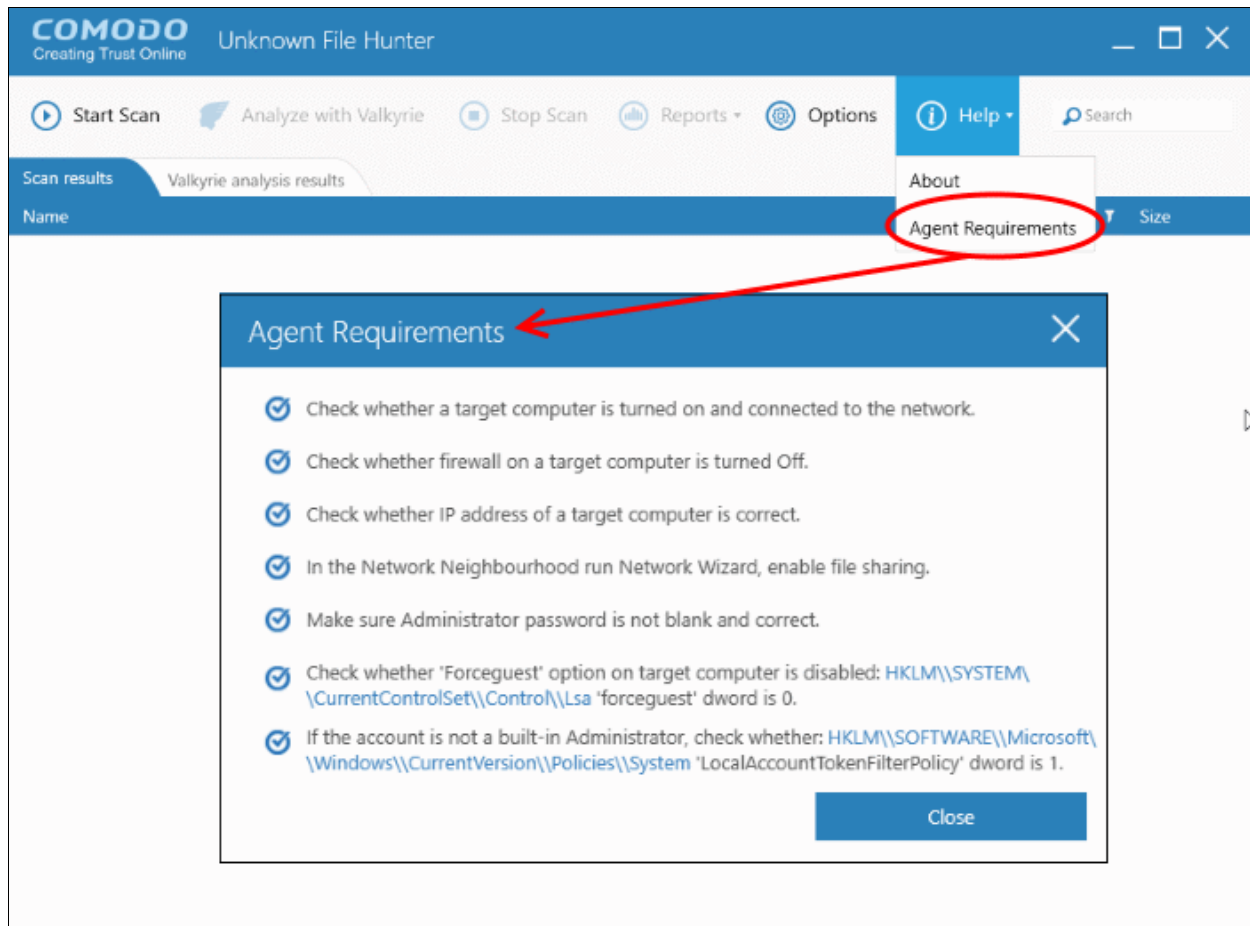
- To view the product details and its version number, click 'About' from the 'Help' in menu.



- 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

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street
Clifton, NJ, 07013
United States
Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford
Road, Salford, Greater Manchester M5 3EQ,
United Kingdom.
Tel : +44 (0) 161 874 7070
Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.comodo.com>.