COMODO
Creating Trust Online®

Comodo
Unknown File Hunter

Software Version 5.0

Administrator Guide

Guide Version 5.0.073118

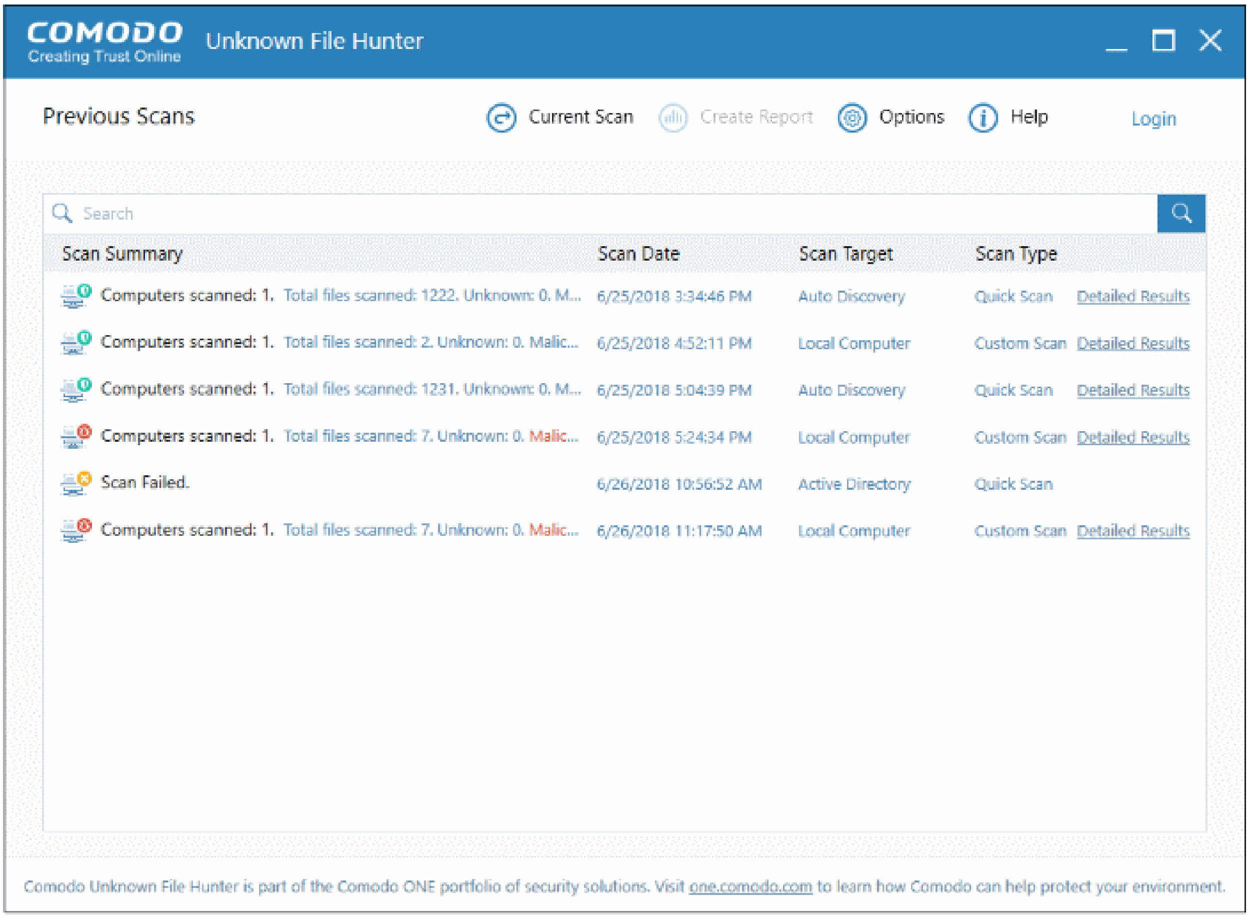
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

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 hidden it can be months before a traditional anti-virus catches up to it. During this time, the threat continues to reside on the victim's computer, executing its payload all the while.

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 and 'Malicious' files will be deleted immediately, it is in the 'unknown' category that most zero-day threats are found. UFH 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.



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	Detailed Results
Computers scanned: 1. Total files scanned: 2. Unknown: 0. Malic...	6/25/2018 4:52:11 PM	Local Computer	Custom Scan	Detailed Results
Computers scanned: 1. Total files scanned: 1231. Unknown: 0. M...	6/25/2018 5:04:39 PM	Auto Discovery	Quick Scan	Detailed Results
Computers scanned: 1. Total files scanned: 7. Unknown: 0. Malic...	6/25/2018 5:24:34 PM	Local Computer	Custom Scan	Detailed Results
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	Detailed Results

Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit 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.

2 Run Unknown File Hunter

Comodo Unknown File Hunter can be downloaded from:

- Comodo One (C1)
- Comodo Valkyrie website

Comodo One

Unknown File Hunter is available for download from your C1 account:

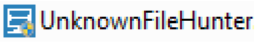
- Login to your C1 account at **https://one.comodo.com/**
- Click 'Tools' > Click 'Download' in the Unknown File Hunter tile
  - You can sign up for a free C1 account at **https://one.comodo.com/**. Creating a C1 account also creates a Valkyrie account for you.
  - You can login to UFH and Valkyrie with your C1 username/password

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**
  - Note - when you create a Valkyrie account, a new C1 account is not created.

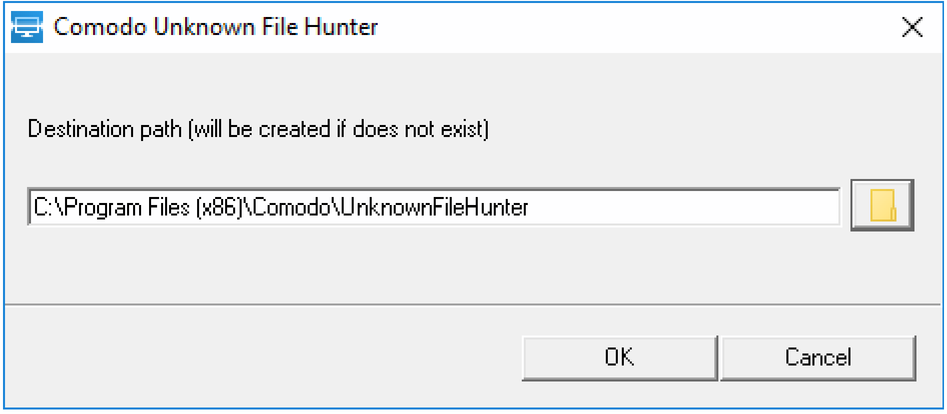
Run Unknown File Hunter

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



UnknownFileHunter

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

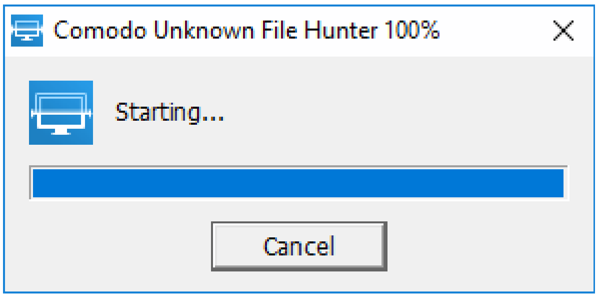


Comodo Unknown File Hunter

Destination path (will be created if does not exist)

