



# Comodo Unknown File Hunter

Software Version 5.0

## Administrator Guide

Guide Version 5.0.091619

## Table of Contents

1 Introduction to Comodo Unknown File Hunter.....	3
2 Run Unknown File Hunter.....	4
2.1 The Main Interface.....	7
2.2 Login to UFH.....	9
3 Scan Computers.....	10
3.1 Scan Computers using Active Directory.....	11
3.2 Scan Computers by Workgroup.....	19
3.3 Scan Computers by Network Addresses.....	22
3.4 Scan Local Computer.....	24
4 Scan Results.....	28
4.1 Comodo Unknown File Hunter Scan Results.....	29
4.2 Valkyrie Analysis Results.....	33
5 Reports.....	37
5.1 Executive Report.....	37
5.2 Device Report.....	39
5.3 Program Report.....	40
6 About Comodo Unknown File Hunter.....	41
7 Agent Requirements.....	42
About Comodo Security Solutions.....	43

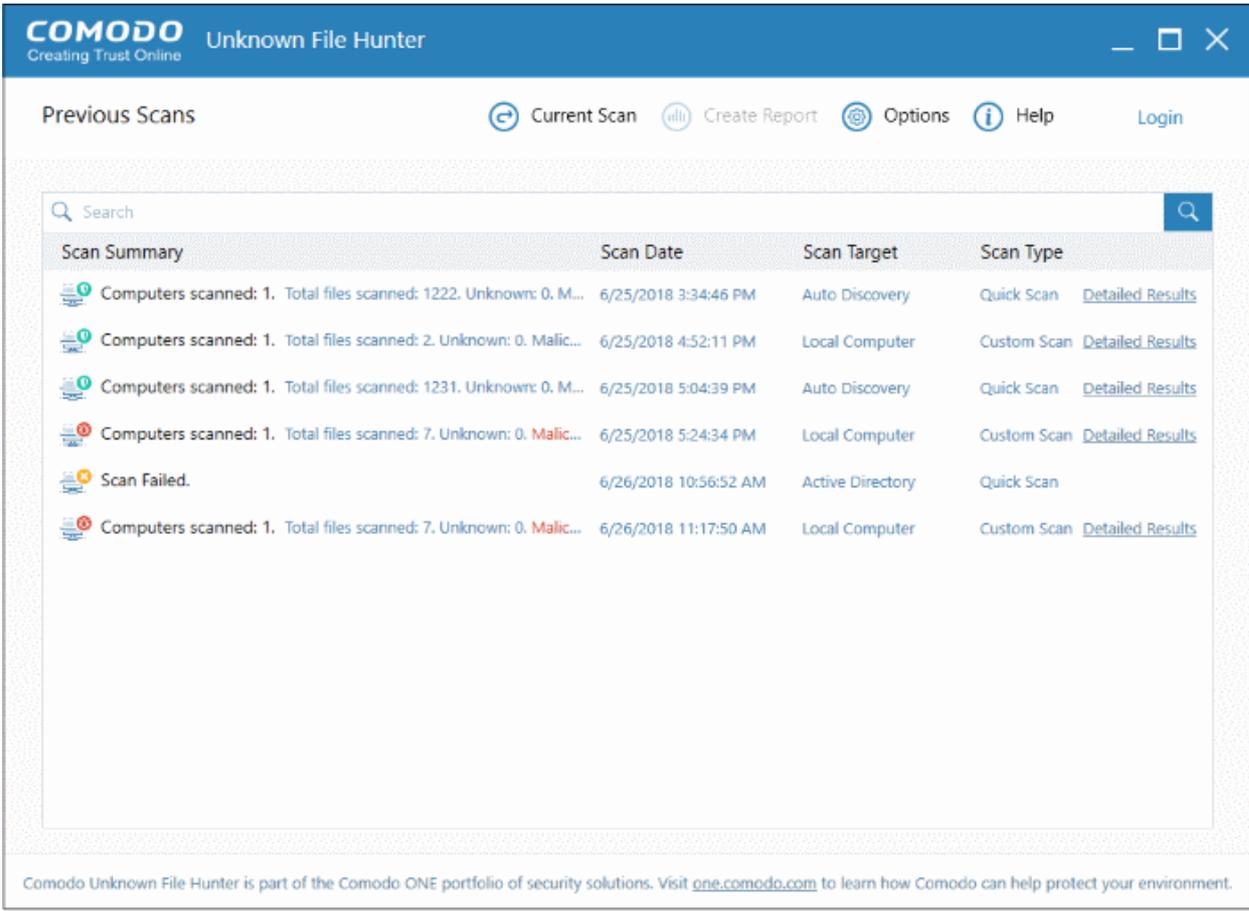
# 1 Introduction to Comodo Unknown File Hunter

Comodo Unknown File Hunter (UFH) is a lightweight scanner which identifies unknown, and potentially malicious files, on your network. After scanning your systems, it will classify all audited files as 'Safe', 'Malicious' or 'Unknown'.

While 'Safe' files are ok to run, and 'Malicious' files are dangers you should remove, it is in the 'Unknown' category where most zero-day threats are found. Traditional antivirus systems allow unknown files to run simply because they haven't yet been 'proven bad'.

Antivirus companies need to first observe the malware in action before they can classify it as malicious. Until this happens, the malware will have a rating of 'unknown' and is free to run undetected. 'Innocent until proven guilty' might be the defining characteristic of a healthy criminal justice system, but it certainly won't keep your network secure.

UFH allows you to upload unknown files to our Valkyrie servers where they will undergo a battery of tests to discover whether or not they are harmful. You can view the results of these tests in the UFH interface.



The screenshot displays the Comodo Unknown File Hunter interface. At the top, the Comodo logo and tagline 'Creating Trust Online' are visible. The main title is 'Unknown File Hunter'. Below the title, there are navigation buttons: 'Previous Scans', 'Current Scan', 'Create Report', 'Options', 'Help', and 'Login'. A search bar is located above the scan results table. The table has four columns: 'Scan Summary', 'Scan Date', 'Scan Target', and 'Scan Type'. The table contains six rows of scan data, each with a status icon (green for success, red for failure) and a 'Detailed Results' link.

Scan Summary	Scan Date	Scan Target	Scan Type
Computers scanned: 1. Total files scanned: 1222. Unknown: 0. M...	6/25/2018 3:34:46 PM	Auto Discovery	Quick Scan <a href="#">Detailed Results</a>
Computers scanned: 1. Total files scanned: 2. Unknown: 0. Malic...	6/25/2018 4:52:11 PM	Local Computer	Custom Scan <a href="#">Detailed Results</a>
Computers scanned: 1. Total files scanned: 1231. Unknown: 0. M...	6/25/2018 5:04:39 PM	Auto Discovery	Quick Scan <a href="#">Detailed Results</a>
Computers scanned: 1. Total files scanned: 7. Unknown: 0. Malic...	6/25/2018 5:24:34 PM	Local Computer	Custom Scan <a href="#">Detailed Results</a>
Scan Failed.	6/26/2018 10:56:52 AM	Active Directory	Quick Scan
Computers scanned: 1. Total files scanned: 7. Unknown: 0. Malic...	6/26/2018 11:17:50 AM	Local Computer	Custom Scan <a href="#">Detailed Results</a>

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

## Features

- No installation required. You can run UFH direct from a USB stick
- Capable of scanning computers from Active Directory, Workgroup or by Network Address
- Unknown files can be automatically uploaded to Comodo Valkyrie and tested for malicious behavior
- Detailed reports provide invaluable insights into the trust level of files on your network

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

- **Introduction**
- **Run Unknown File Hunter**
- **Scan Computers**
  - **Scan Computers using Active Directory**
  - **Scan Computers by Workgroup**
  - **Scan Computers by Network Addressees**
  - **Scan Local Computer**
- **Scan Results**
  - **Comodo Unknown File Hunter Tool Scan Results**
  - **Valkyrie Analysis Results**
- **Reports**
  - **Executive Report**
  - **Device Report**
  - **Program Report**
- **About Unknown File Hunter**
- **Agent Requirements**

## 2 Run Unknown File Hunter

Comodo Unknown File Hunter can be downloaded from:

- **Comodo Dragon (CD) / Comodo One**
- **Comodo Valkyrie website**

### Comodo Dragon / Comodo One management console

Unknown File Hunter is available for download from your Dragon / Comodo One account:

- Login to your Comodo Dragon / Comodo One account at <https://platform.comodo.com/app/login/> / <https://one.comodo.com/app/login>
- Click 'Tools' > Click 'Download' in the Unknown File Hunter tile
  - You can sign up for a free Comodo Dragon / Comodo One account at <https://platform.comodo.com/signup/> / <https://one.comodo.com/signup/>. Creating a Dragon / Comodo One account also creates a Valkyrie account for you.
  - You can login to UFH and Valkyrie with your Dragon / Comodo One credentials

### Comodo Valkyrie Website

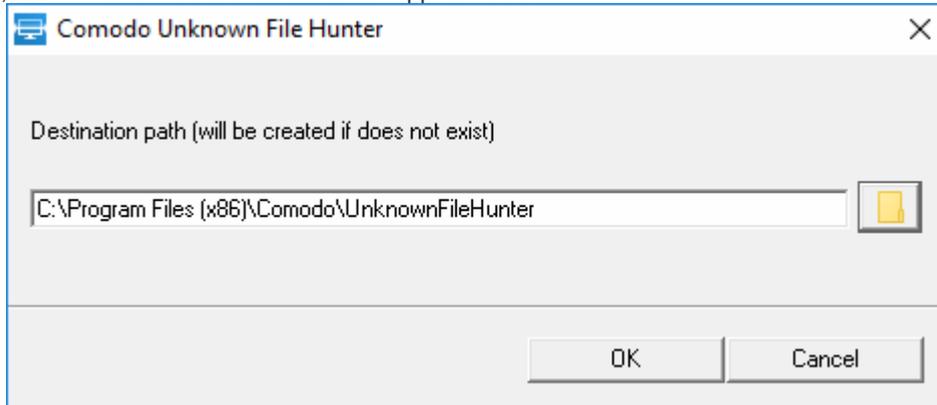
- Go to <https://valkyrie.comodo.com/>
- Click 'Download Unknown File Hunter'
  - You can create a Valkyrie account at <https://valkyrie.comodo.com>

### Run Unknown File Hunter

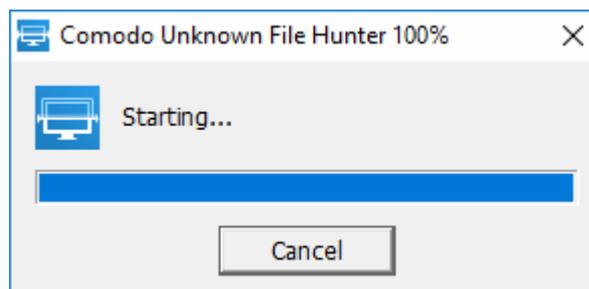
- Launch the tool by double-clicking on the application icon:

## UnknownFileHunter

- Next, choose the location from which the app should run:



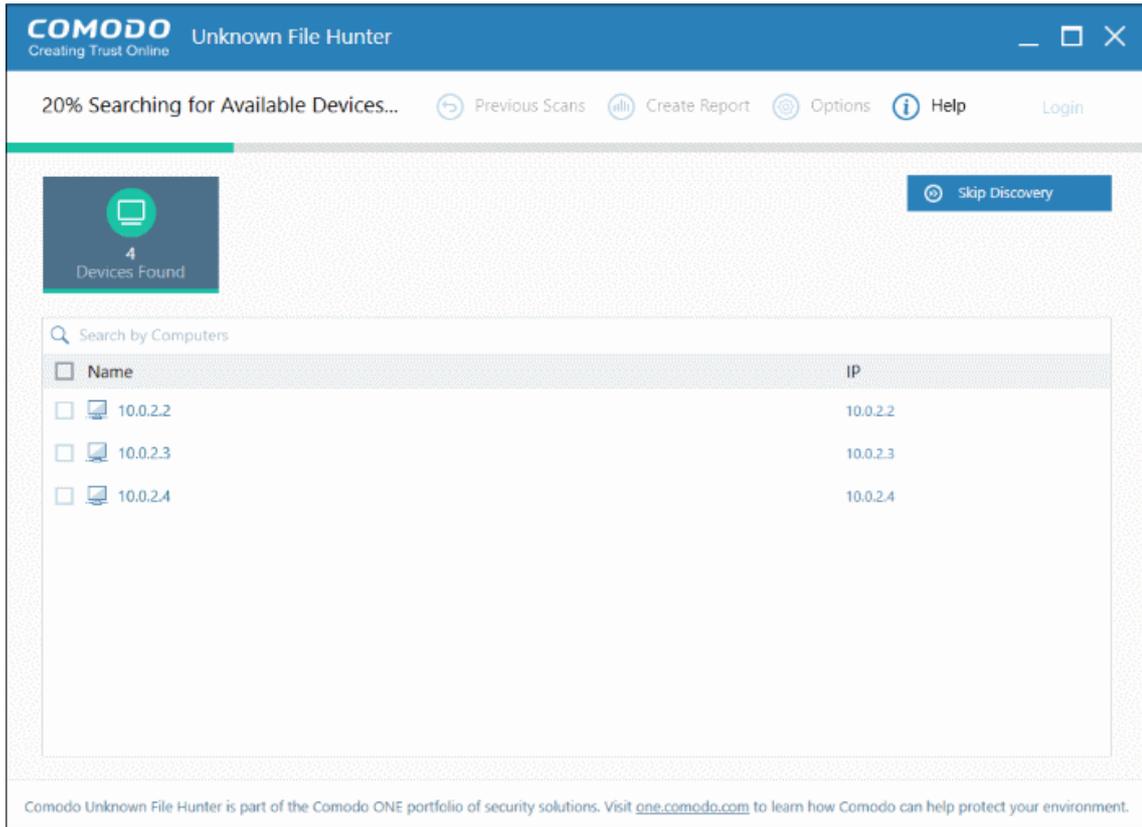
- The default location is C:\Program Files (x86)\Comodo\UnknownFileHunter. Click the folder icon to change the path if required. Note: This dialog will appear each time you run the application and you can choose different locations as you prefer.



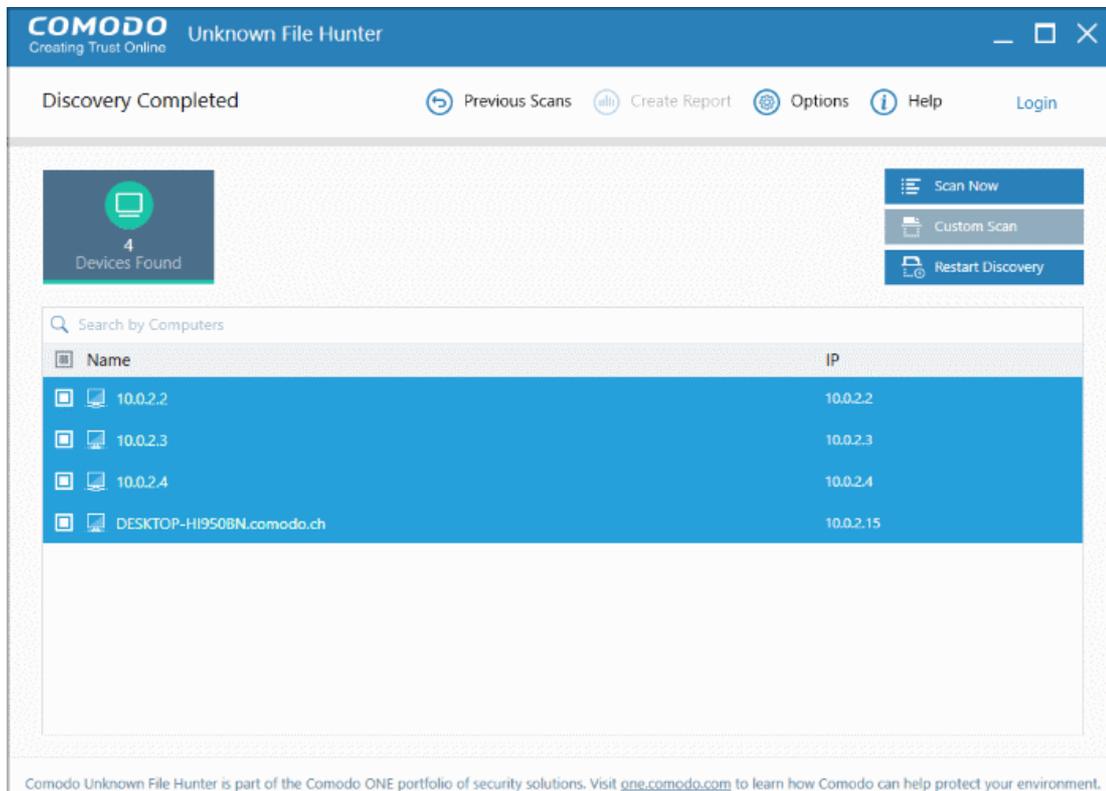
- Please read the EULA before continuing. Click the 'License agreement' link to read the full agreement. Click 'I Accept' to continue. Note: The EULA will appear when you first run the tool on a computer.



- The app will search for available devices on your network:

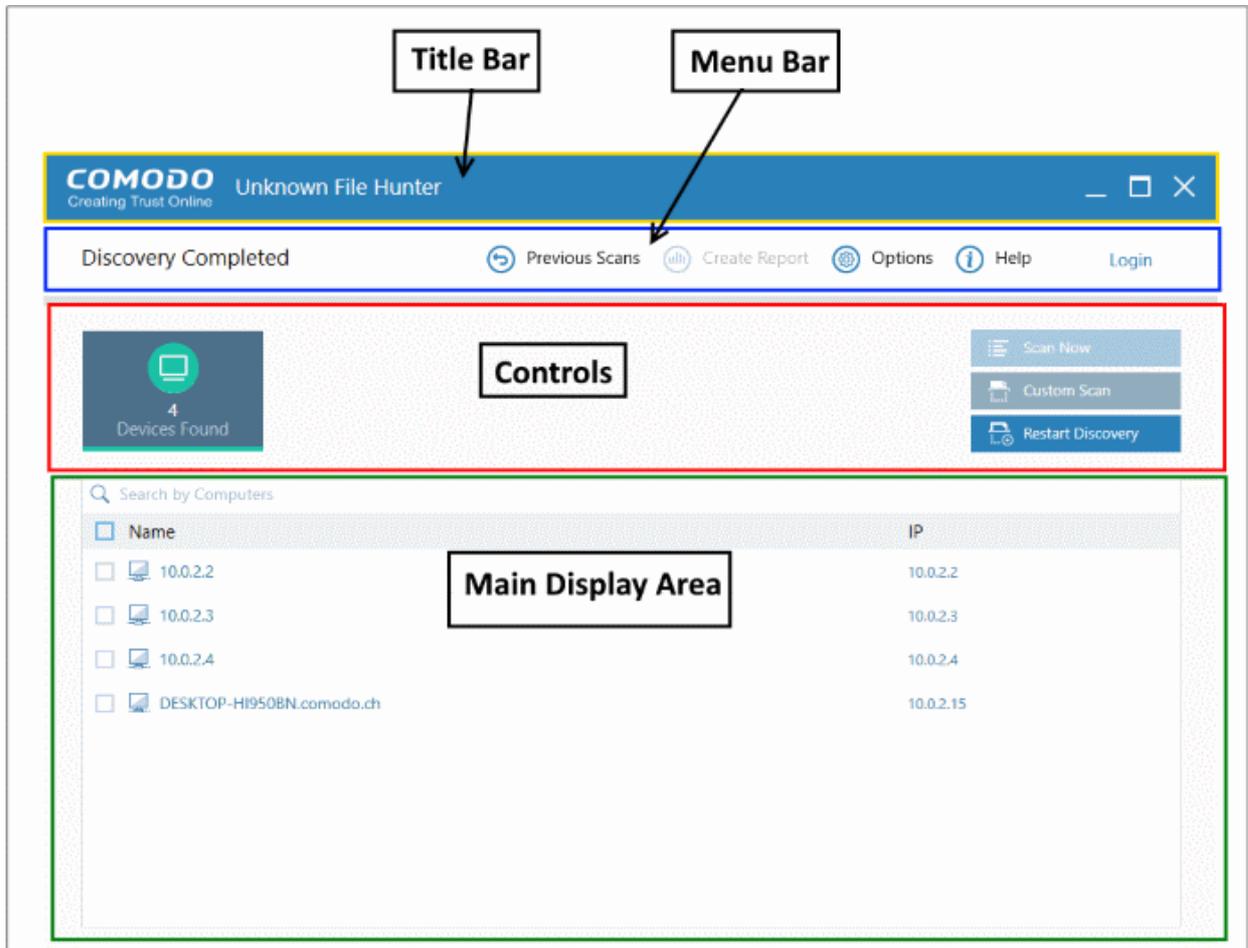


- Select all devices that you want to scan and click 'Scan Now'.