C:\Program Files (x86)\Comodo\UnknownFileHunter

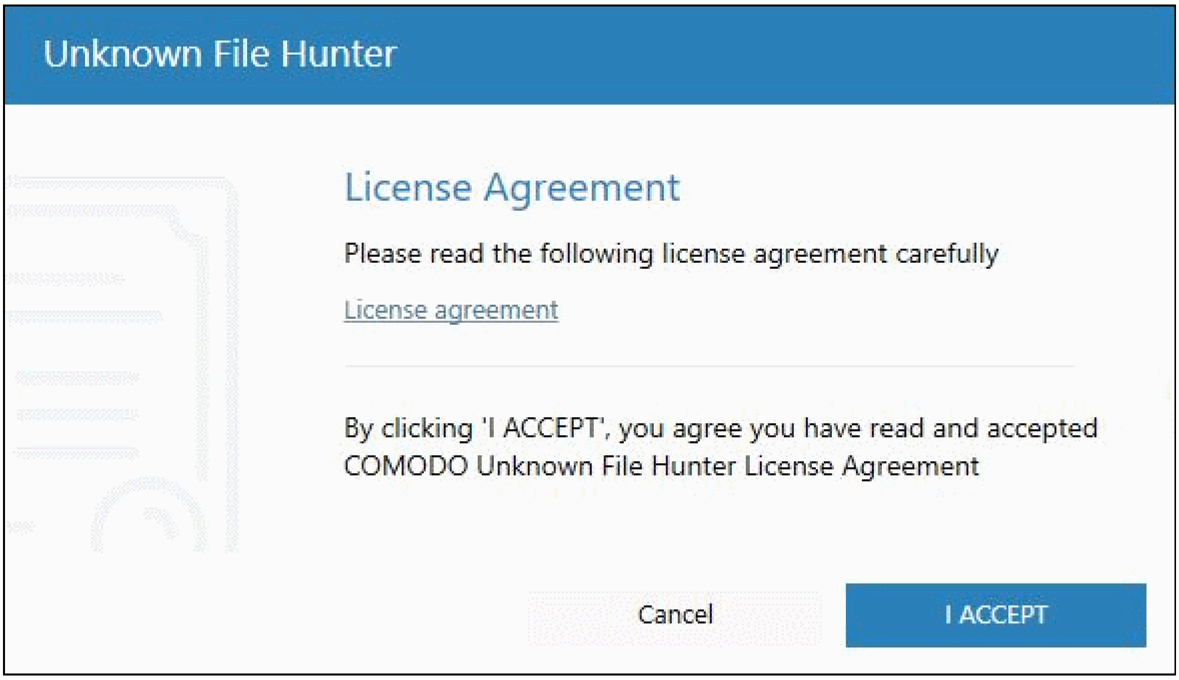
- The default location is C:\Program Files (x86)\Comodo\UnknownFileHunter. Click the folder icon to change the path if required. Note: This dialog will appear each time you run the application and you can choose different locations as you prefer.



Comodo Unknown File Hunter 100%

Starting...

- 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.



Unknown File Hunter

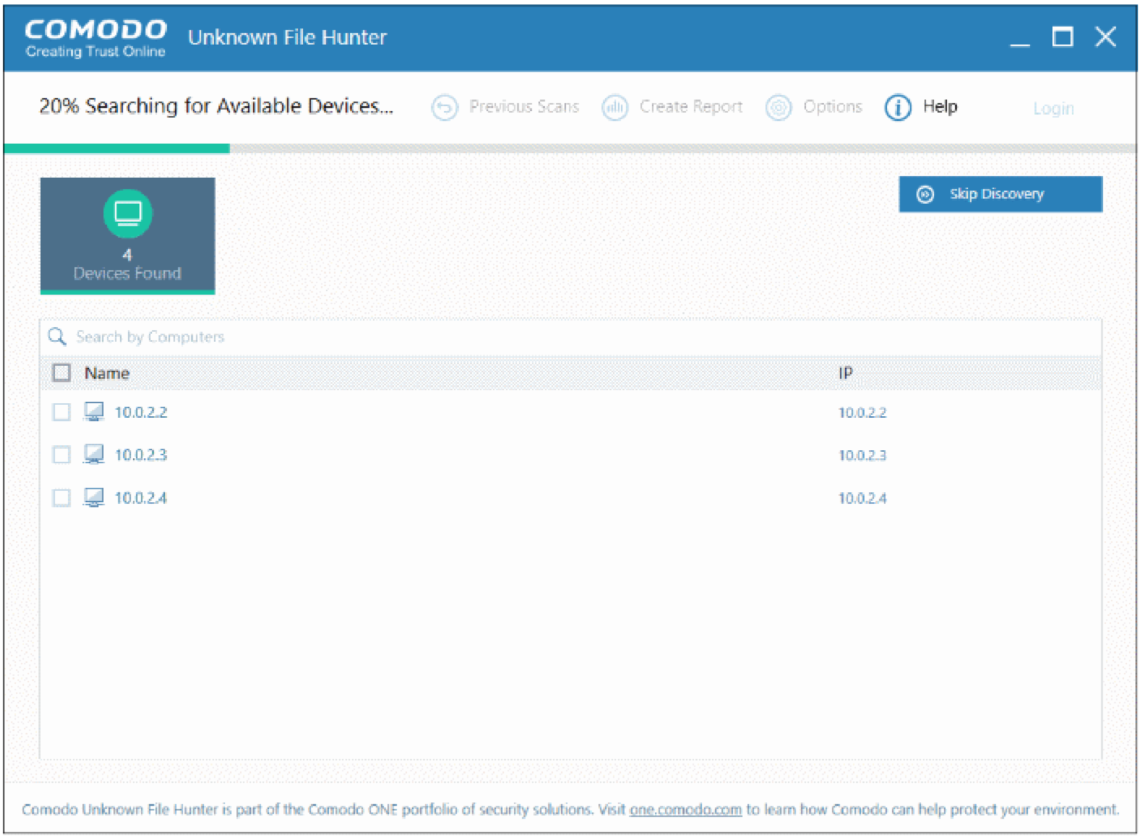
License Agreement

Please read the following license agreement carefully

License agreement

By clicking 'I ACCEPT', you agree you have read and accepted COMODO Unknown File Hunter License Agreement

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

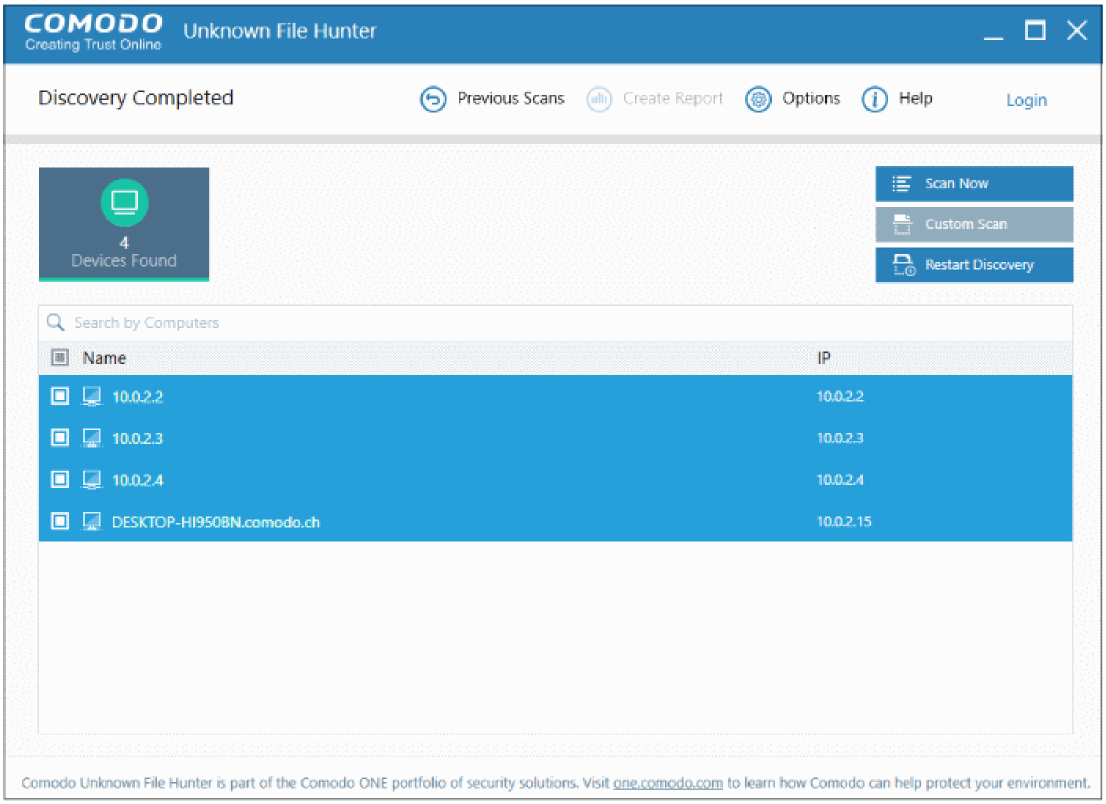


20% Searching for Available Devices...

Name	IP
□ 10.0.2.2	10.0.2.2
□ 10.0.2.3	10.0.2.3
□ 10.0.2.4	10.0.2.4

Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

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



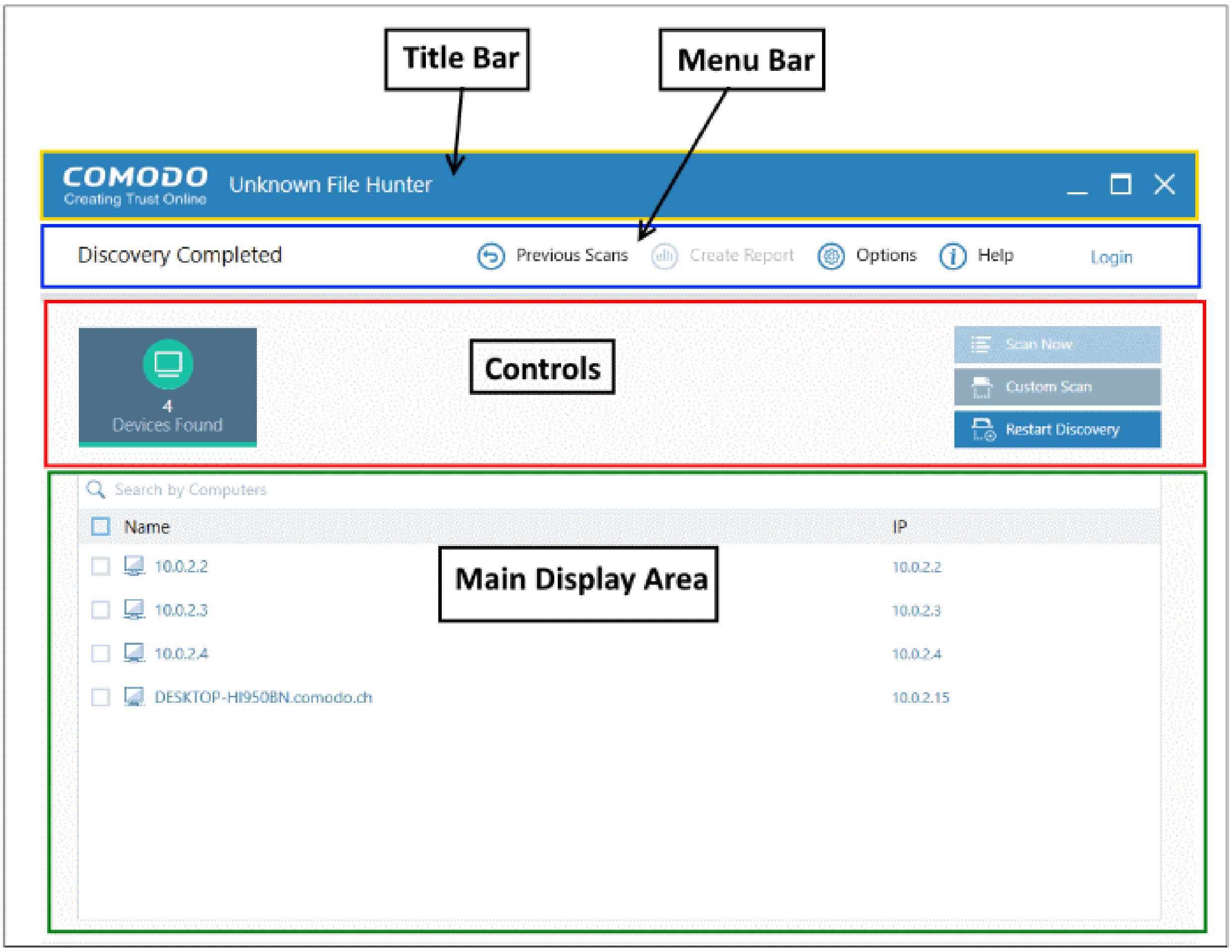
Discovery Completed

Name	IP
☑ 10.0.2.2	10.0.2.2
☑ 10.0.2.3	10.0.2.3
☑ 10.0.2.4	10.0.2.4
☑ DESKTOP-HI950BN.comodo.ch	10.0.2.15

Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

2.1 The Main Interface

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

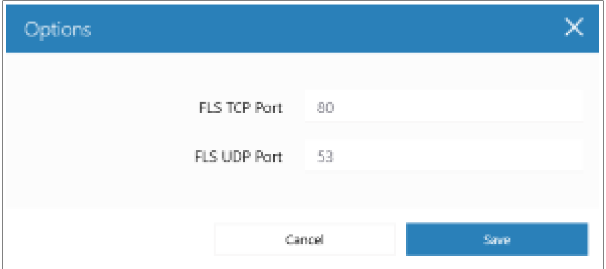


Name	IP
□ 10.0.2.2	10.0.2.2
□ 10.0.2.3	10.0.2.3
□ 10.0.2.4	10.0.2.4
□ DESKTOP-HI950BN.comodo.ch	10.0.2.15

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.