## 2.1 The Main Interface

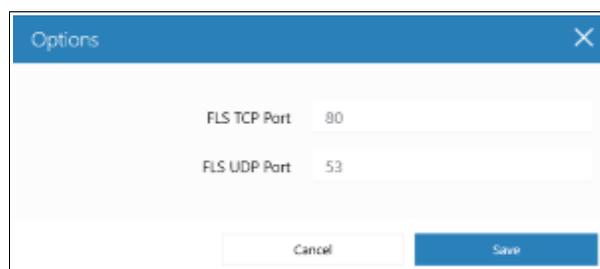
The main interface lets you configure and run scans, view results and generate risk reports.



### Main Functional Areas

- **Menu Bar** – Shows the current status of the scan and contains the following buttons:
  - **Previous Scans / Current Scan** - View results of past scans / current scan.
  - **Create Report** - View reports generated by the UFH tool. See '**Reports**' for more details.
  - **Options** – Shows the port numbers that UFH 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.

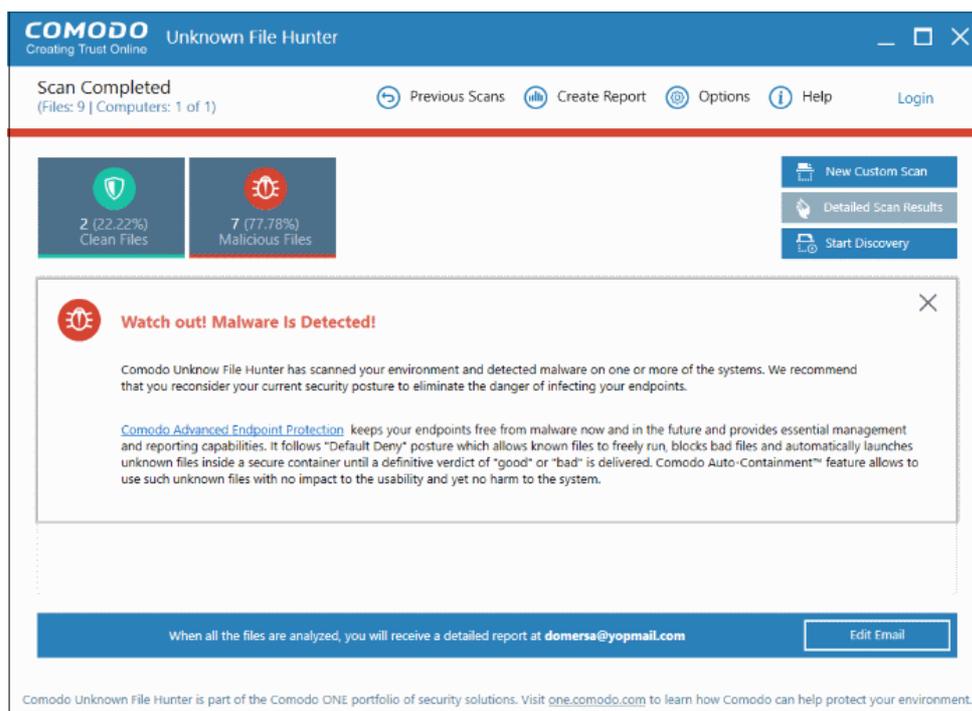


- **Help** – Contains 'About' and 'Agent Requirements'

'About' - shows product and version information.

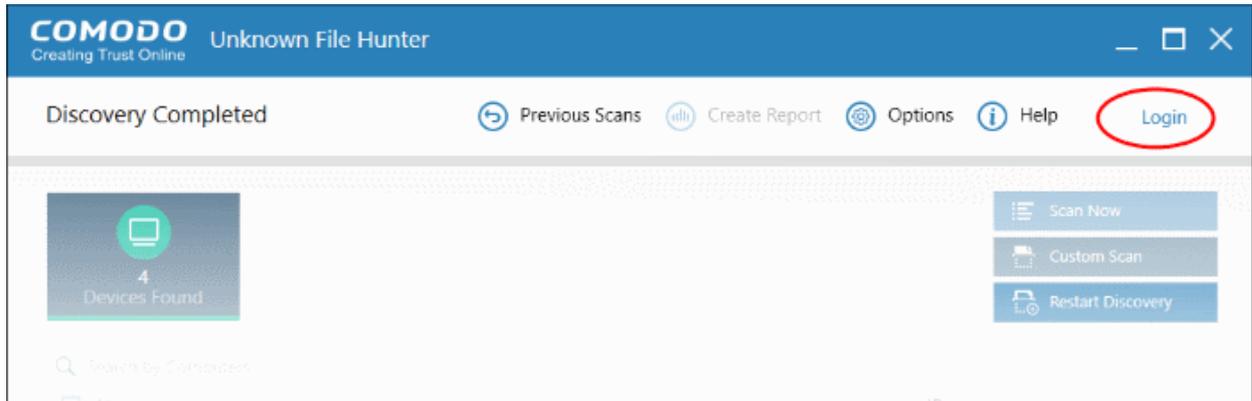
'Agent Requirements' - Troubleshooting advice if you experience problems connecting to your target computer.

- **Login** – You can use the tool as a guest or login as a registered user. See 'Login to UFH' for more information.
- **Controls** – On the left, UFH shows messages such as the number of devices found, number of malicious files detected and so on. Also contains control buttons for:
  - **Scan Now / New Custom Scan / Stop Scan** - Scan target computers to identify unknown files. You can add computers via Active Directory, Workgroup or Network Addresses.
    - Scan Now – Shown when you first open the application.
    - New Custom Scan – Shown after you have run the first scan for the session.
    - Stop Scan – Cancel a scanning process.
    - See '**Scan Computers**' for more details.
  - **Custom Scan / Detailed Scan Results**
    - Custom Scan – Configure your scan. You can scan by Active Directory, network address, workgroup and local computer. See '**Scan Computers**' for more information.
    - Detailed Scan Results – Shown after a scan is completed. Click this button to view full results of the scan at <https://valkyrie.comodo.com>. See '**Valkyrie Analysis Results**' for more information.
  - **Start Discovery / Skip Discovery / Restart Discovery** – Start/stop discovery of devices on your network.
- **Main Display Area** - Details of discovered endpoints, scanned endpoints and scan results. See '**Scan Computers**' and '**Scan Results**' for more details.
  - **Search** - Look for discovered endpoints by name or IP.
  - **Notifications** - Information about unknown and malicious files detected after a scan finishes. Click the 'Edit Email' button to change the recipient list for Valkyrie analysis results.

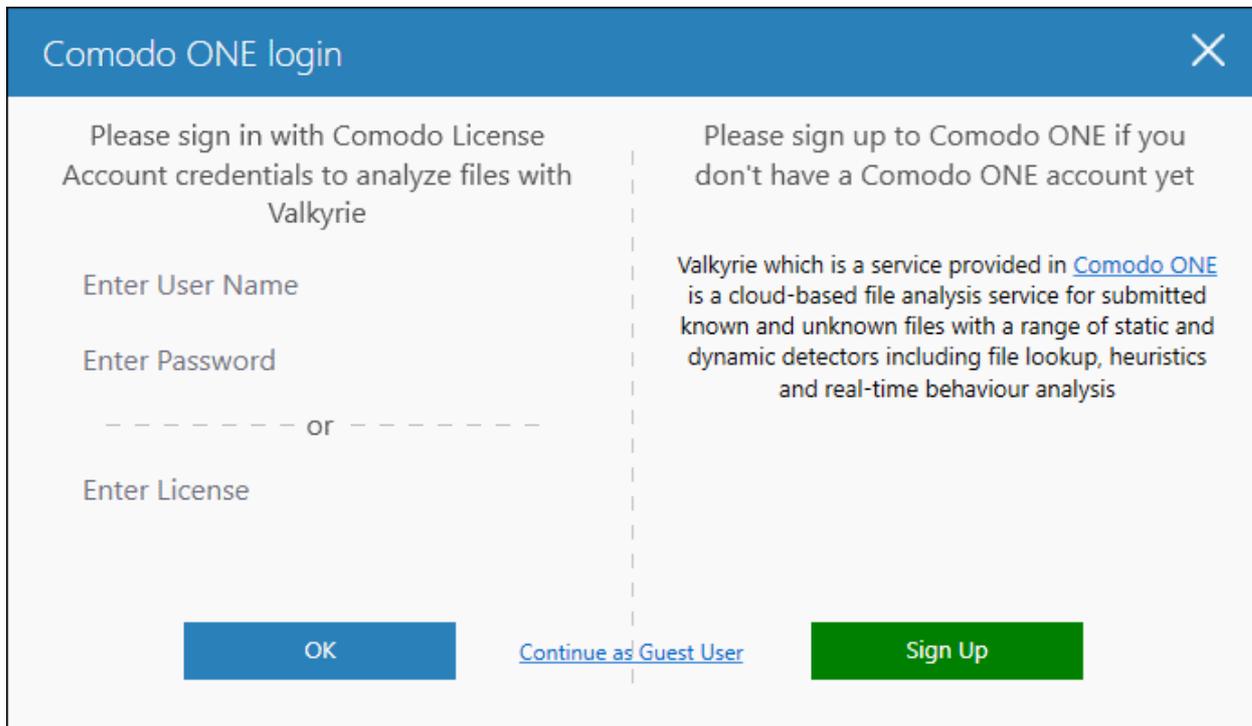


## 2.2 Login to UFH

- Open the UFH executable to start the application.



- Click 'Login' at top-right of the screen.
- If you do not login, you can scan but cannot upload unknown files to Valkyrie for analysis.

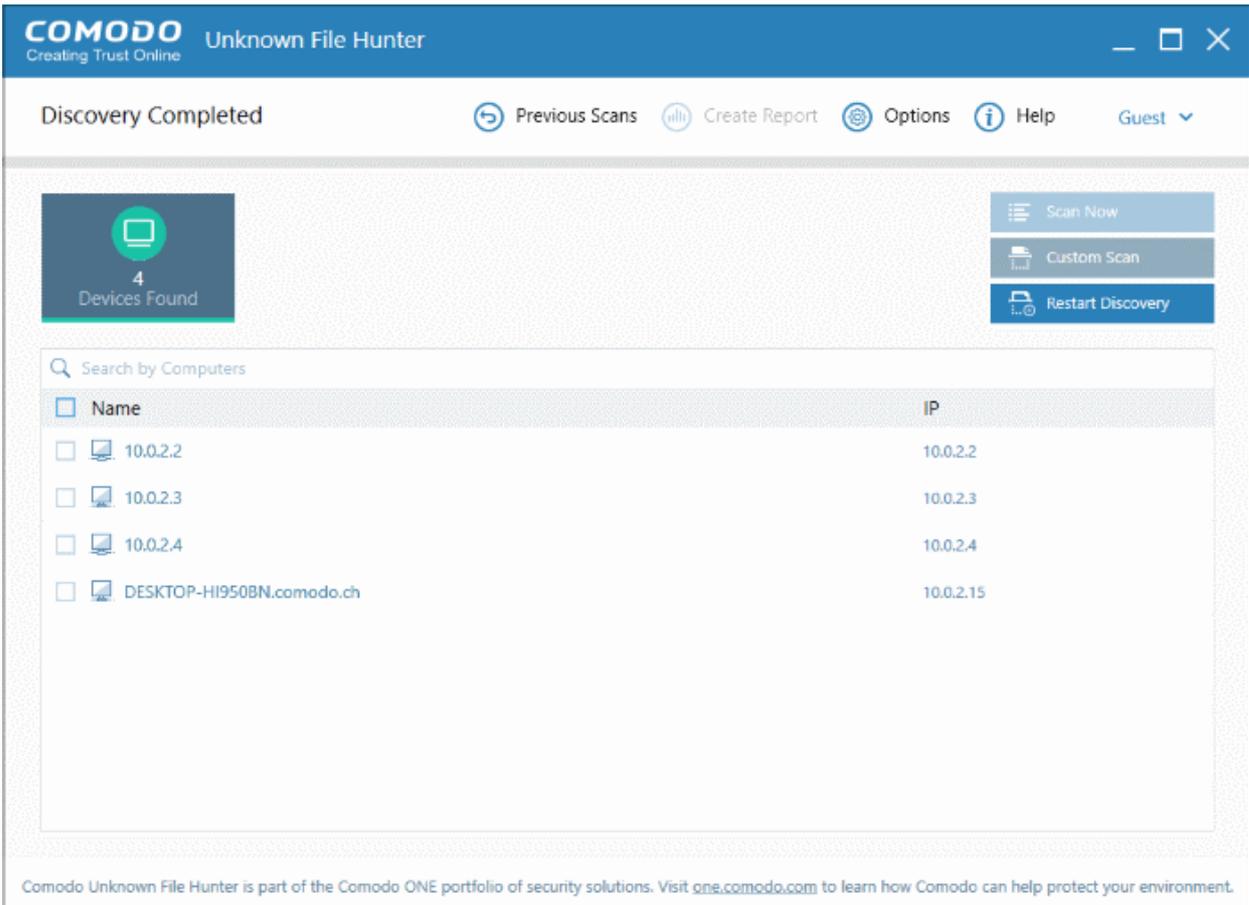


- Click 'Continue as Guest User' if you want to login later on, or if you do not have an account.
- Existing users - login with your Comodo or Valkyrie username/password, or with your Valkyrie license number.
- If you do not have a license, click 'Sign Up' to create a free Valkyrie account.

## 3 Scan Computers

There are multiple ways you can scan computers for unknown files:

- **Active Directory** - Scan endpoints which belong to an Active Directory domain
- **Workgroup** –Scan endpoints that belong to a workgroup
- **Network Address** - Scan endpoints by specifying their host name/IP address, or scan all endpoints on an IP range
- **This Computer** – Scan your local device.



The screenshot displays the Comodo Unknown File Hunter web interface. The top navigation bar includes the Comodo logo, the text "Creating Trust Online", and the product name "Unknown File Hunter". A status bar indicates "Discovery Completed" and provides links for "Previous Scans", "Create Report", "Options", "Help", and a user profile "Guest".

On the left, a card shows "4 Devices Found". On the right, there are buttons for "Scan Now", "Custom Scan", and "Restart Discovery".

The main content area features a search bar labeled "Search by Computers" and a table of discovered devices:

<input type="checkbox"/> Name	IP
<input type="checkbox"/> 10.0.2.2	10.0.2.2
<input type="checkbox"/> 10.0.2.3	10.0.2.3
<input type="checkbox"/> 10.0.2.4	10.0.2.4
<input type="checkbox"/> DESKTOP-HI9508N.comodo.ch	10.0.2.15

At the bottom, a footer note states: "Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](https://one.comodo.com) to learn how Comodo can help protect your environment."

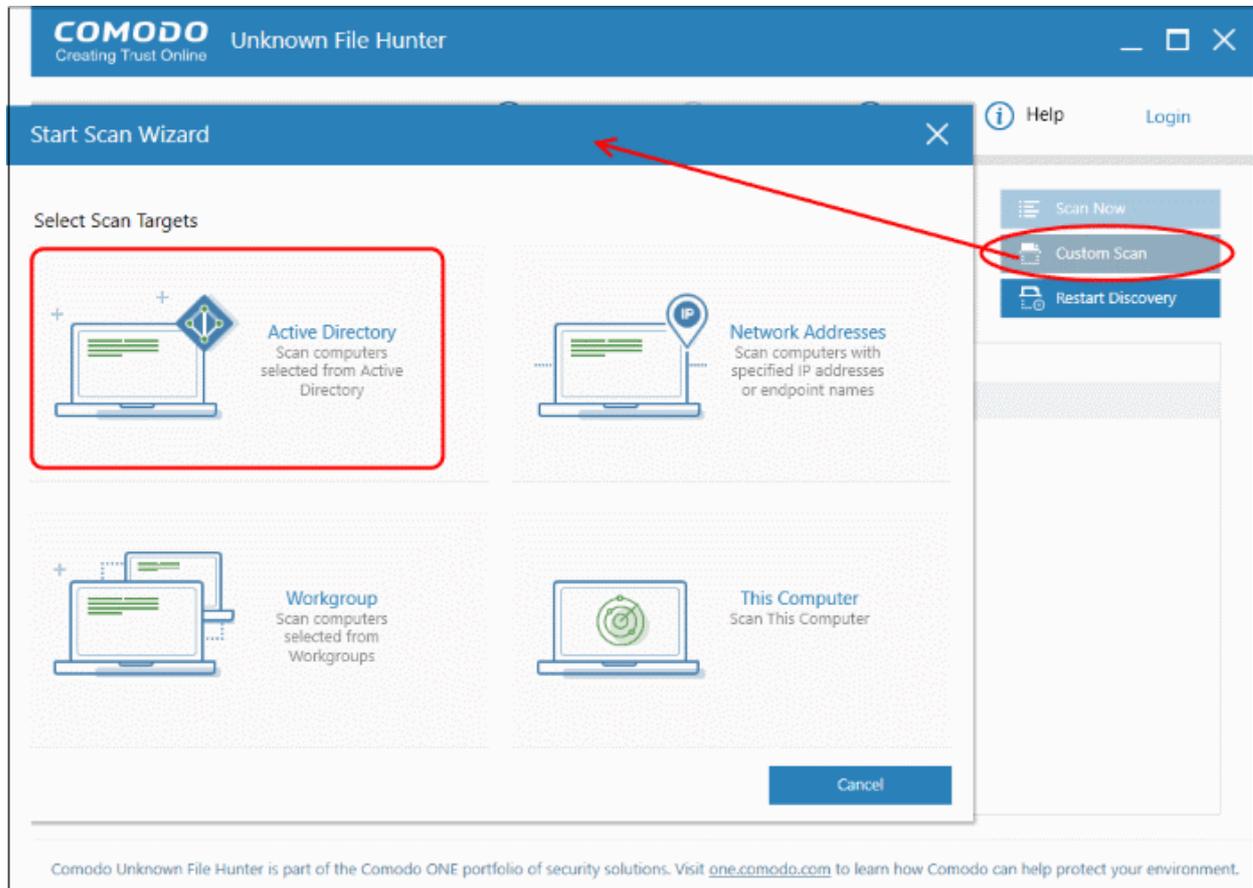
See the following sections for help on each method:

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

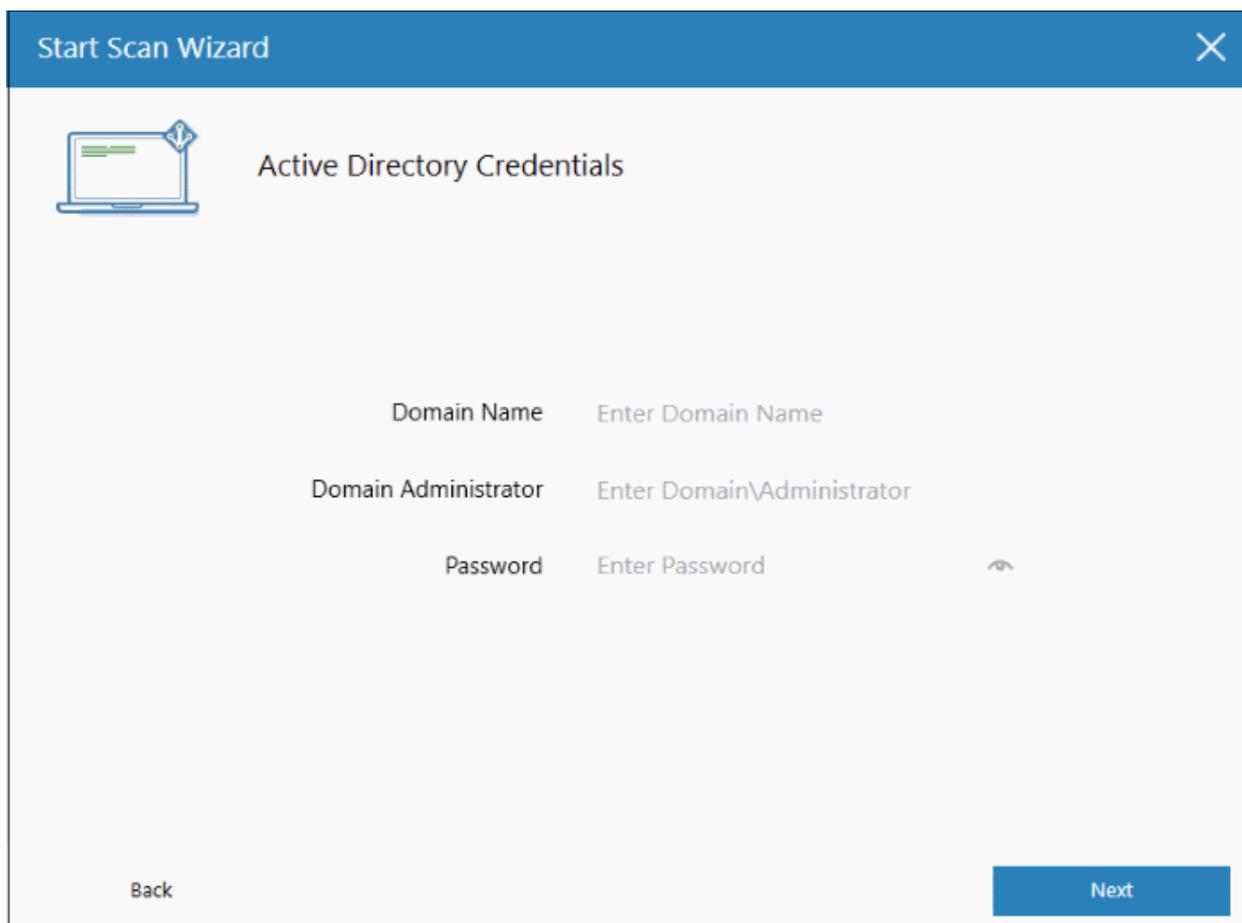
## 3.1 Scan Computers using Active Directory

To scan all or selected endpoints in an Active Directory domain:

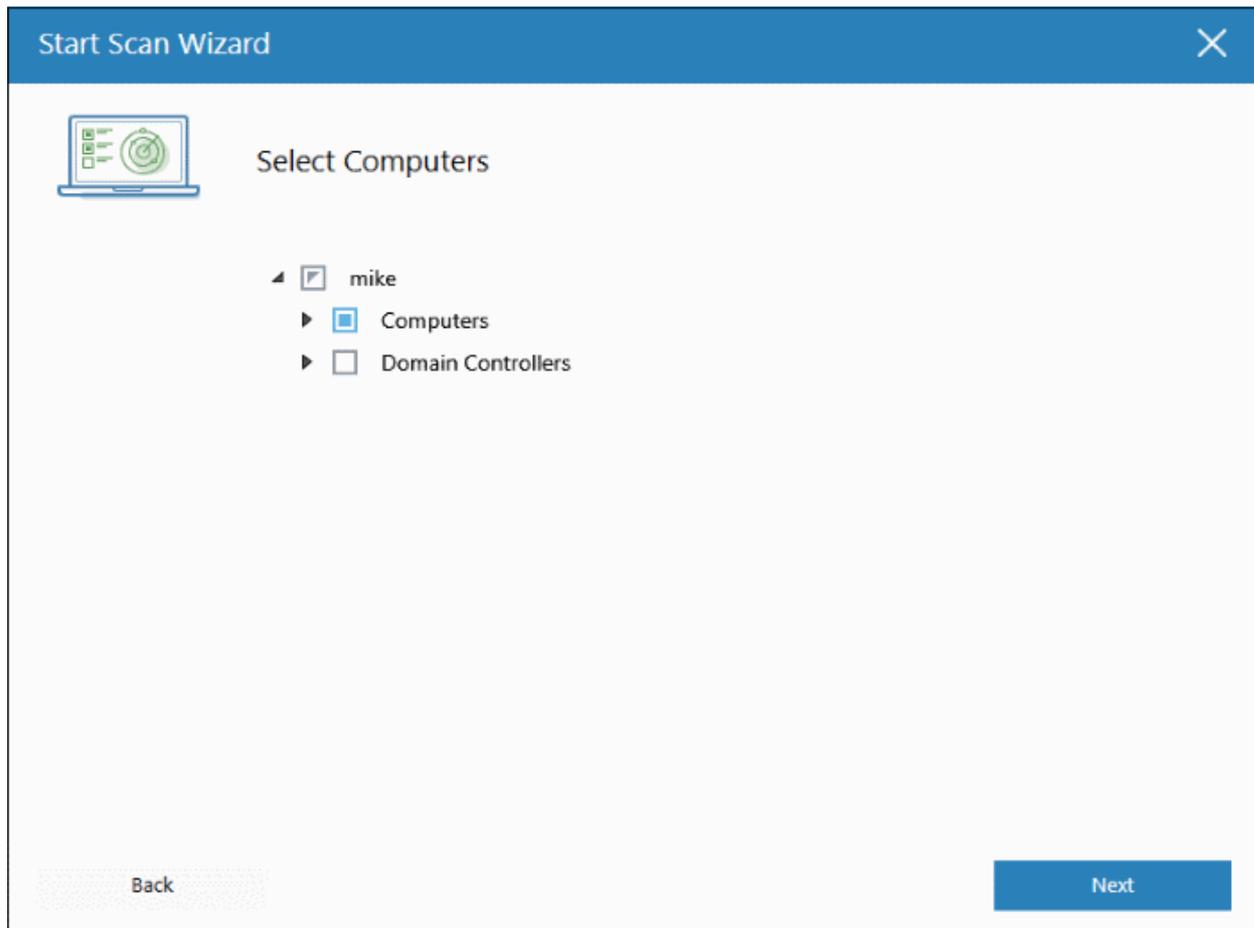
- Open Unknown File Hunter
- Click the 'Custom Scan' \ 'New Custom Scan' button
- Select 'Active Directory' to open the AD configuration screen:



- Enter the name of your Active Directory domain and provide admin username and password:



- After logging in, the 'Select Computers' screen will open:
- Choose the endpoints that you want to scan and a scan type:
  - Quick Scan:** Scans critical and commonly infected areas of target endpoints
  - Full Scan:** Scans all files and folders on target endpoints.



- Click 'Scan Now' to begin the scan.
- Scan progress is shown for each computer, including the number of unknown files and malicious files found so far. Overall scan progress is shown on the menu bar.



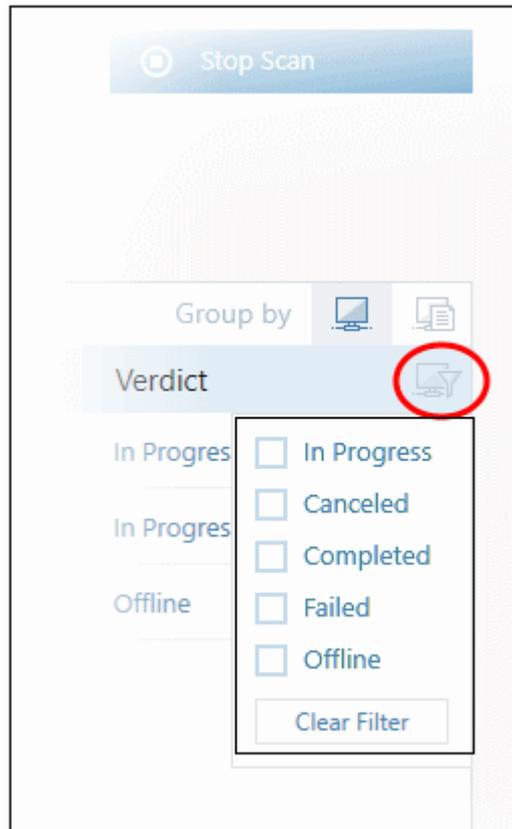
- 'Stop Scan' - Discontinue the scan.
- 'Edit Email' – Specify the email address to which the scan report should be sent

The tiles above the scan area show how many files of each type have been found so far:

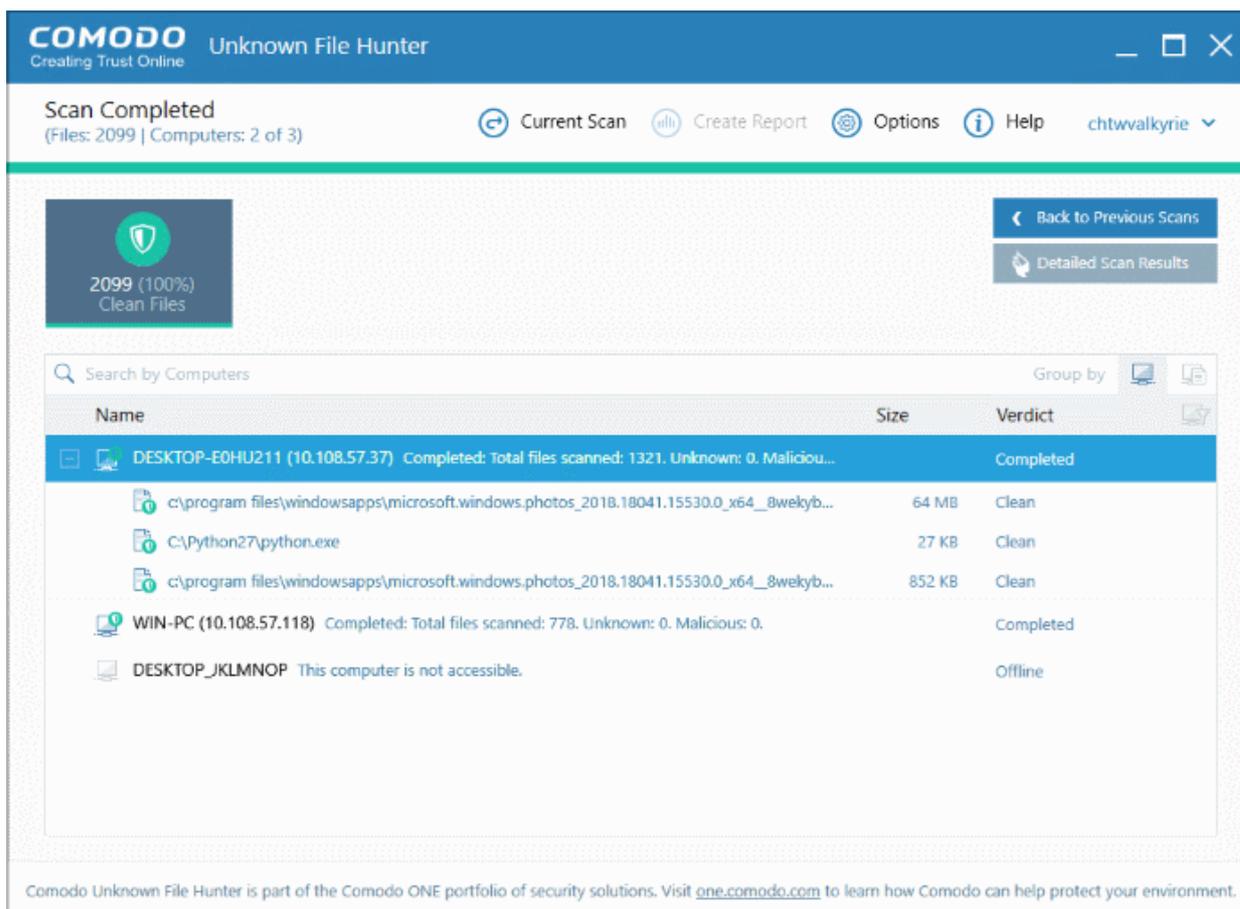
	<p>Safe files. These files are on the Comodo whitelist are OK to run.</p>
	<p>Unknown, potentially malicious files.</p> <ul style="list-style-type: none"> <li>• These files are automatically uploaded to Valkyrie for analysis during the scan.</li> <li>• You can view the analysis results by signing in to your Valkyrie account at <a href="https://valkyrie.comodo.com/login">https://valkyrie.comodo.com/login</a></li> <li>• You also can sign into Valkyrie with your Comodo Dragon / Comodo One username and password.</li> </ul> <p>See '<a href="#">Valkyrie Analysis Results</a>' for more information.</p>

 <p>7 (100%) Malicious Files</p>	<p>Malicious files. These files are on the Comodo blacklist of known malware and should not be allowed to run on your network.</p>
---	--

- Click the funnel icon to filter scans by status:



Results are shown when the scan finishes:



Scan Interface - Table of Column Descriptions	
Column Header	Description
Name	The name of the computer on which the scan was run. Click '+' to view files discovered on the computer.
Size	The size of the analyzed file.
Verdict	<p>Status of the file. The possible values are:</p> <ul style="list-style-type: none"> <li>In Progress – Unknown file which is queued for upload to Valkyrie, Comodo's file analysis system</li> <li>Uploading – Unknown file which is currently being submitted to Valkyrie</li> <li>In Analysis – Unknown file which is currently being tested by Valkyrie</li> <li>Clean – Valkyrie tests found the file is safe to run</li> <li>Malicious – Valkyrie tests found the file is harmful and should not be allowed to run</li> <li>No Threat Found – Unknown file which has been passed onto human experts for further testing. Valkyrie's automated tests did not find any malicious behavior, but the file exhibited certain traits which warrant further investigation. We advise you to run this file in the container/sandbox until a full verdict is available, or avoid running it altogether.</li> </ul>

- Each scan result is shown on a different row and contains information such as the number and type of files

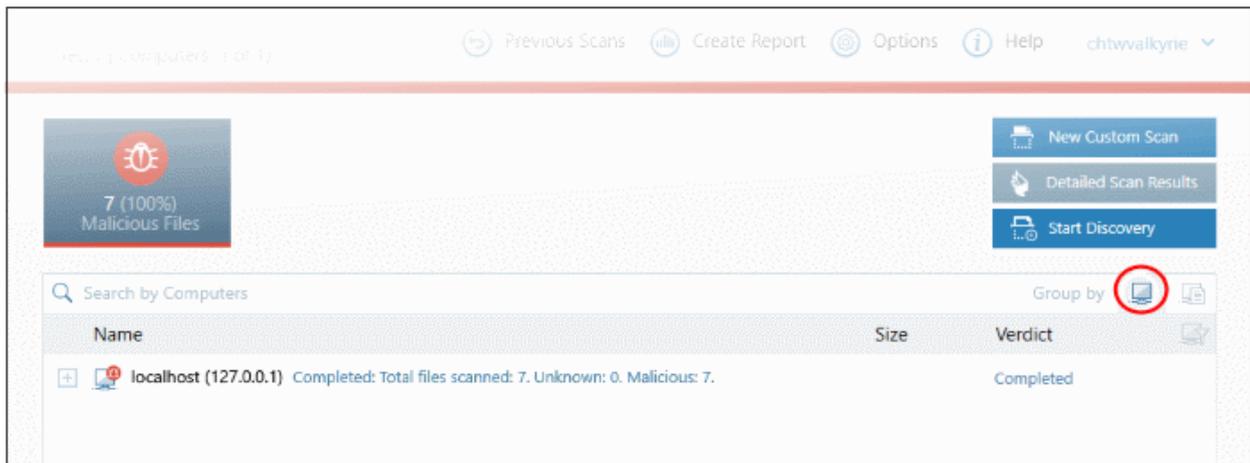
found.

- 'Clean' - Unknown files that have been analyzed by Valkyrie and found safe.
- Click the 'Group By' icons on the right to change how results are displayed:
  - **Group by Computer:** Lists all computers scanned. Expand any computer to view the unknown / malicious files on those computers.
  - **Group by File:** Lists all unknown / malicious files discovered by the scan. Expand any file to view the computers on which it was discovered.