FLS TCP Port 80

FLS UDP Port 53

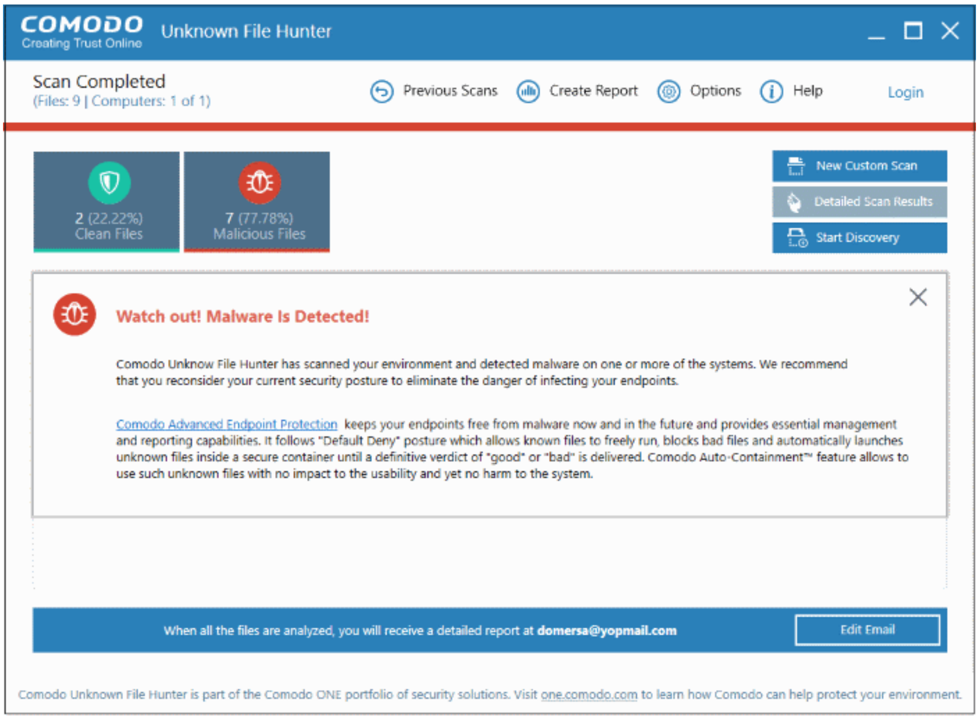
  - **Help** – Contains 'About' and 'Agent Requirements'

  '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.



Scan Completed
(Files: 9 | Computers: 1 of 1)

Watch out! Malware Is Detected!

Comodo Unknow File Hunter has scanned your environment and detected malware on one or more of the systems. We recommend that you reconsider your current security posture to eliminate the danger of infecting your endpoints.

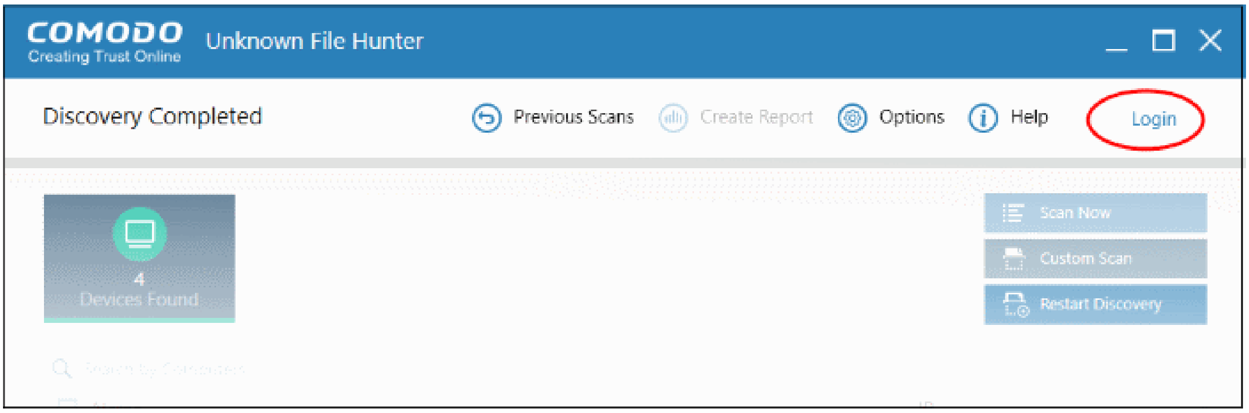
Comodo Advanced Endpoint Protection keeps your endpoints free from malware now and in the future and provides essential management and reporting capabilities. It follows "Default Deny" posture which allows known files to freely run, blocks bad files and automatically launches unknown files inside a secure container until a definitive verdict of "good" or "bad" is delivered. Comodo Auto-Containment™ feature allows to use such unknown files with no impact to the usability and yet no harm to the system.

When all the files are analyzed, you will receive a detailed report at **domersa@yopmail.com**

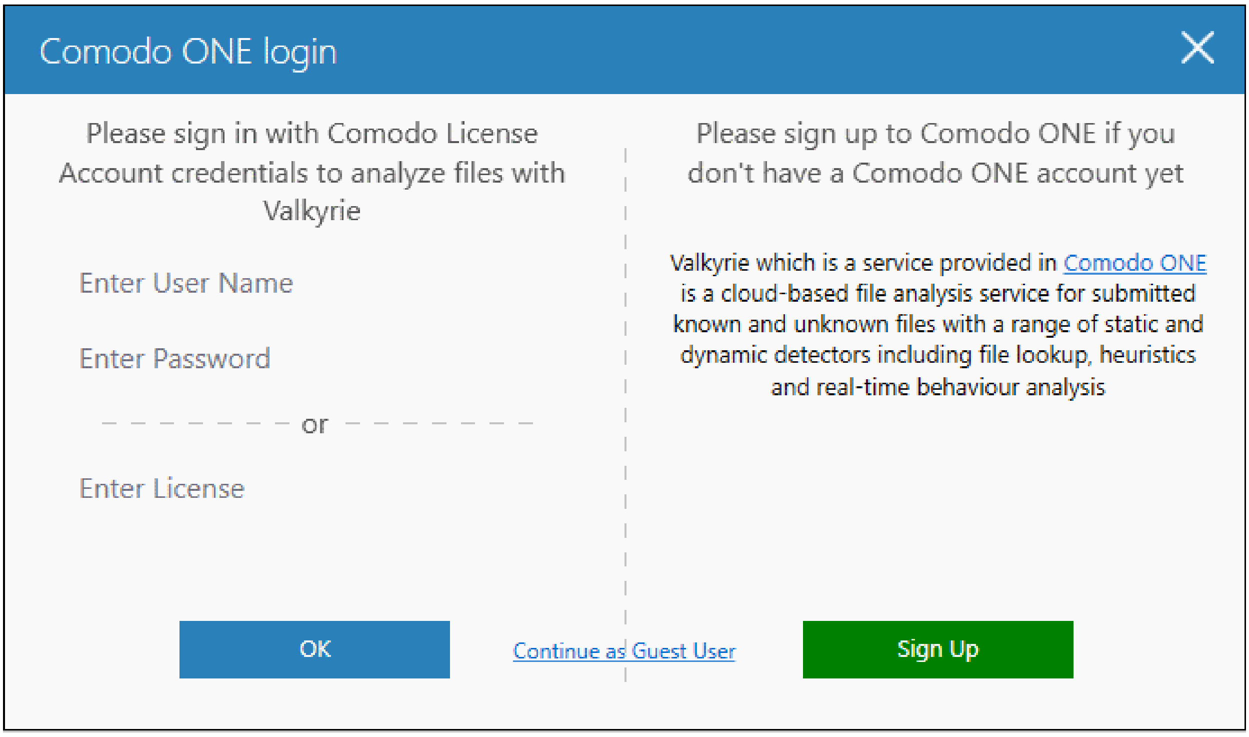
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