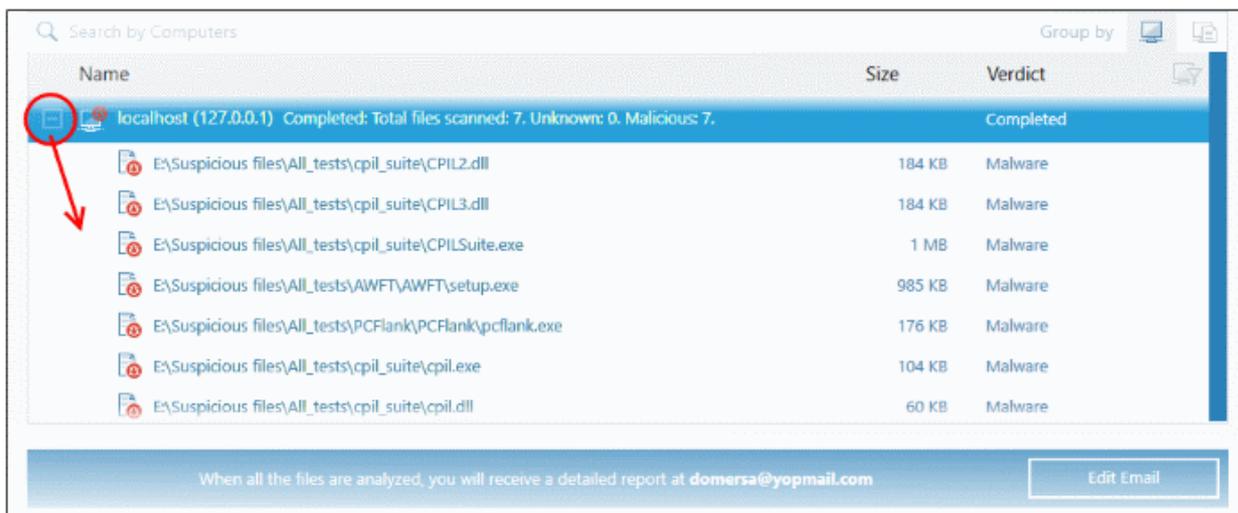
## Group by Computer



- Click the computer icon to view results by computer:

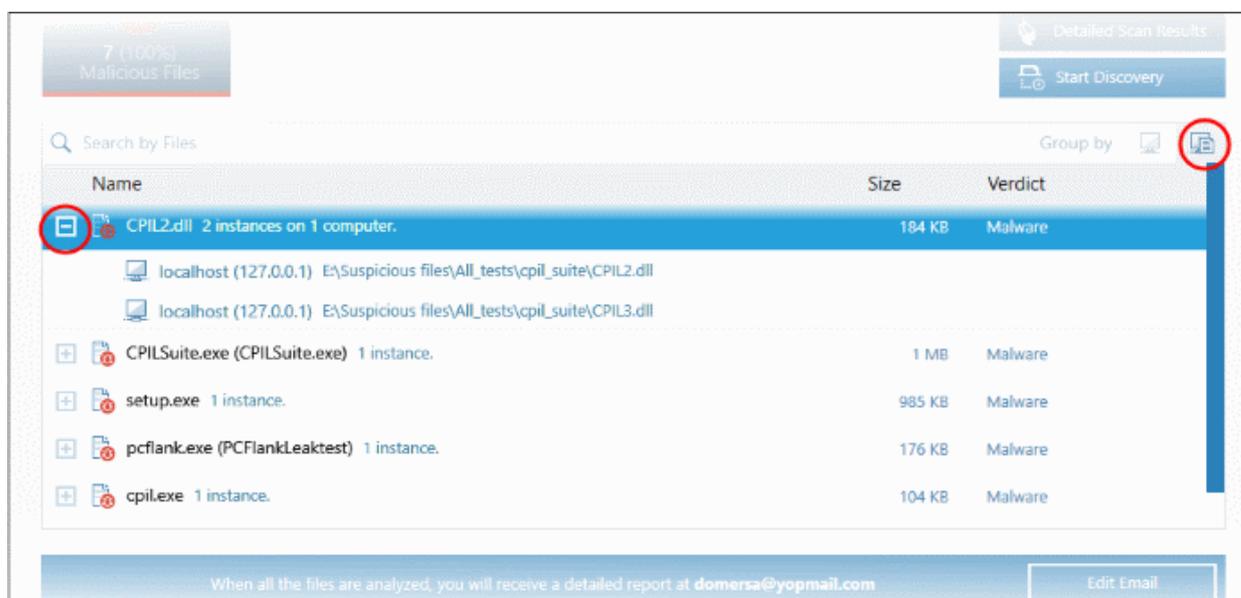


- Click '+' beside an endpoint to view the location of the unknown / malicious files



## Group by File

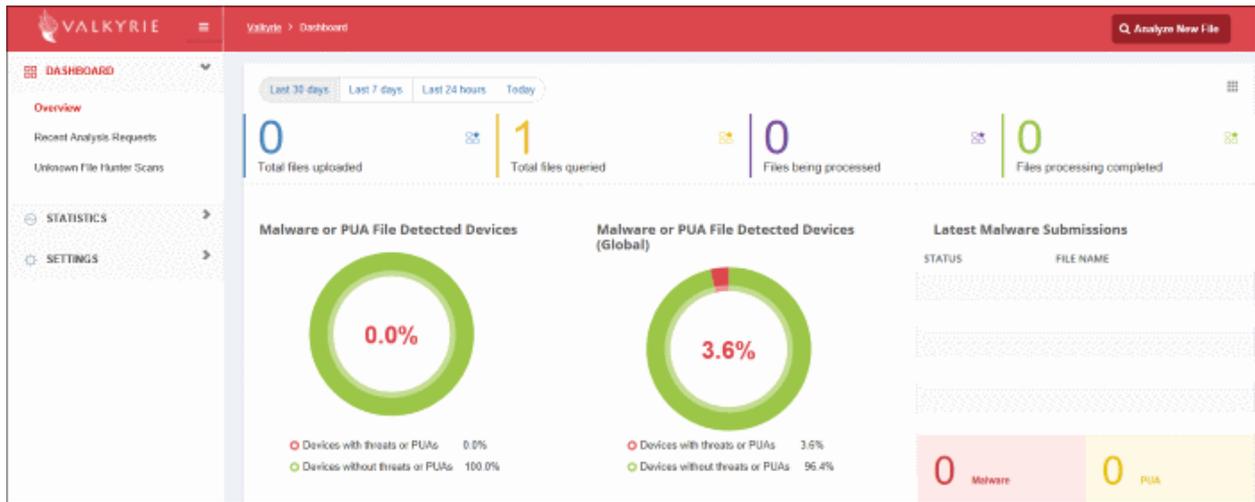
- Click the computer with file icon on the right



- Click the '+' beside a file to view the number of instances and the path of the file on the endpoint(s)

Valkyrie is an online file verdict service which analyzes the behavior of unknown files with a range of static and dynamic tests. Unknown files are automatically submitted to Valkyrie.

- Click 'Detailed Scan Results' to view verdicts on unknown files.
- Existing users can login by entering their Comodo username/password, or you can create an account.
- Valkyrie results will be shown in the UFH interface and, in more detail, in the Valkyrie portal:

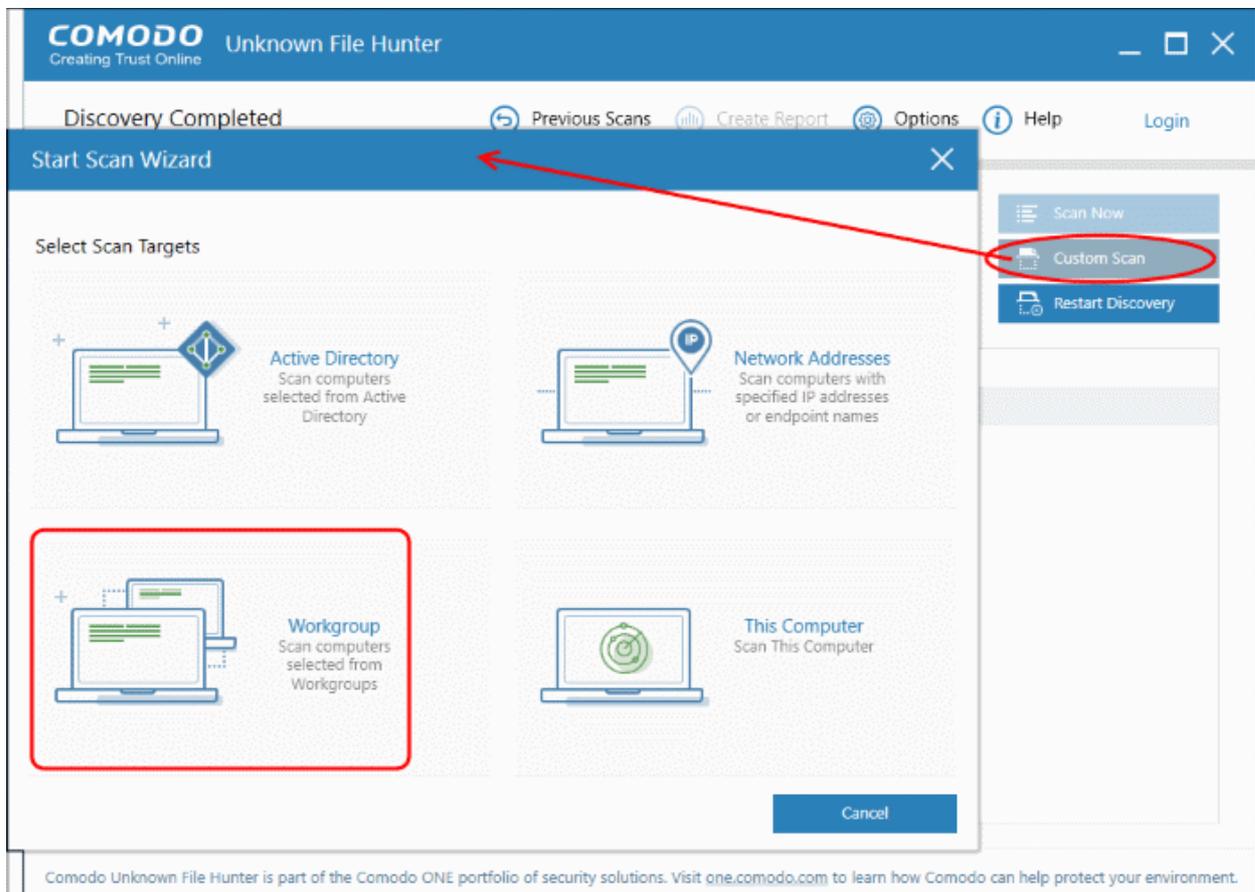


See 'Valkyrie Analysis Results' in 'Scan Results' for more details.

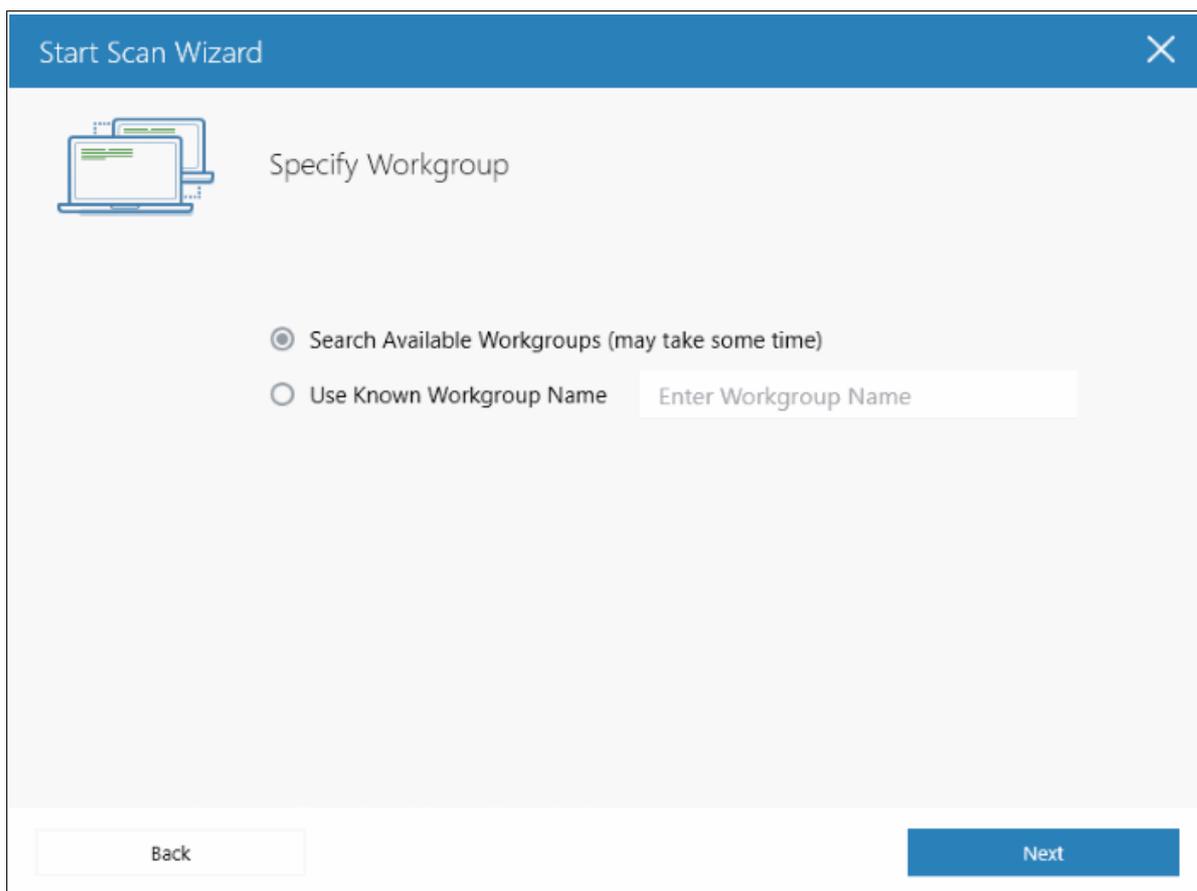
## 3.2 Scan Computers by Workgroup

To scan all or selected computers in a Workgroup:

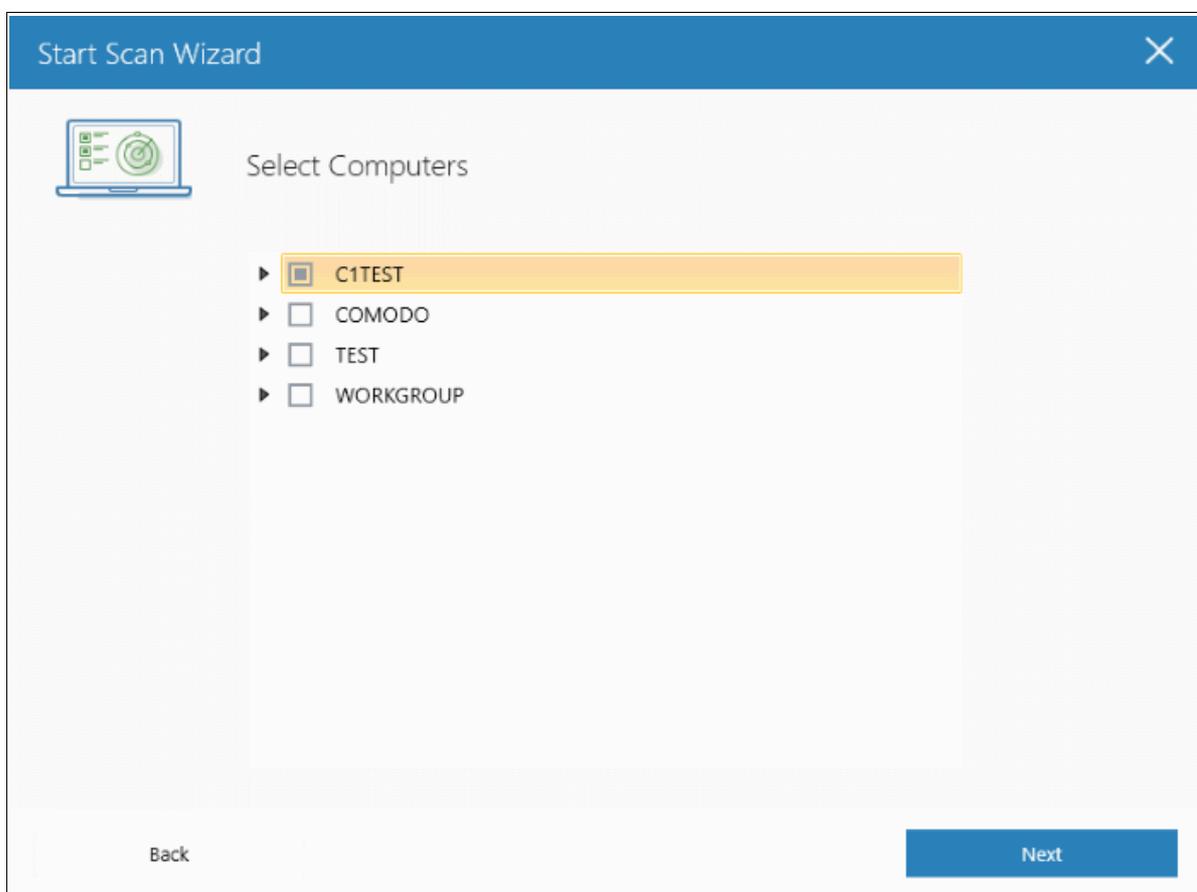
- Click the 'Custom Scan' \ 'New Custom Scan' button
- Click 'Workgroup':



- Select the workgroup you want to scan. You can search for a group or enter a group name directly:



- Next, select the endpoints you want to scan then choose a scan type:



- Enter the administrator's credentials

Start Scan Wizard

Scan Credentials

Login

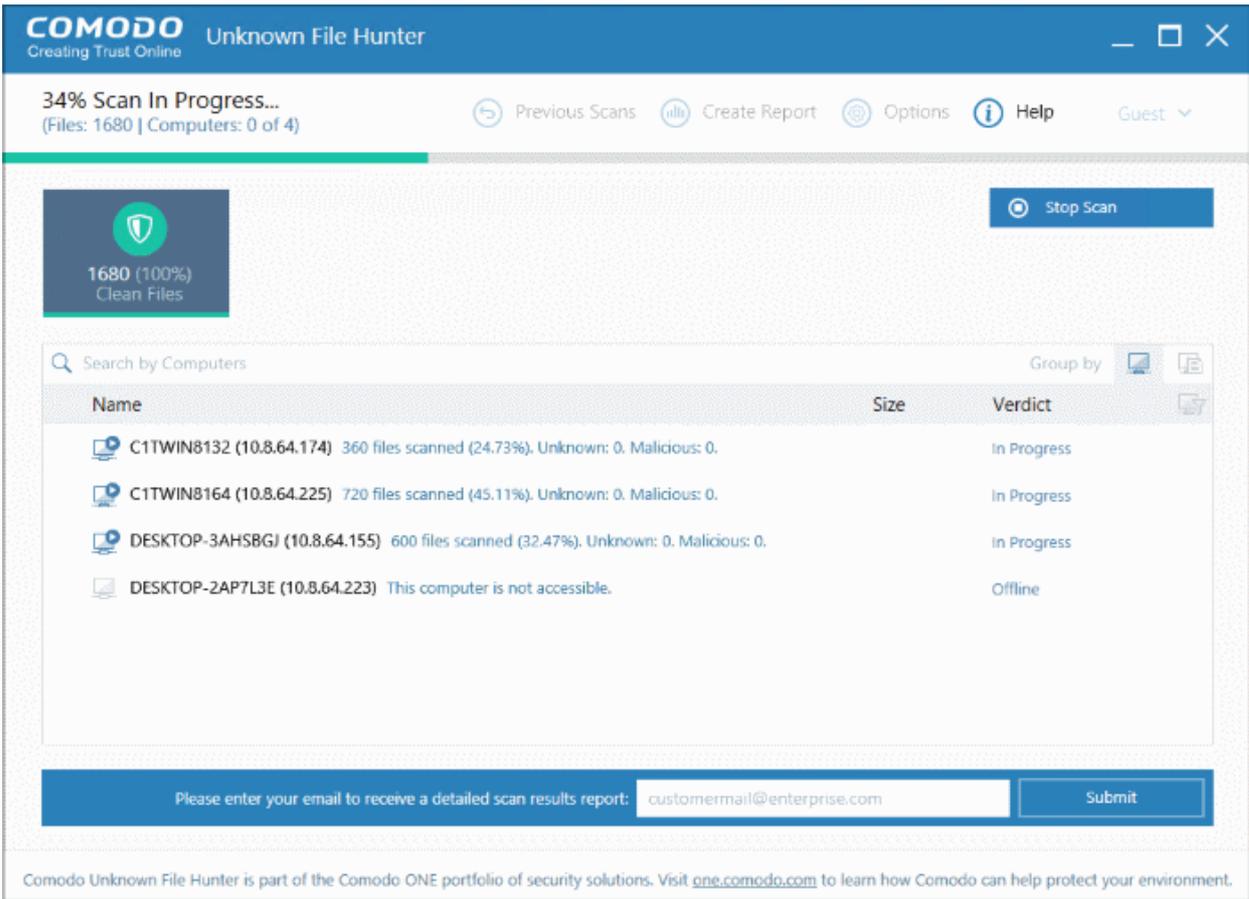
Password

Back Quick Scan Full 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 start after the login credentials have been verified:



The screenshot displays the Comodo Unknown File Hunter web interface. At the top, the status bar shows "34% Scan In Progress..." with "Files: 1680 | Computers: 0 of 4". Navigation links include "Previous Scans", "Create Report", "Options", "Help", and a user profile "Guest". A progress indicator shows "1680 (100%) Clean Files" and a "Stop Scan" button.

The main content area features a search bar "Search by Computers" and a table of scan results. The table has columns for "Name", "Size", and "Verdict".

Name	Size	Verdict
C1TWIN8132 (10.8.64.174) 360 files scanned (24.73%). Unknown: 0. Malicious: 0.		In Progress
C1TWIN8164 (10.8.64.225) 720 files scanned (45.11%). Unknown: 0. Malicious: 0.		In Progress
DESKTOP-3AHSBGJ (10.8.64.155) 600 files scanned (32.47%). Unknown: 0. Malicious: 0.		In Progress
DESKTOP-2AP7L3E (10.8.64.223) This computer is not accessible.		Offline

At the bottom, there is a form to "Please enter your email to receive a detailed scan results report:" with the email address "customermail@enterprise.com" and a "Submit" button.

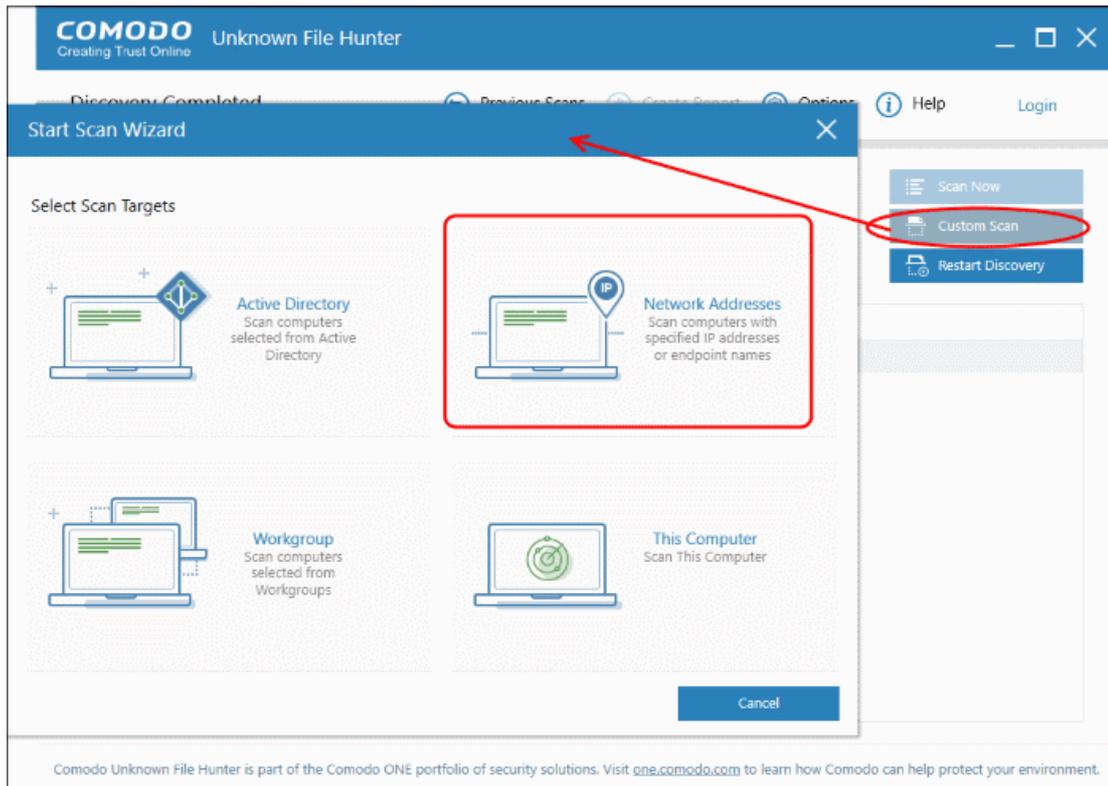
Footer text: "Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit [one.comodo.com](http://one.comodo.com) to learn how Comodo can help protect your environment."

The remainder of the process is the same as for scanning an Active Directory domain. [Click here](#) for details about the rest of the process.

### 3.3 Scan Computers by Network Addresses

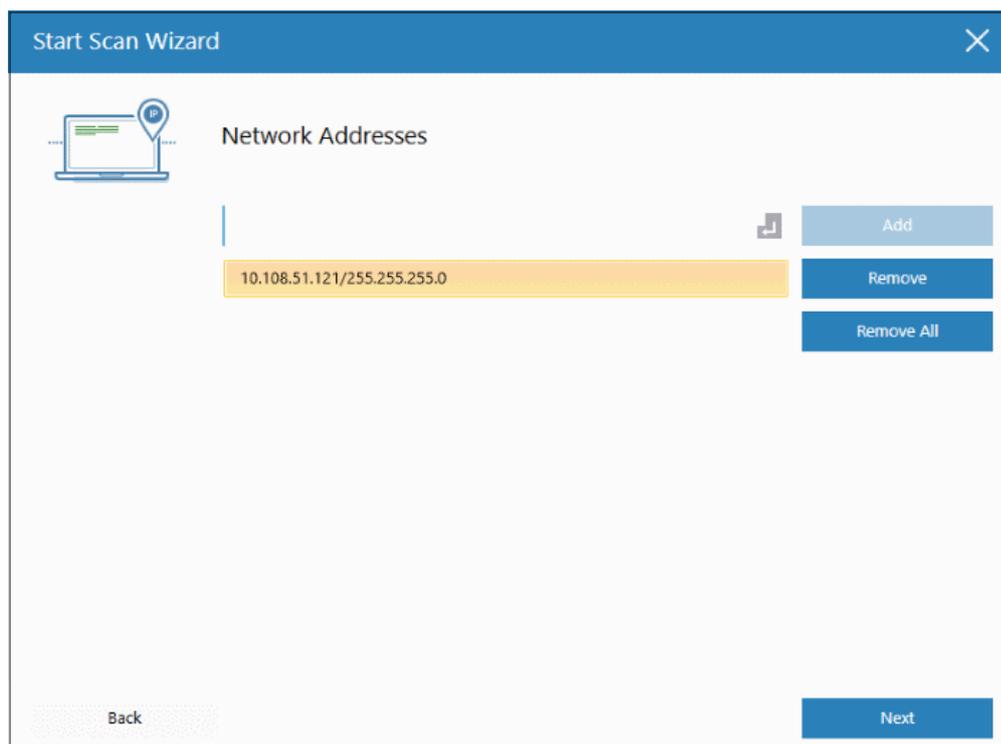
To scan computers by specifying their IP address or hostname:

- Click the 'Custom Scan' button
- Click 'Network Addresses'

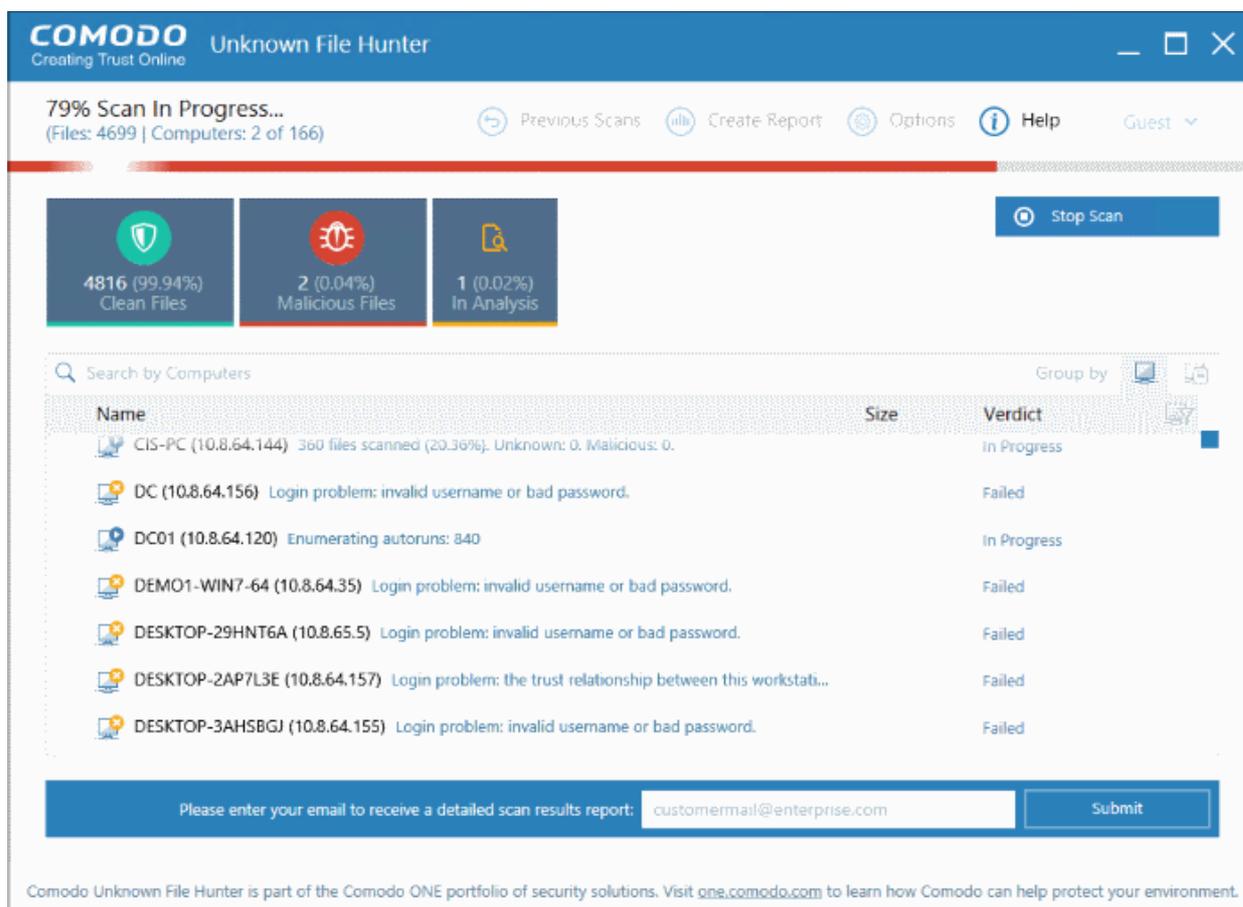


Next, enter the addresses you want to scan. You can add addresses in the following format:

- IP address - 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
- Host Name – e.g., 'Home Computer'



- Click the 'Add' button to register the item for the scan.
- Repeat the process to add more addresses/host-names.
- Click 'Remove' to delete an item.
- 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.

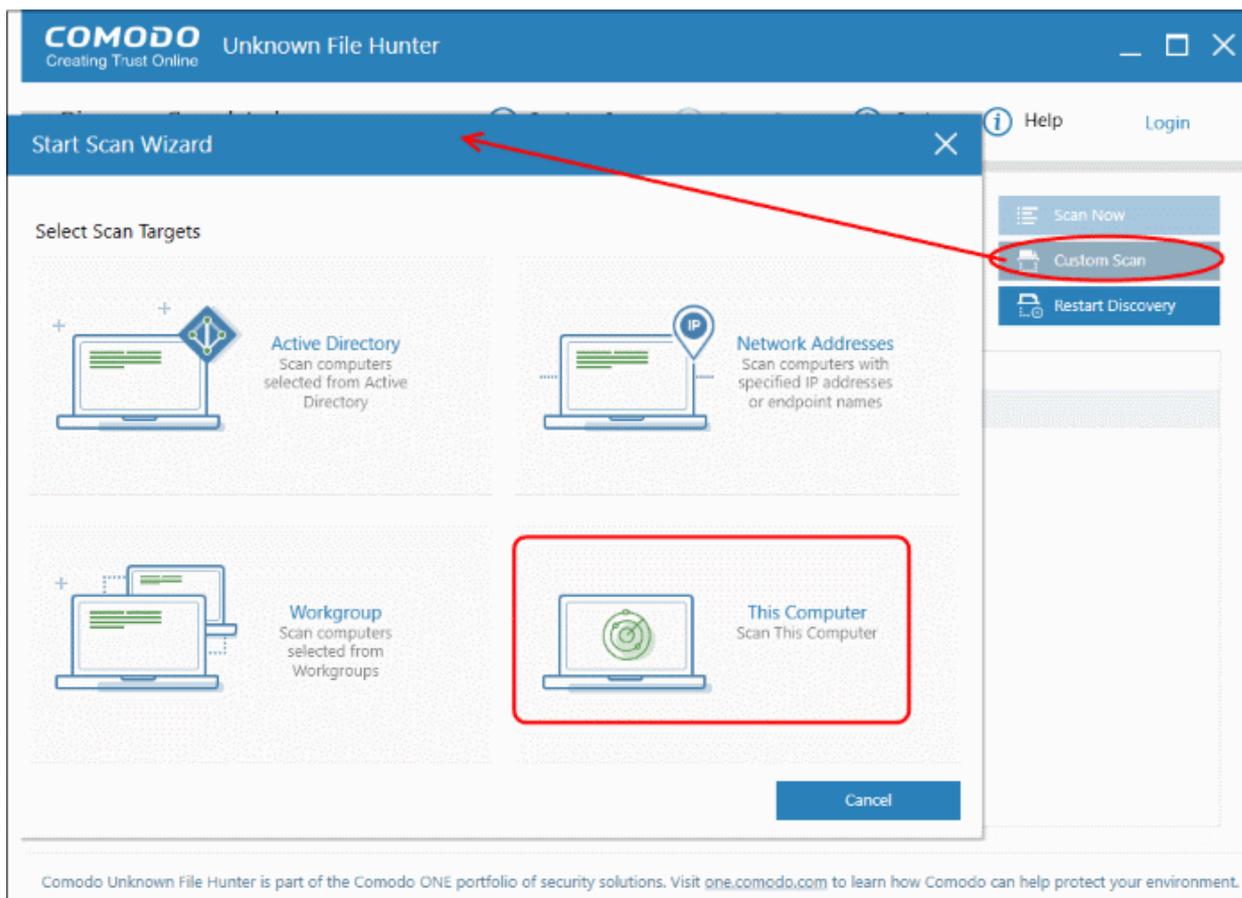


The remainder of the process is the same as for scanning an Active Directory domain. [Click here](#) for details about the rest of the process.

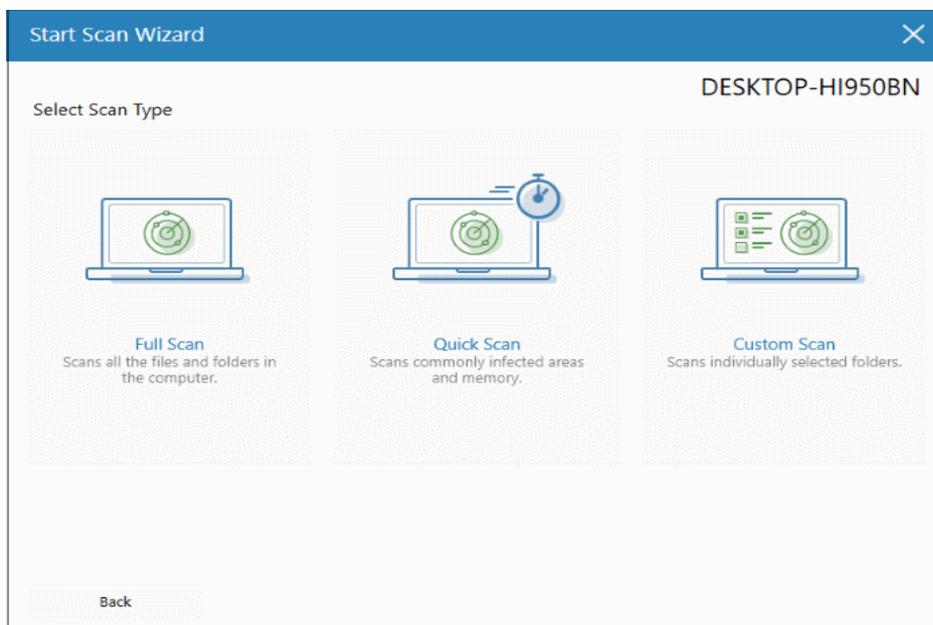
## 3.4 Scan Local Computer

To scan the computer you are currently using:

- Click the 'Custom Scan' button
- Click 'This computer':



- Choose the type of scan you want to run:

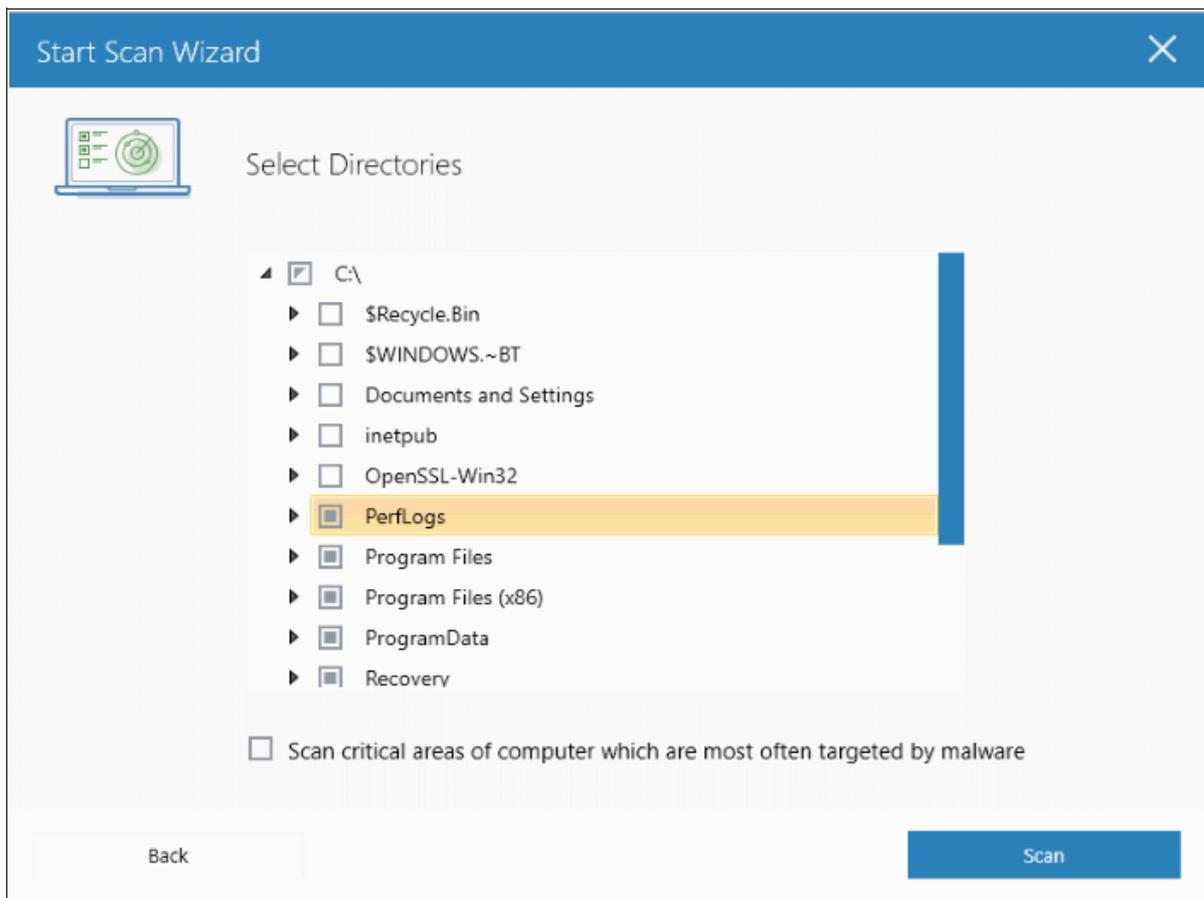


**Quick Scan:** Scan critical and commonly infected areas on the local computer

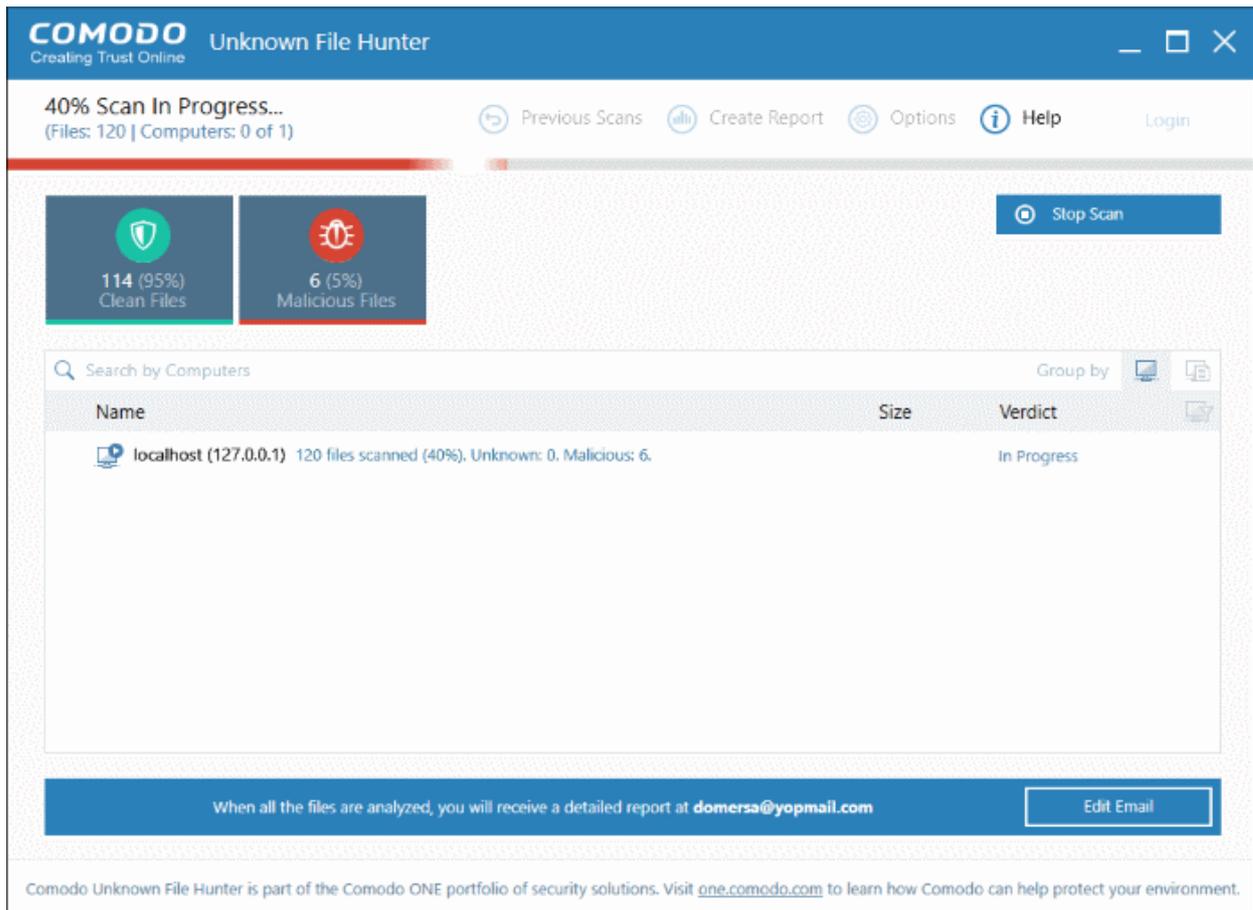
**Full Scan:** Scan all files and folders on on the local computer

**Custom Scan:** Scan selected files or folders on the local computer

- Quick scans and full scans will begin immediately.
- For a 'Custom Scan', you need to choose the directories and files you want to scan:



- 'Scan critical areas...' - If enabled, the scan will cover frequently targeted areas of your computer in addition to the items in your custom scan.
- Click 'Scan' to start the scan.