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.



Please sign in with Comodo License Account credentials to analyze files with Valkyrie

Enter User Name

Enter Password

or

Enter License

Please sign up to Comodo ONE if you don't have a Comodo ONE account yet

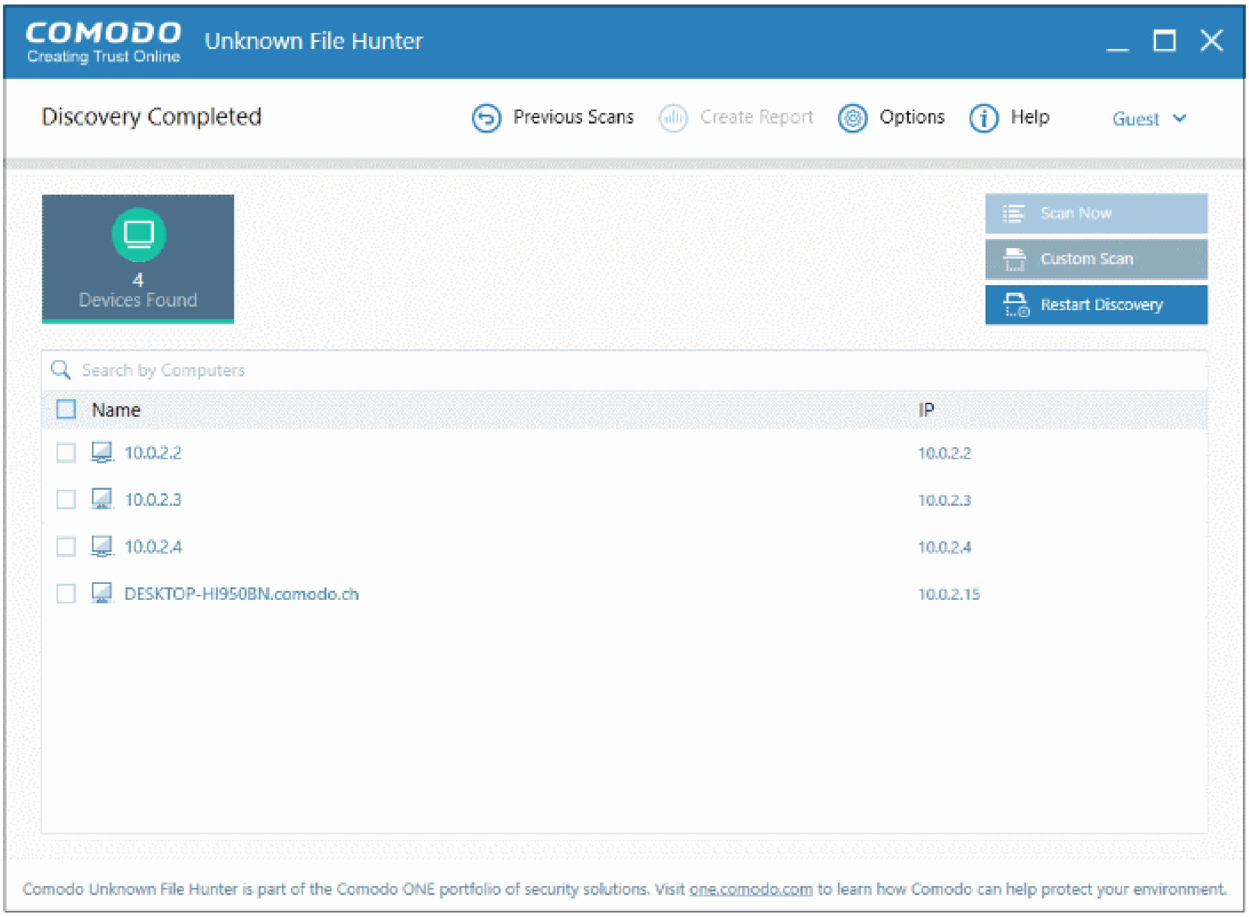
Valkyrie which is a service provided in Comodo ONE is a cloud-based file analysis service for submitted known and unknown files with a range of static and dynamic detectors including file lookup, heuristics and real-time behaviour analysis

- 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 C1 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.



Name	IP
10.0.2.2	10.0.2.2
10.0.2.3	10.0.2.3
10.0.2.4	10.0.2.4
DESKTOP-HI950BN.comodo.ch	10.0.2.15

Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

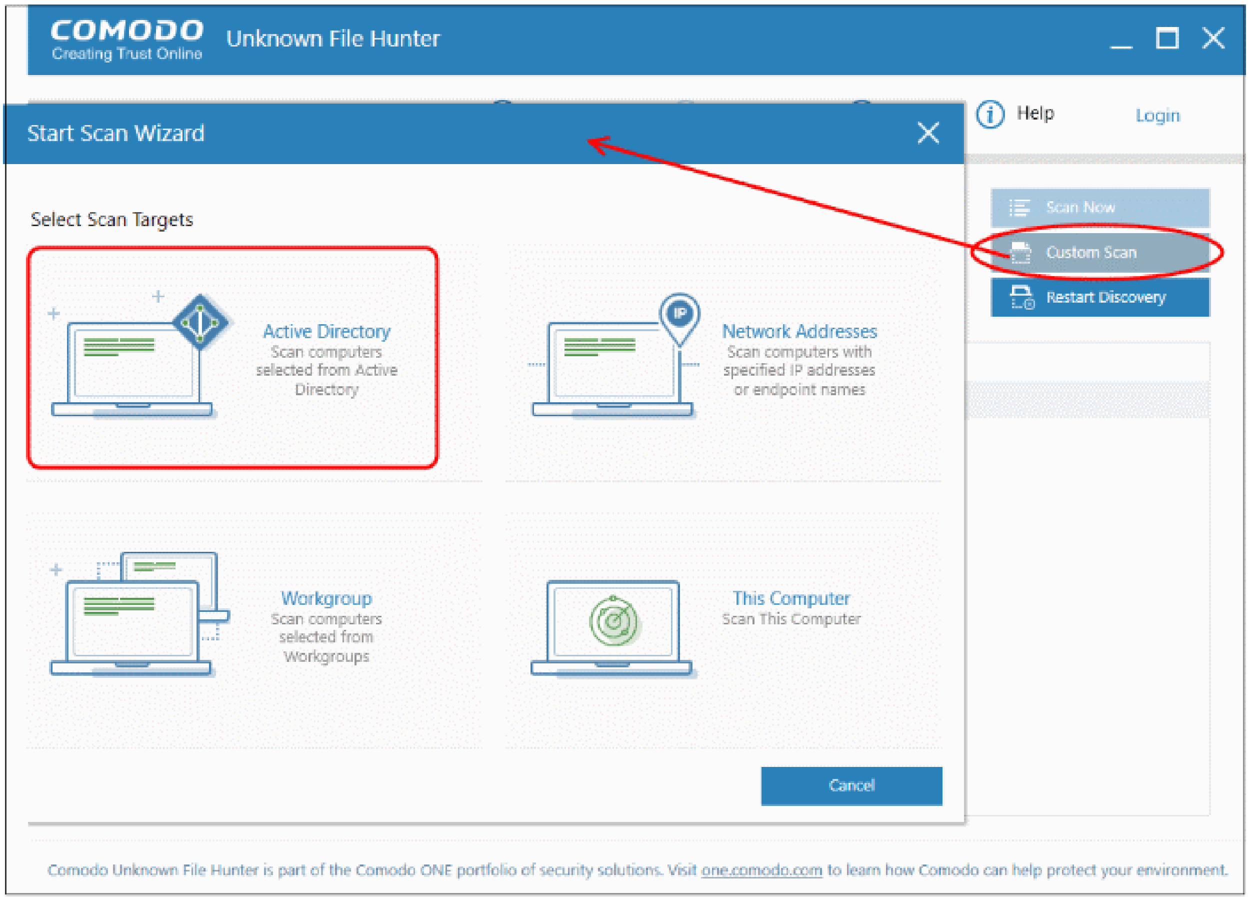
See the following sections for help on each method:

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

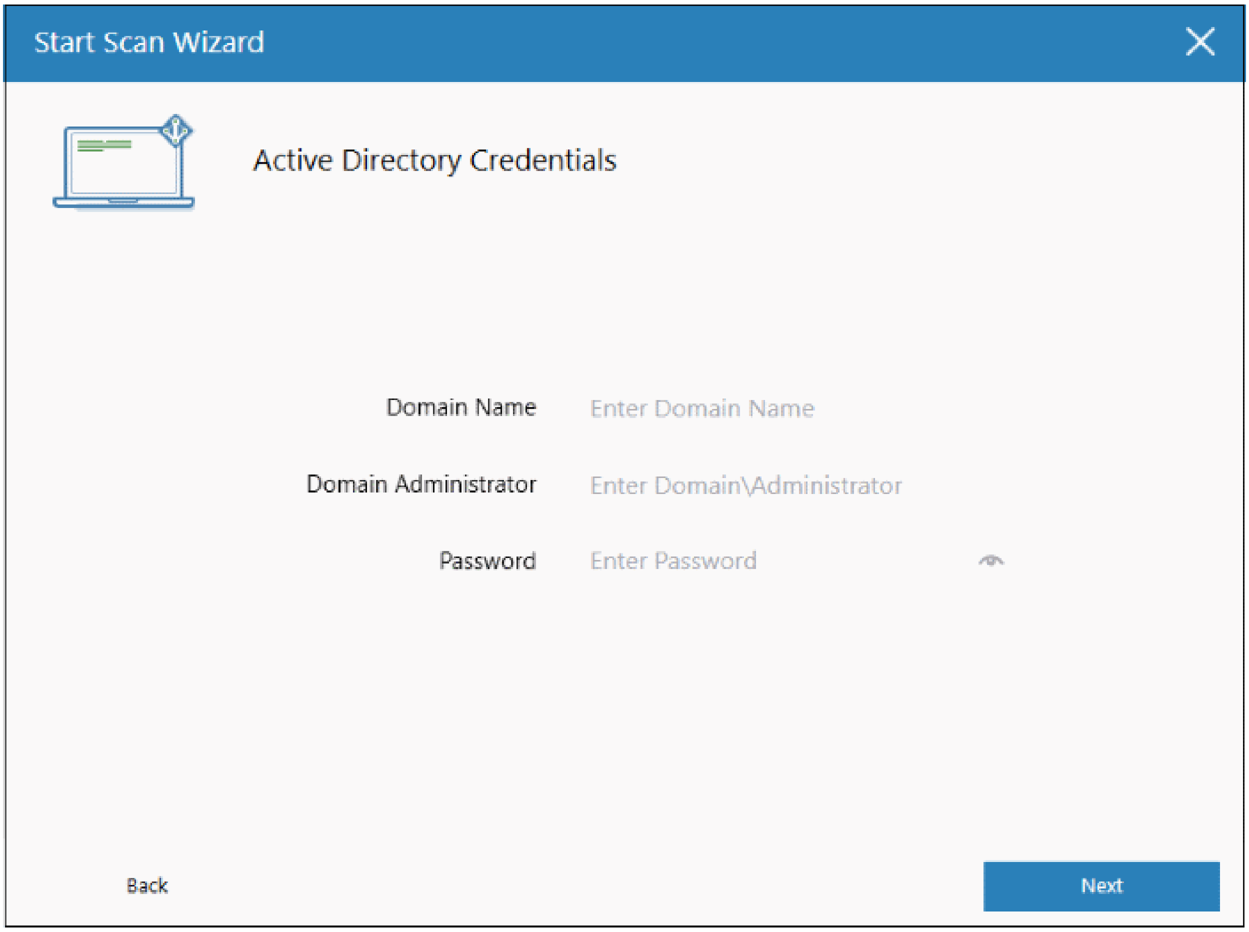
3.1 Scan Computers using Active Directory

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:


COMODO
Creating Trust Online
Unknown File Hunter
Help
Login
Start Scan Wizard
Select Scan Targets
Active Directory
Scan computers selected from Active Directory
Network Addresses
Scan computers with specified IP addresses or endpoint names
Workgroup
Scan computers selected from Workgroups
This Computer
Scan This Computer
Cancel
Scan Now
Custom Scan
Restart Discovery
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

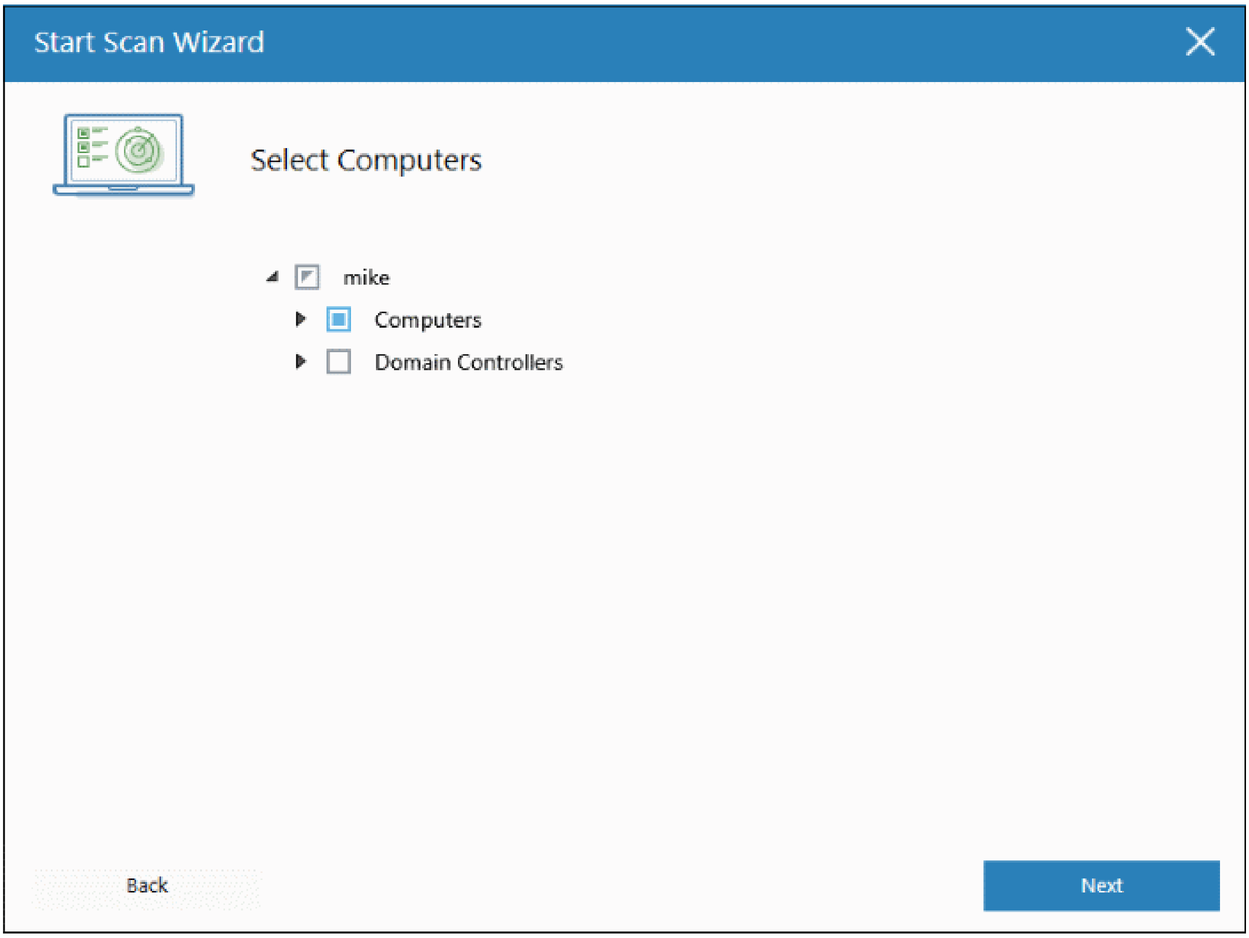
- Enter the name of your Active Directory domain and provide admin username and password:



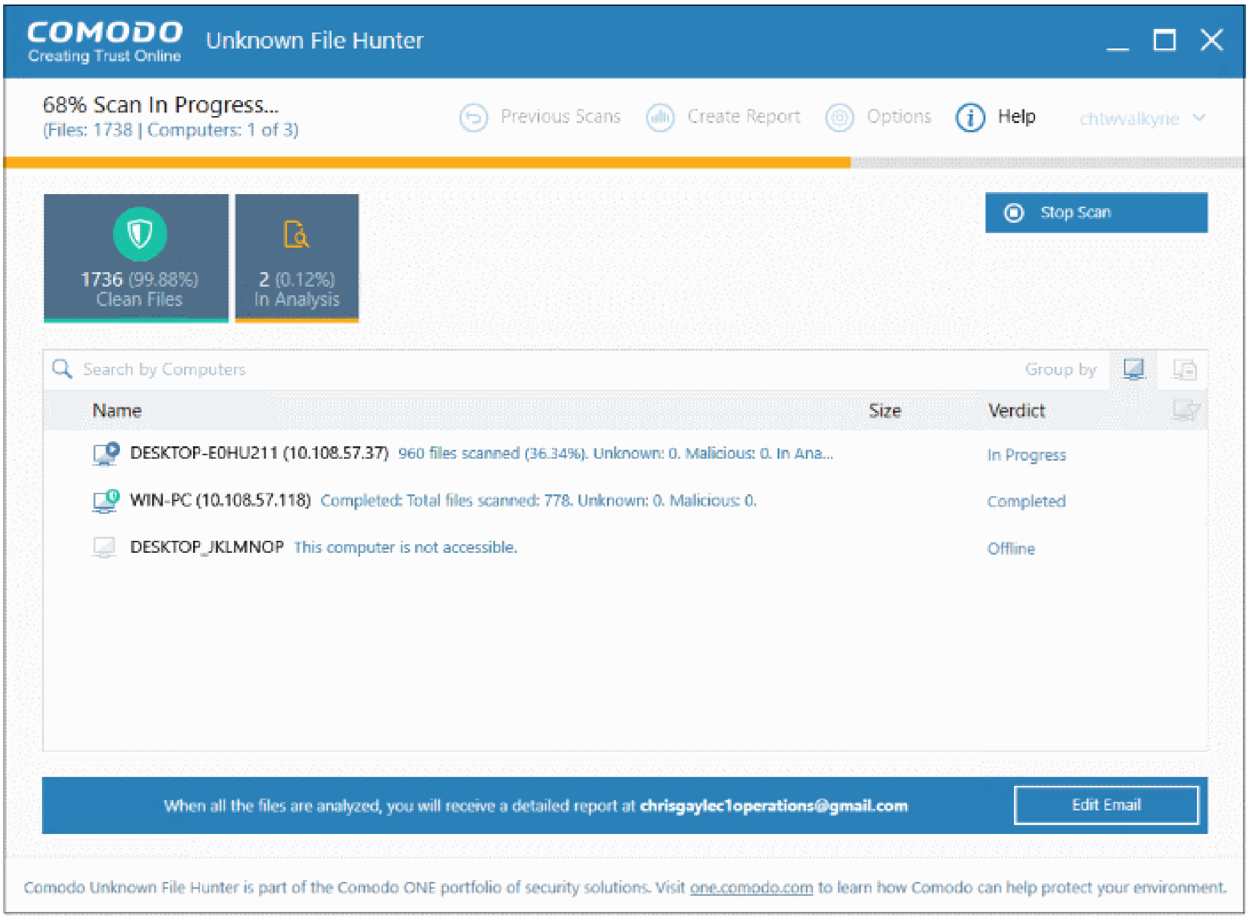
- After logging in, the 'Select Computers' screen will open:
- Choose the endpoints that you want to scan and a scan type:

  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.