The remainder of the process is the same as for scanning an Active Directory domain. [Click here](#) for details about the rest of the process.

## 4 Scan Results

### Scan process and scan results:

- Comodo has a huge database of blacklisted and whitelisted files on its File Lookup Server (FLS).
- The UFH scanner first checks the rating of all files on an endpoint against these FLS lists.
- File trust ratings are as follows:
  - Clean – A whitelisted file which is safe to run.
  - Malicious – A blacklisted file which is a known threat / malware.
  - Unknown – There is no trust verdict available for this file. The file will be uploaded to Valkyrie.
- Valkyrie is Comodo's **file analysis** and verdicting service. The service inspects unknown files with a battery of dynamic and static tests in order to establish the file's trust rating. Files may also undergo further testing by human experts.
- After analysis, the previously unknown files are rated as 'Clean' or 'Malicious' and the results passed back to UFH.
  - Click 'Current Scan' / 'Previous' scans to browse scan results.
  - Click 'Detailed Scan Results' to view full test results on the Valkyrie website. You will need to login at <https://valkyrie.comodo.com> with your Comodo account username and password.

**COMODO** Unknown File Hunter  
Creating Trust Online

Scan Completed  
(Files: 34795 | Computers: 1 of 1)

Previous Scans Create Report Options Help Login

34781 (99.96%) Clean Files | 8 (0.02%) Malicious Files | 6 (0.02%) Unknown Files

New Custom Scan  
Detailed Scan Results  
Start Discovery

Search by Computers Group by

Name	Size	Verdict
localhost (127.0.0.1) Completed: Total files scanned: 34796, Unknown: 6, Malicious: 8.		Completed
C:\ProgramData\SpeedBit\DAPI\Plugins\189AE673-13C1-4133-A470-8C4DDD1AC88C\1.0.1...	12 KB	Clean
C:\Program Files\WindowsApps\Shared\limitedTime\InfusedApps\Packages\Microsoft.Win...	269 KB	Clean
C:\Windows\InfusedApps\Packages\microsoft.windowscommunicationsapps_17.8241.4127...	44 KB	Clean
C:\Windows\InfusedApps\Packages\Microsoft.XboxSpeechToTextOverlay_1.17.29001.0_x64...	550 KB	Clean
C:\Windows\InfusedApps\Packages\Microsoft.BingNews_4.3.193.0_x86_8wekyb3d8bbwe...	8 MB	Clean
C:\Windows\InfusedApps\Packages\Microsoft.WindowsCamera_2017.727.20.0_x64_8weky...	105 KB	Clean
C:\Program Files\WindowsApps\Shared\limitedTime\microsoft.windowscommunicationsap...	10 KB	Clean

When all the files are analyzed, you will receive a detailed report at [domersa@yopmail.com](mailto:domersa@yopmail.com) [Edit Email](#)

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

Click the following links for more details on UFH scan results:

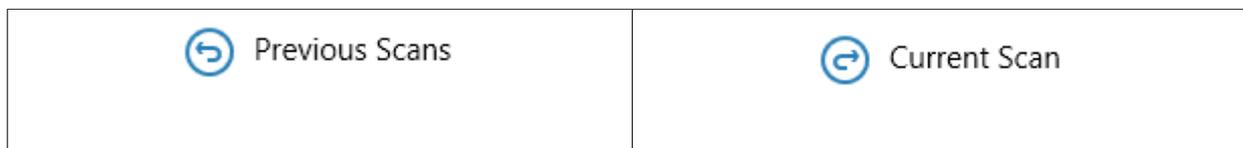
- [Comodo Unknown File Hunter Scan Results](#)
- [Valkyrie Analysis Results](#)

## 4.1 Comodo Unknown File Hunter Scan Results

Results are shown in the UFH interface as soon as the scan finishes.

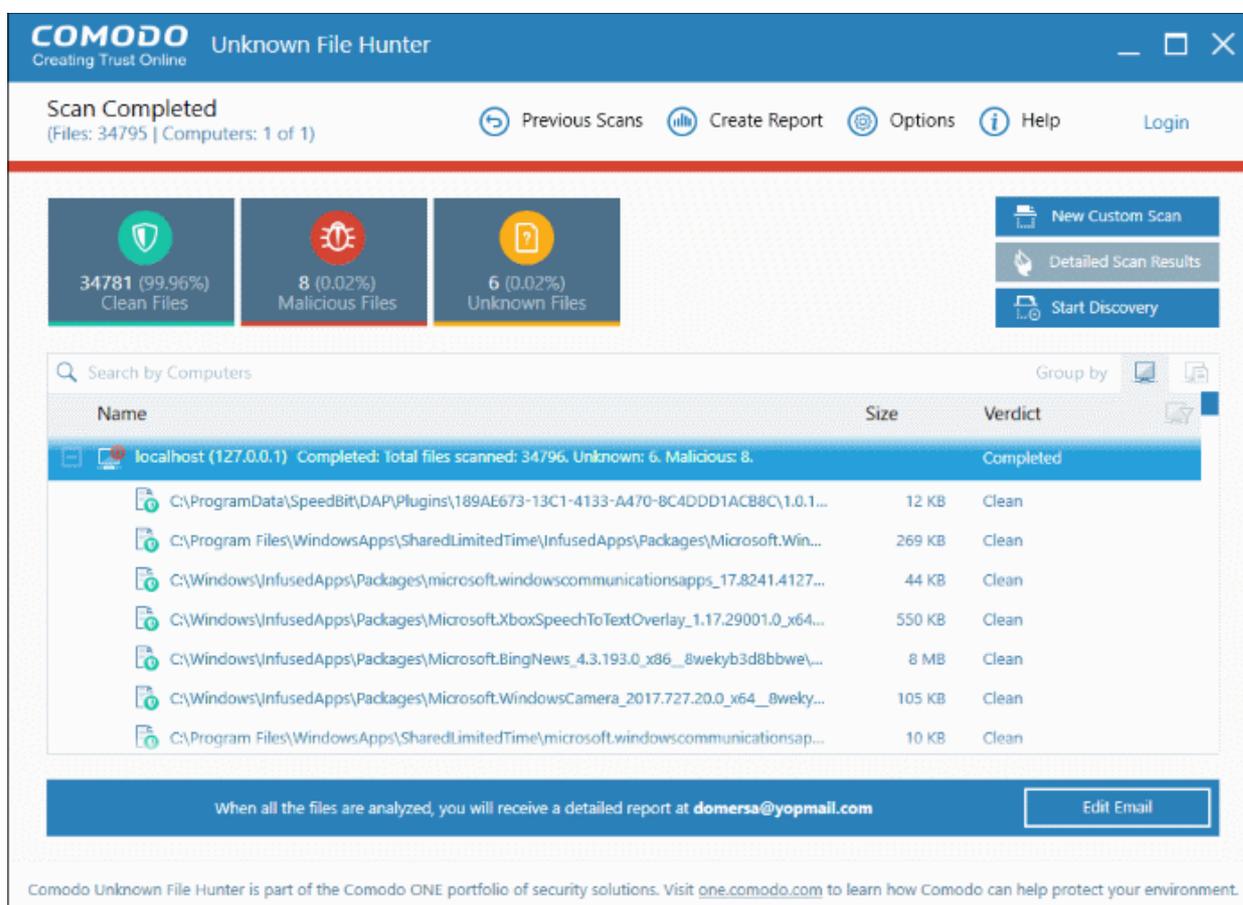
- **Current Scan interface** – Full results of the most recent scan.
- **Previous Scan interface** – A list of all previously run scans. Expand any scan to view per-endpoint results.

Click 'Previous Scans'/'Current Scan' to switch between the two interfaces:



### Current Scan Results

- Click 'Current Scan' at the top to view the results of the most recent scan:



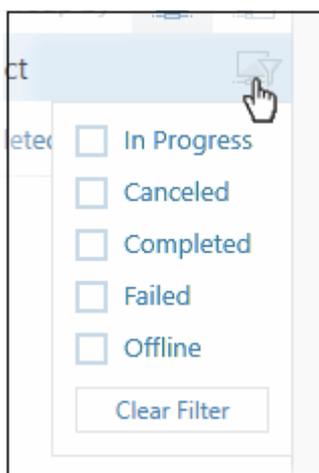
- Click '+' beside a hostname to view all files analyzed on the endpoint. Double-click on any file to view file details.
- The tiles above the results table show the total number of unknown, malicious and clean files.
  - 'Unknown' means no trust rating is available for the file. After expert analysis these will be categorized as either 'Safe' or 'Malicious'.

Current Scan Results Interface - Table of Column Descriptions	
Column Header	Description
Name	The name of the computer on which the scan was run. Click '+' to view the full path of the

	file.
Size	The size of the analyzed file.
Verdict	<p>The trust rating of the file. The possible values are:</p> <ul style="list-style-type: none"> <li>Completed – Unknown file which has been successfully uploaded to Valkyrie for analysis.</li> <li>In Analysis – Unknown file which is currently being tested by Valkyrie</li> <li>Clean – Files found to be safe after Valkyrie analysis</li> <li>Malicious – Files found to be unsafe after FLS and Valkyrie analysis</li> <li>No Threat Found - No malicious intent was found by Valkyrie's automated tests but the file has been passed onto human experts for further analysis. These files are listed as 'Unknown' in the tiles above the table. They will be classified as either 'Clean' or 'Malicious' after the human analysis concludes.</li> </ul>

## Searching, sorting and filtering Options

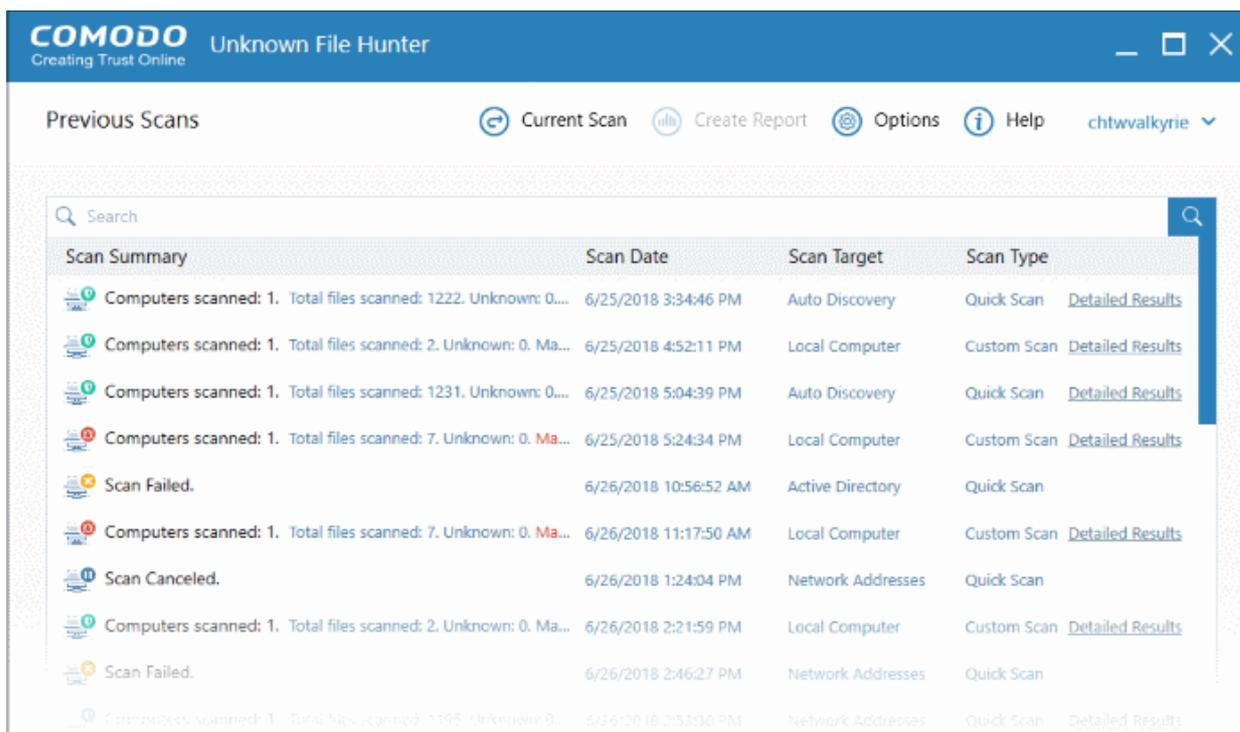
- Use the search box to look for endpoints by name or IP address. Clear the search box to display all endpoints again.
- Click the column headers to sort results by name, size and verdict.
- Click the funnel icon at the end of 'Name' column to choose result filters:



## Previous Scans Results

- Click 'Previous Scans' at the top

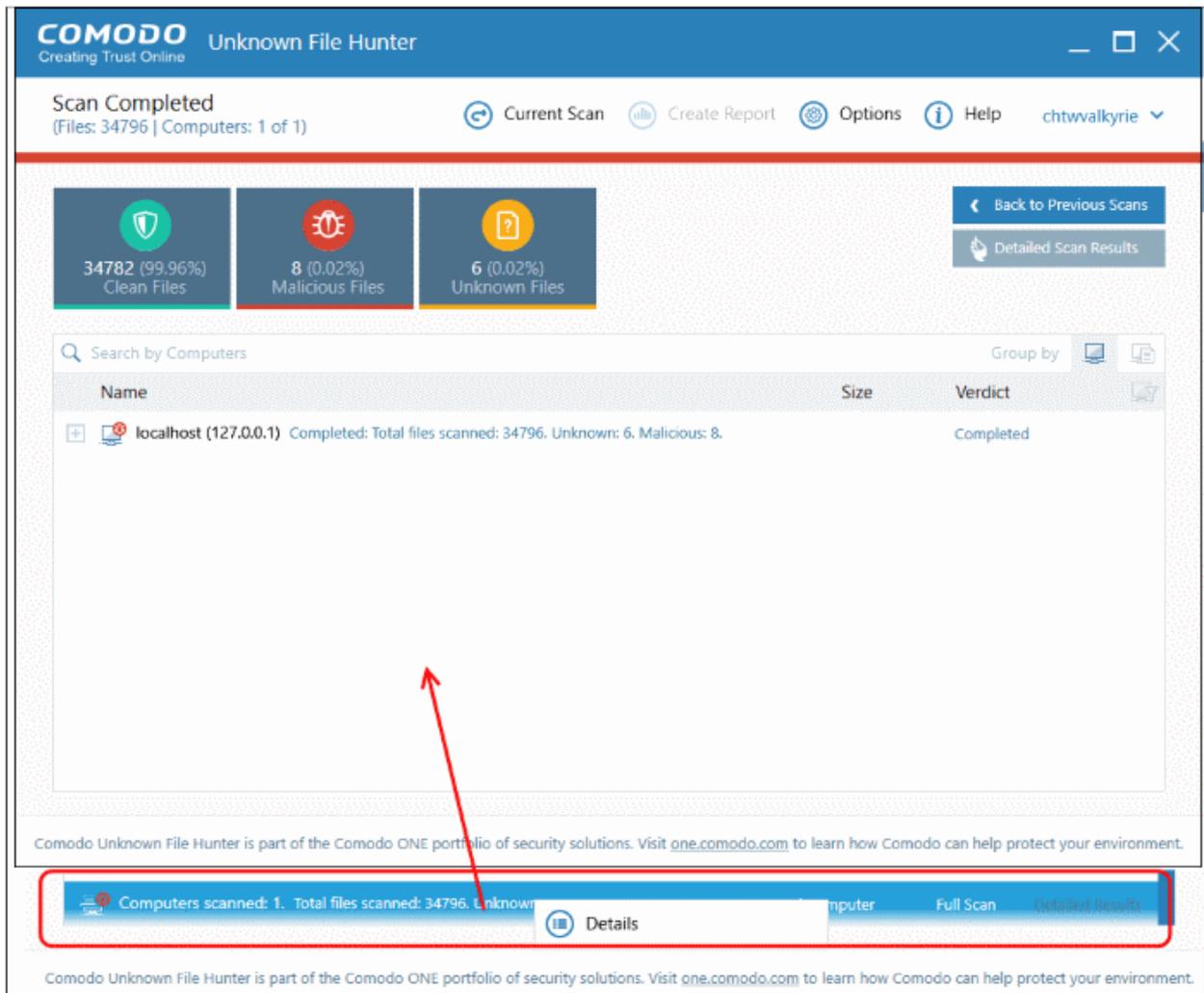
The results of the previous scans will be shown:



**Previous Scan Results Interface - Table of Column Descriptions**

Column Header	Description
Scan Summary	<p>Indicates the status of scans.</p> <ul style="list-style-type: none"> <li>Scan Failed – The scan was unsuccessful.</li> <li>Scan Canceled – The scan was canceled by the admin.</li> <li>Computer scanned – The number beside it indicates the number of endpoints that were scanned for that scan.</li> </ul>
Scan Date	The date and time the scan was run.
Scan Target	<p>Indicates the type of scan:</p> <ul style="list-style-type: none"> <li>Auto Discovery – Scan run on discovered endpoints on the network</li> <li>Active Directory – Scan run on endpoints which belong to an Active Directory domain</li> <li>Network Addresses – Scan executed by specifying their host name/IP address, or scan all endpoints on an IP range</li> <li>Local Computer – Scan run on the local device</li> </ul>
Scan Type	Indicates whether it is a quick or full scan
Detailed Results	Click this link to open <a href="https://valkyrie.comodo.com">https://valkyrie.comodo.com</a> with full details of Valkyrie results. See 'Valkyrie Analysis Results' for more information.

- Double-click a scan or right-click then 'Details' to open the scan details interface



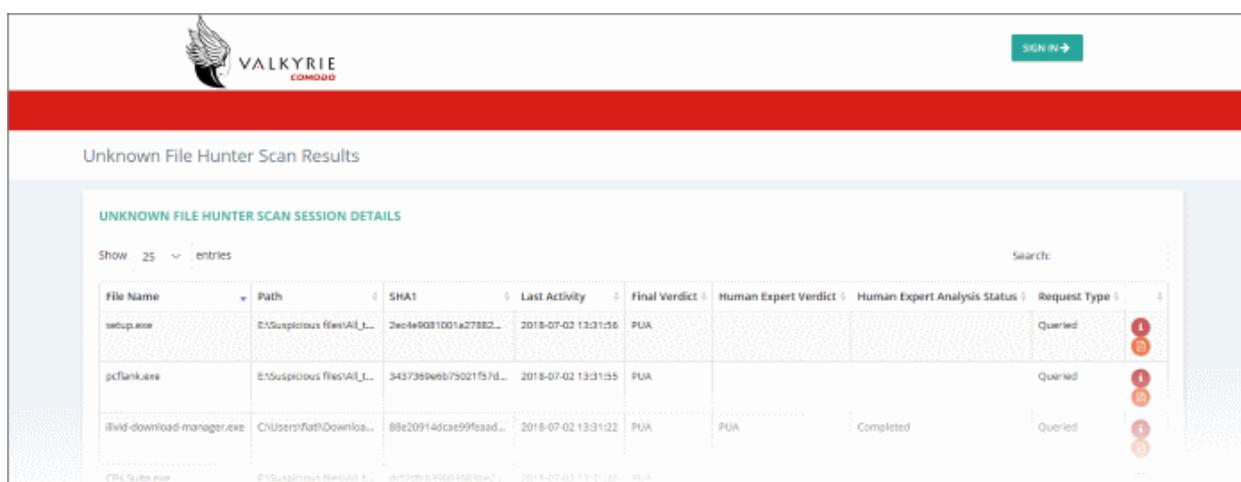
The interface is similar to current scan results explained above.

- Click 'Detailed Scan Results' button to view full results at <https://valkyrie.comodo.com> . See '**Valkyrie Analysis Results**' for more information.
- Click 'Back to Previous Scans' to return to 'Previous Scans' screen.

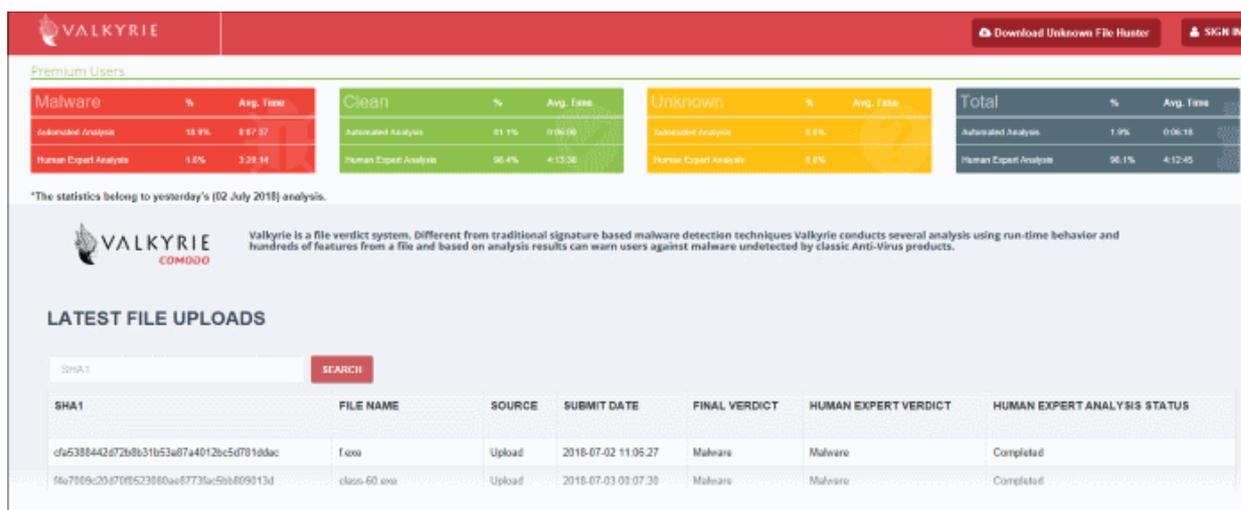
## 4.2 Valkyrie Analysis Results

- Files with a trust rating of 'Unknown' are automatically uploaded to Valkyrie for analysis.
- The service examines each file with a battery of dynamic and static tests in order to establish the file's trust rating. If required, files undergo further analysis by human experts.
- Valkyrie's automated and human tests will ultimately produce a verdict of 'Clean' or 'Malicious' which is returned to the UFH interface.
- You can view overall scan results in the UFH interface.
- Click 'Detailed Scan Results' to login at <https://valkyrie.comodo.com> and view full results of Valkyrie tests on your unknown files.
- You can login with your Comodo, Comodo Dragon or Comodo One username and password.

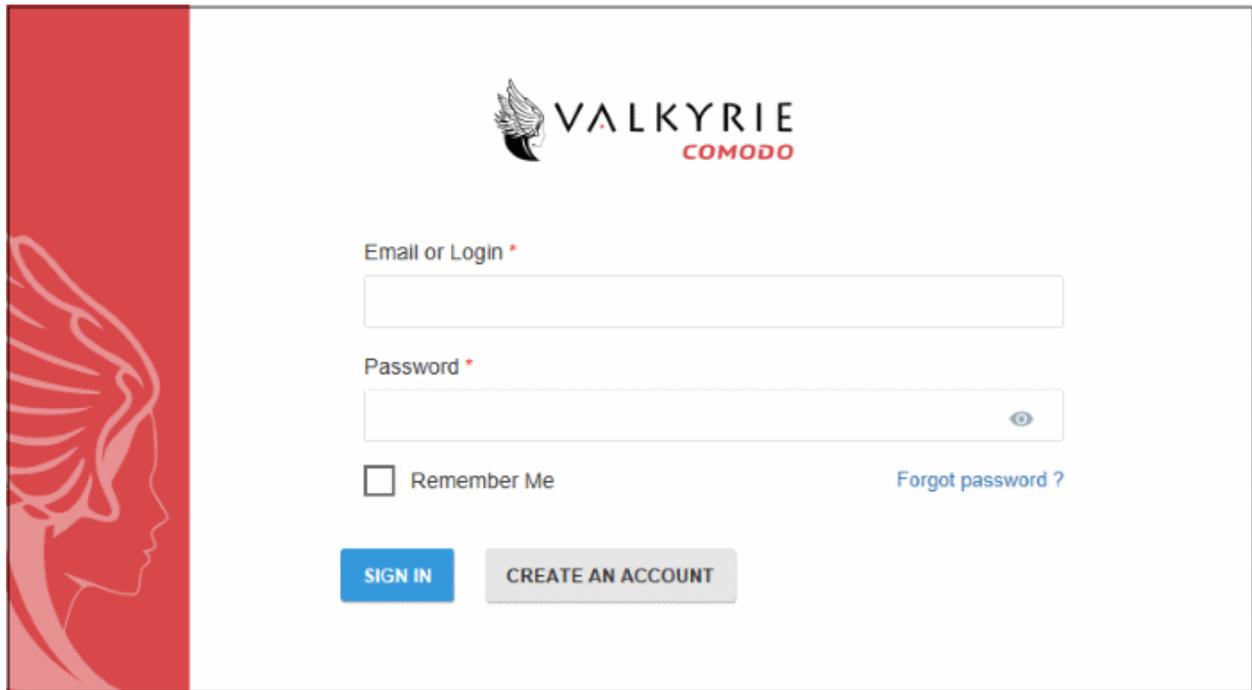
If you have not logged in to your Valkyrie account, the scan results for the clicked item will be shown:



- Click 'Sign in' at the top-right. Valkyrie home page with details of all files uploaded by all customers will be displayed:

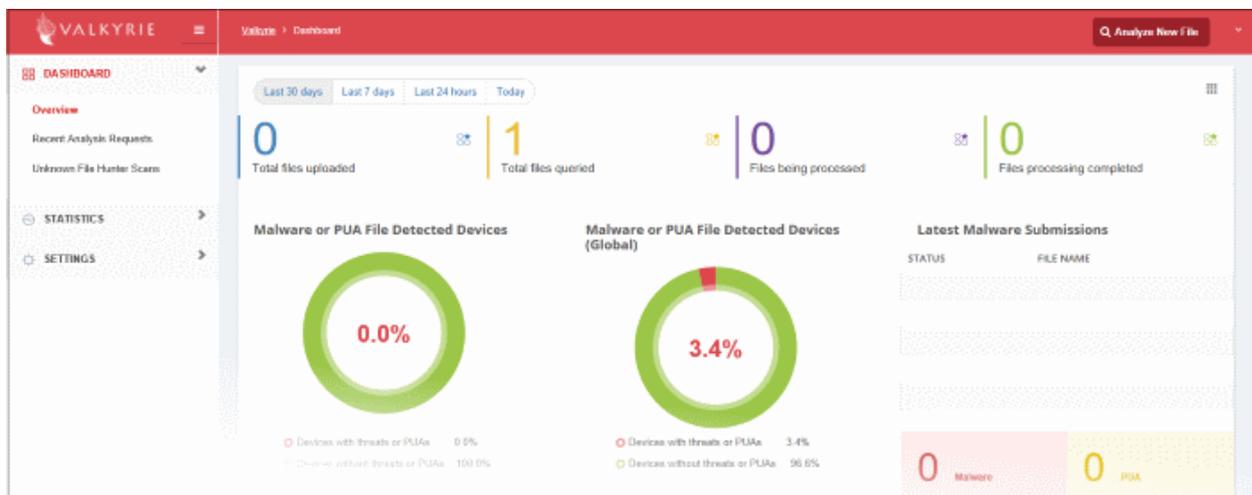


- Click 'Sign in' at the top-right of the Valkyrie home page



- Dragon / Comodo One customers can use their credentials to login.
- 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.

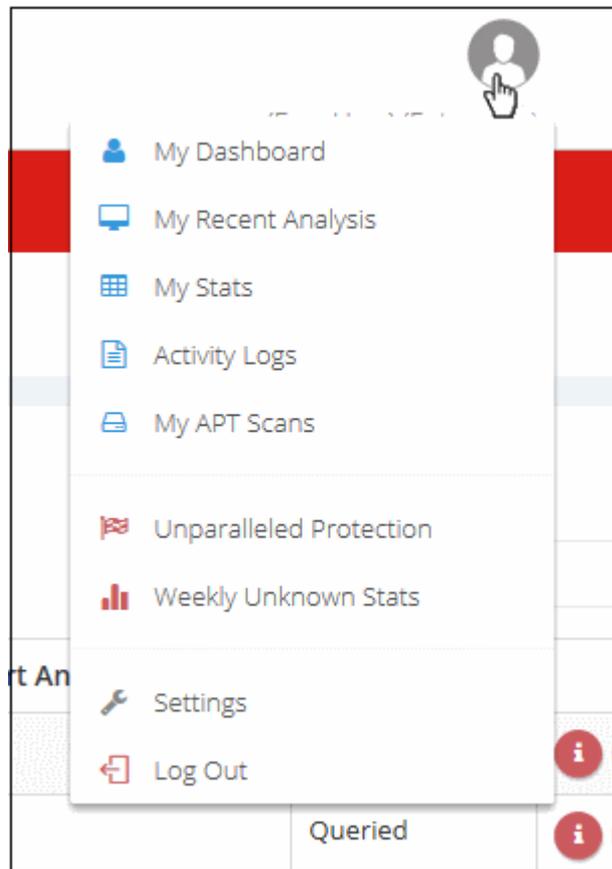
The 'Dashboard' page will be displayed by default.



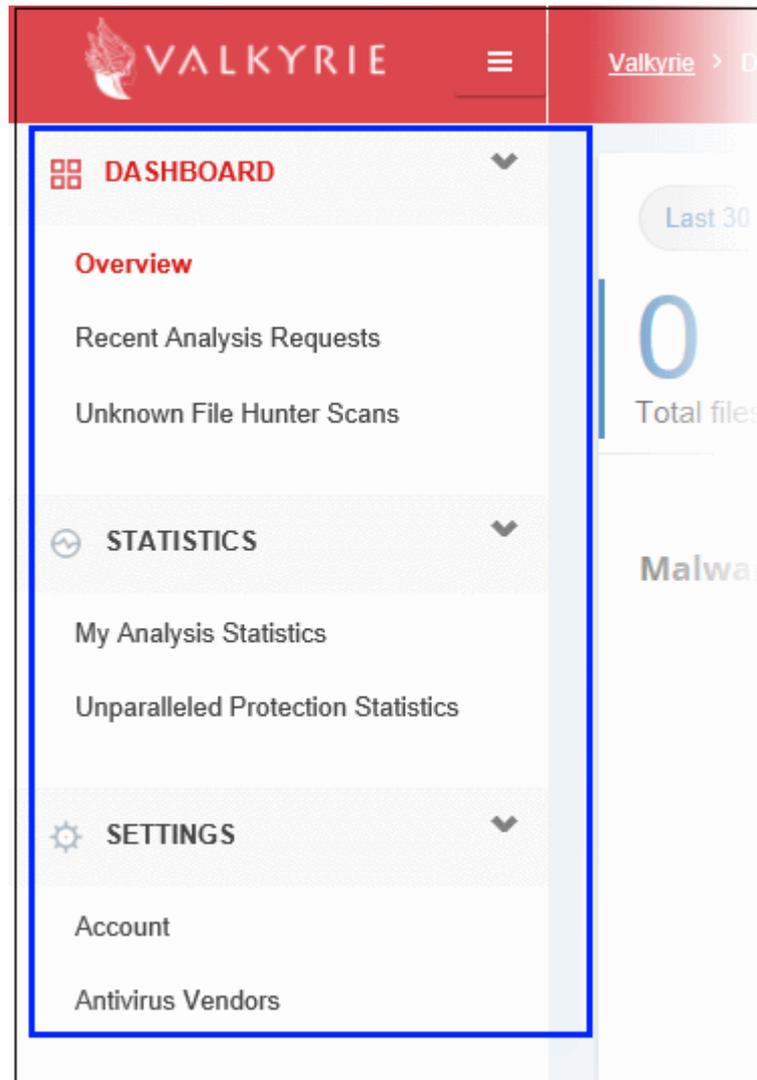
If you are already logged into your Valkyrie account, clicking the 'Detailed Scan Results' in the 'Current Scan' page or 'Detailed Results' link in the 'Previous Scans' page will open the results page of the respective link.

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Request Type
pcfank.exe	E:\Suspicious files\AI_te...	3437369e6b75021f57d...	2018-07-03 14:28:16	PUA			Queried
cpl.exe	E:\Suspicious files\AI_te...	795fe8537ec514f3667...	2018-07-03 14:28:15	PUA			Queried
cpl.dll	E:\Suspicious files\AI_te...	d3be9ebc642f164efb08...	2018-07-03 14:28:14	PUA			Queried
CPLSuite.exe	E:\Suspicious files\AI_te...	dcf2dfcb39003683be2e...	2018-07-03 14:28:13	PUA			Queried
CPL3.dll	E:\Suspicious files\AI_te...	57b72ae6c605290c60f8...	2018-07-03 14:28:13	PUA			Queried
setup.exe	E:\Suspicious files\AI_te...	2wc4e9081001a27882d...	2018-07-03 14:28:12	PUA			Queried

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



Alternatively, you can navigate to different pages from the left side menu of the home page:



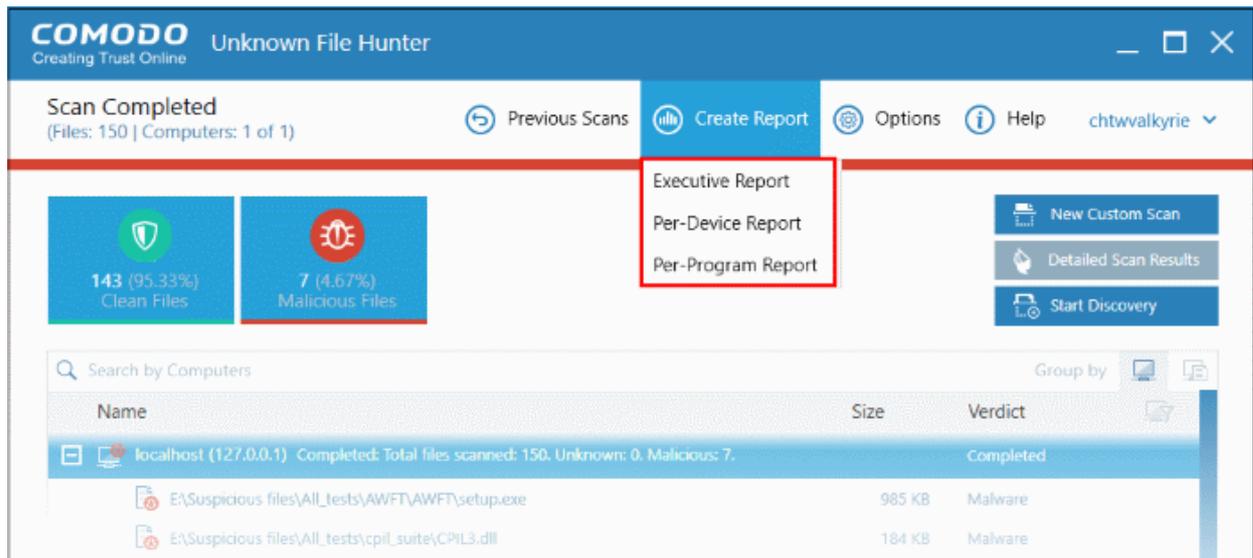
See our dedicated Valkyrie guide at <https://help.comodo.com/topic-397-1-773-9567-Valkyrie-Analysis-Results.html> for more information.

## 5 Reports

Reports are available for each scan you run and are divided into three categories:

- Executive Report - A summary of the scan. Includes details such as the number of devices scanned, the number of unknown programs found and so on
- Per Device Report - Scan results grouped by device.
- Per Program Report – A report with details on each unknown / malicious program. The report also specifies which devices the file was found.

You can generate reports from the 'Create Report' menu



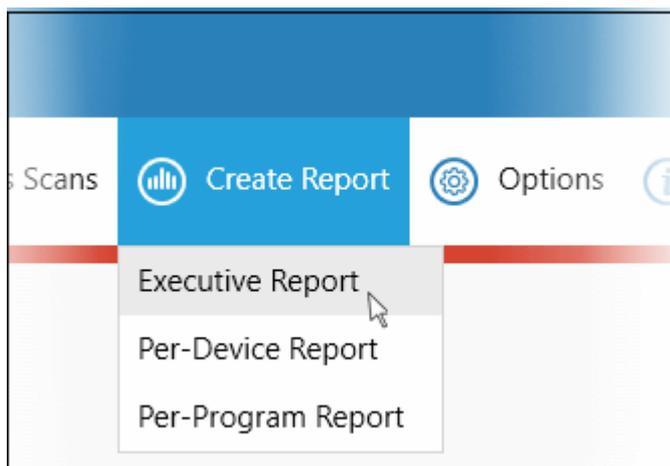
See the following sections for help on each report type:

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

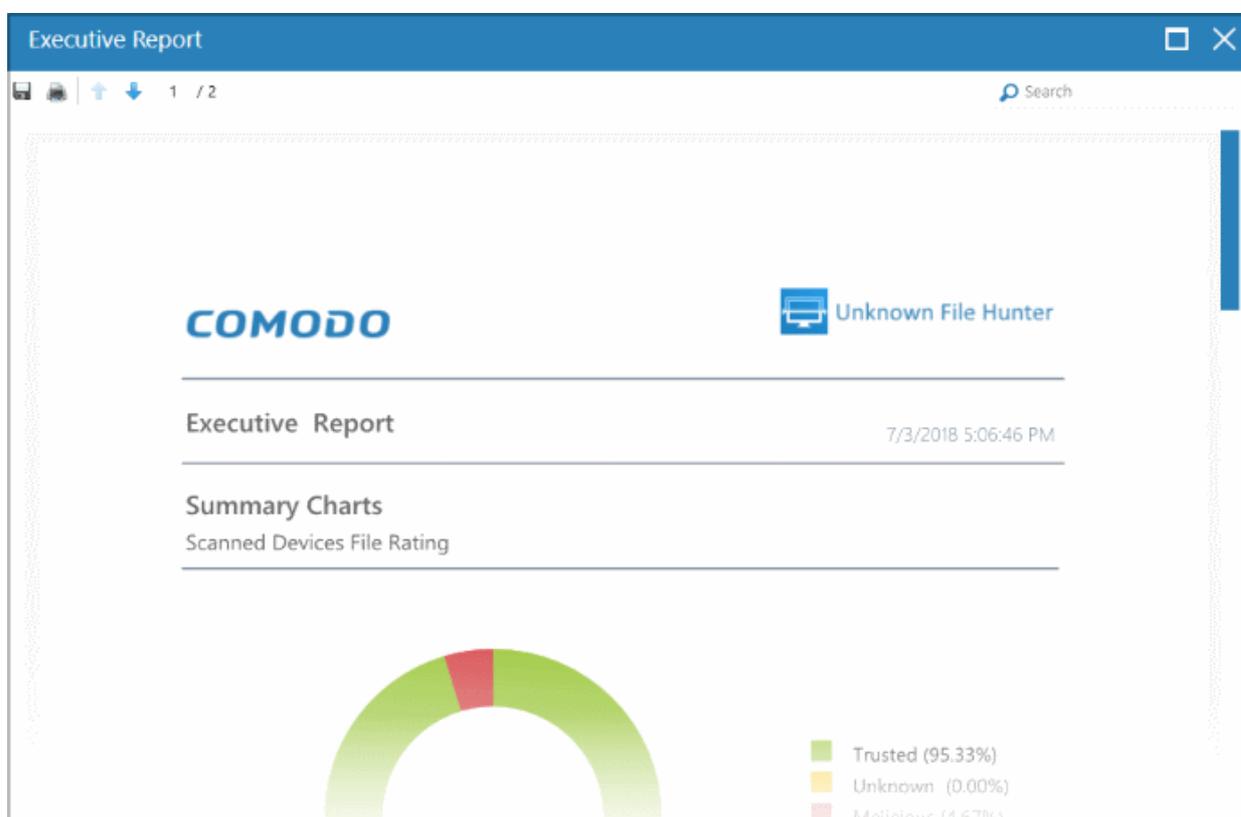
### 5.1 Executive Report

The executive report is a top-level summary of the scan results. Details include scan start/finish times, the number of devices scanned and the trust rating of discovered files.

To generate an 'Executive' report results, click 'Create Reports' and then 'Executive Report'



The report will be generated and displayed:



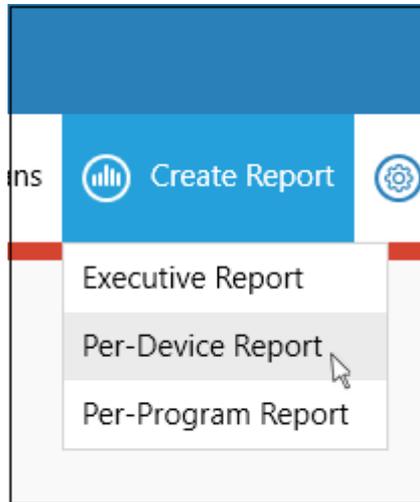
Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **Summary Charts** - Provides the details of programs found on the scanned devices and the rating of the scanned devices.
  - **Scanned Devices File Rating** - Results displayed in pie chart of the programs that were scanned on the devices. Provides the percentage of trusted programs, unknown programs and malware.
  - **Device Assessment** - The statuses of the scanned devices in pie chart providing the percentage of devices that are found safe, infected and at risk.

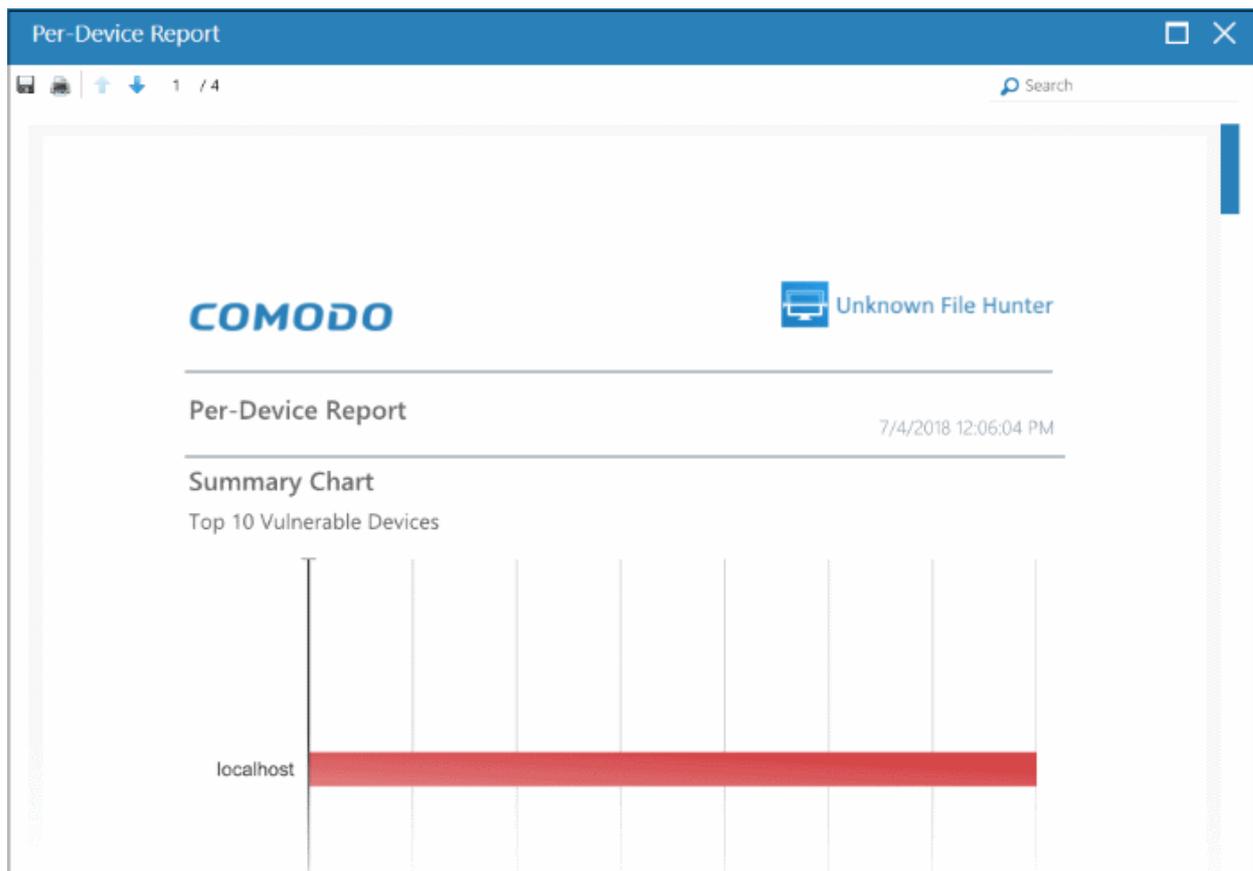
## 5.2 Device Report

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.

To generate a 'Per Device' report, click 'Reports' then 'Per Device Report'



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.

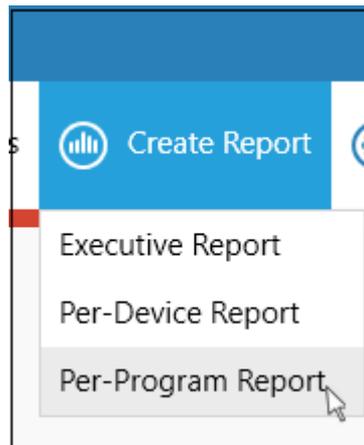
- **Summary Chart** - Provides the details in bar graph the top 10 endpoints that are detected with unknown/malware files.

- **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.
- **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.

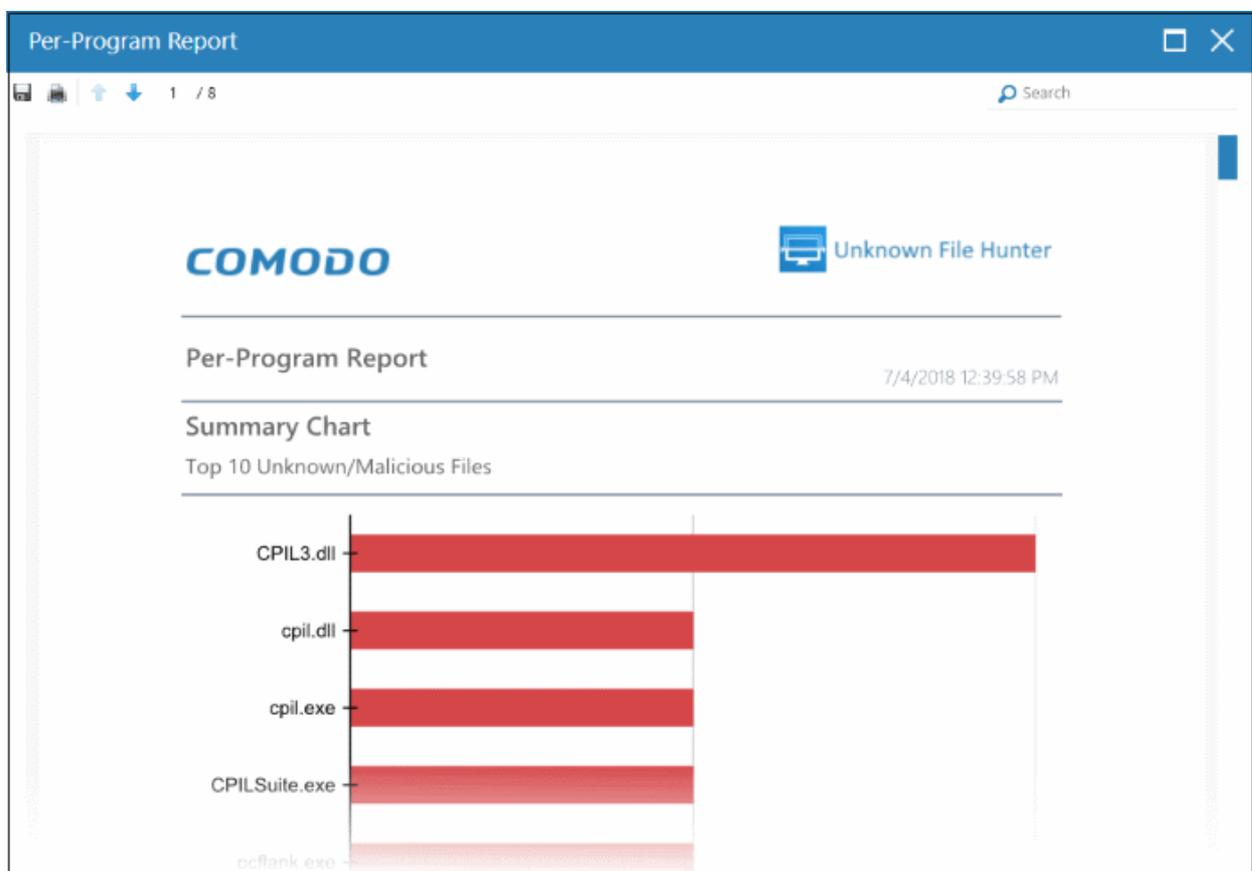
## 5.3 Program Report

The 'Per Program Report' shows scan results grouped by filename. It includes details about each malware/unknown file found, the devices on which they were found, the file path and more.

- Click 'Reports' > 'Per Program Report' to generate a report of this type:



- The report will be generated immediately.
- Click the floppy-disk icon at top-left to save the report in .pdf format (it is not saved automatically).



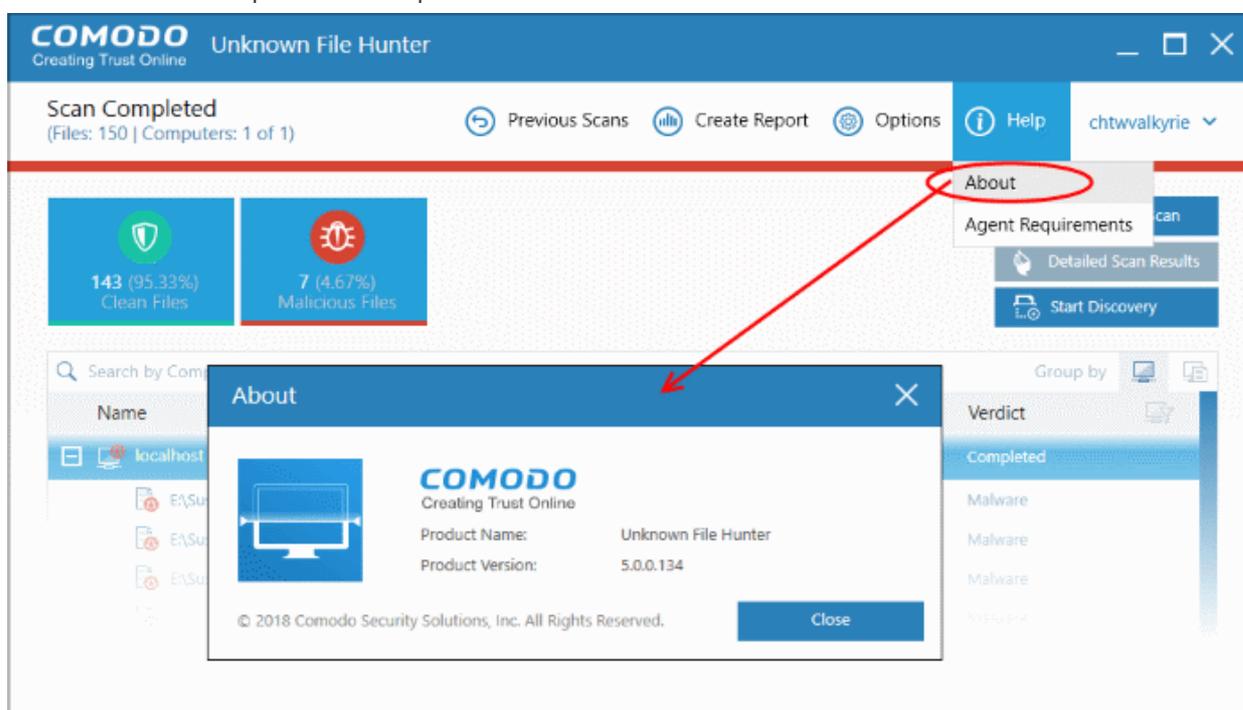
Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **Summary Chart** - The 10 most prevalent unknown and malicious programs on your network
- **Report Summary** - General scan info. Number of devices scanned, date and time of the scan, number of malware/unknown files found etc.
- **Details per Program** - Granular details about each file, including the names of the devices it was found on, IP addresses of the devices and more.

## 6 About Comodo Unknown File Hunter

The 'About' dialog shows product and version information.

- Click 'Help' > 'About' to open the interface:

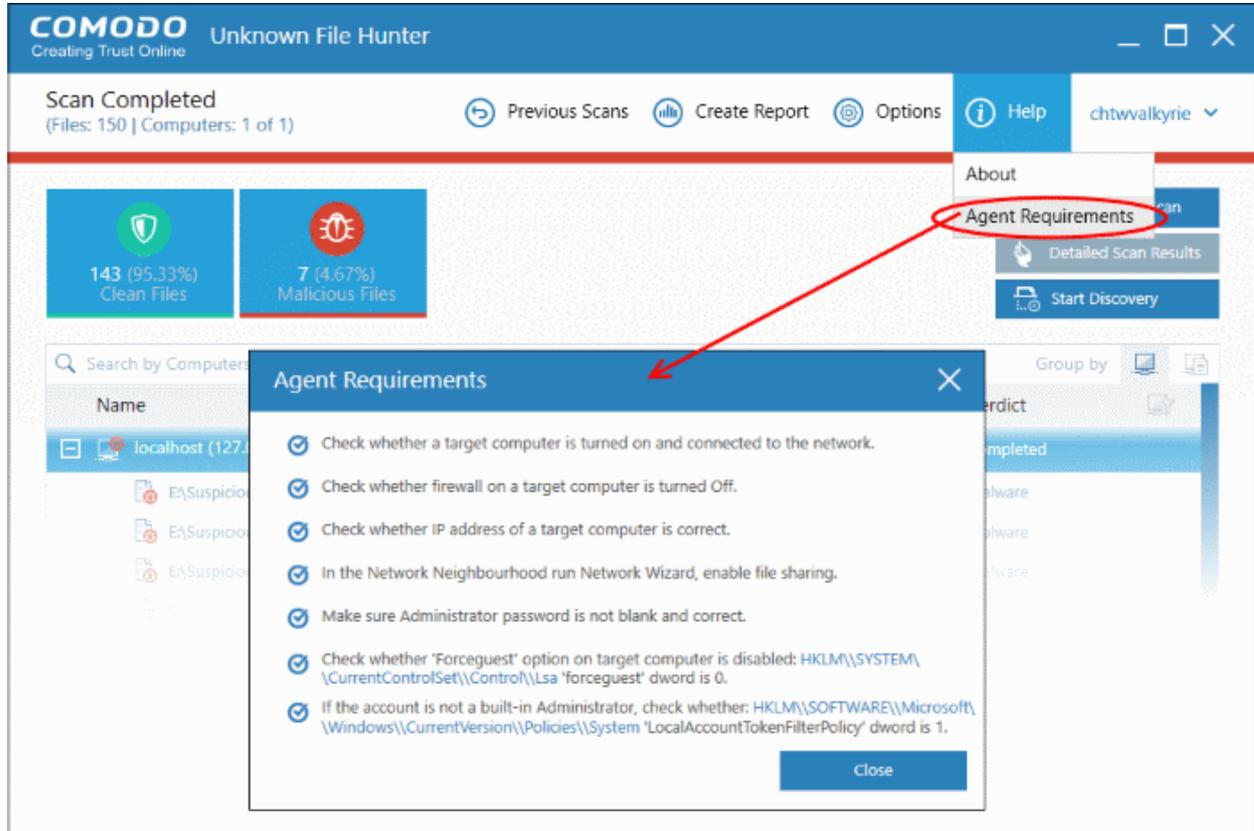


- Product Name - The full name of the product
- Product Version - The version number of the product
- Click the 'Close' button to return to the application.

# 7 Agent Requirements

'Agent Requirements' shows advice to help you run scans successfully.

- Click 'Help' > 'Agent Requirements' to open the interface:



## About Comodo Security Solutions

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

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

## About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.636

Tel : +1.703.581.6361

<https://www.comodo.com>

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