COMODO Creating Trust Online — Unknown File Hunter

68% Scan In Progress...
(Files: 1738 | Computers: 1 of 3)

Previous Scans | Create Report | Options | Help | chtwvalkyrie

1736 (99.88%) Clean Files

2 (0.12%) In Analysis

Stop Scan

Search by Computers — Group by

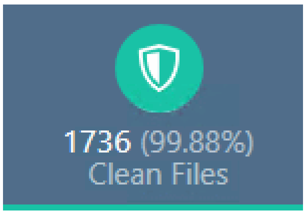
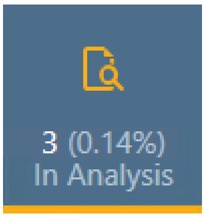
Name	Size	Verdict
DESKTOP-E0HU211 (10.108.57.37) 960 files scanned (36.34%). Unknown: 0. Malicious: 0. In Ana...		In Progress
WIN-PC (10.108.57.118) Completed: Total files scanned: 778. Unknown: 0. Malicious: 0.		Completed
DESKTOP_JKLMNOP This computer is not accessible.		Offline

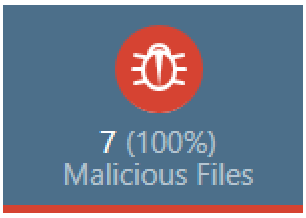
When all the files are analyzed, you will receive a detailed report at **chrisgaylec1operations@gmail.com** — Edit Email

Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

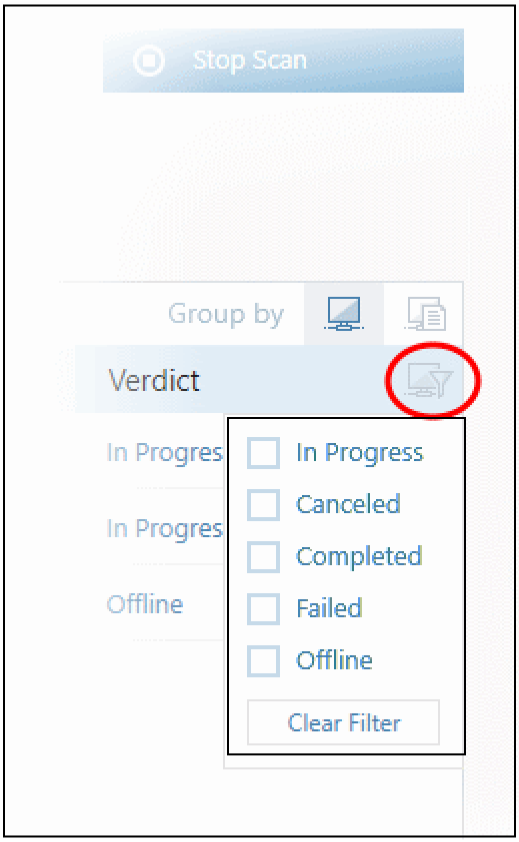
- 'Stop Scan' - Discontinue the scan.
- 'Edit Email' – Specify the email address to which the scan report should be sent

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

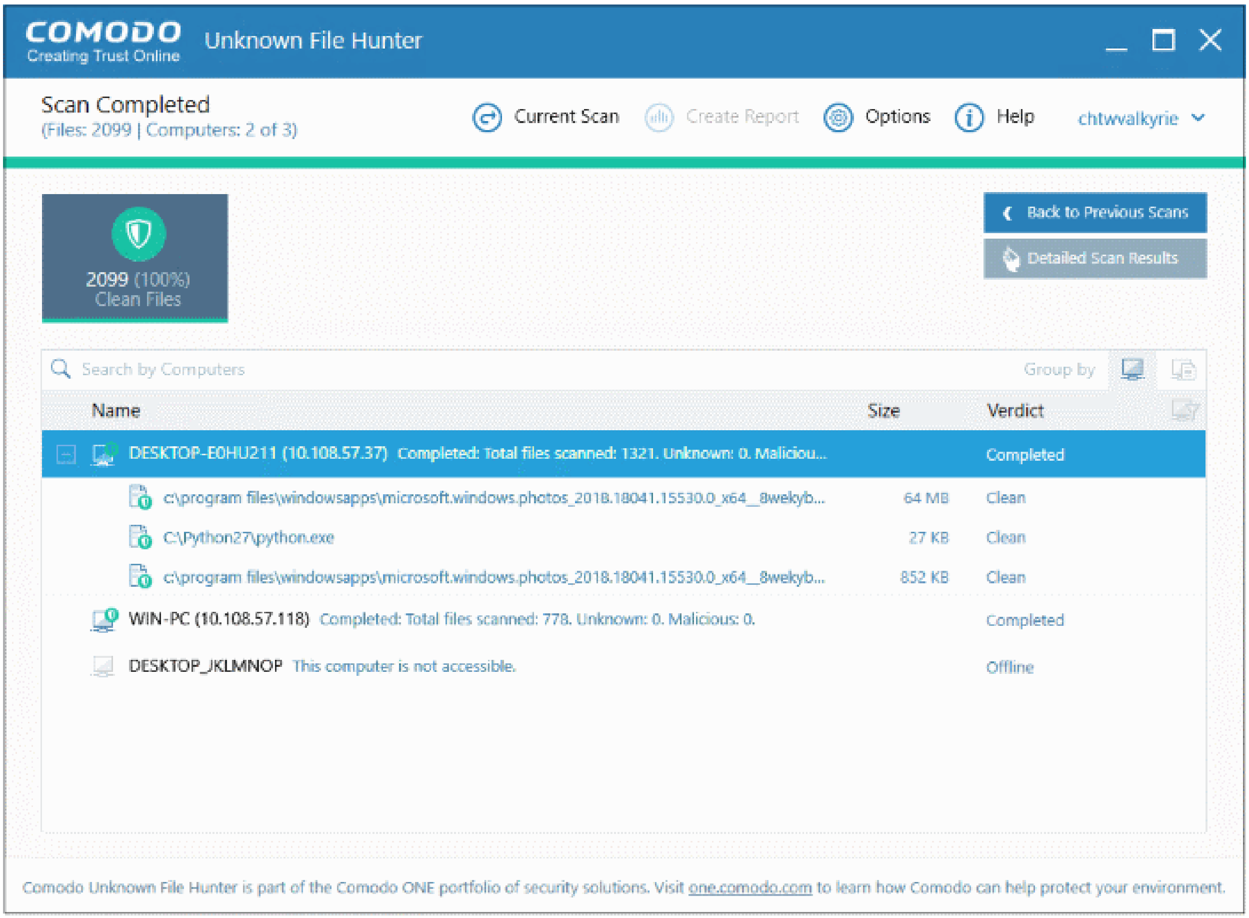
 1736 (99.88%) Clean Files	Safe files. These files are on the Comodo whitelist are OK to run.
 3 (0.14%) In Analysis	Unknown, potentially malicious files. • These files are automatically uploaded to Valkyrie for analysis during the scan. • You can view the analysis results by signing in to your Valkyrie account at **https://valkyrie.comodo.com/login** • You also can sign into Valkyrie with your Comodo One username and password. See '**Valkyrie Analysis Results**' for more information.

	Malicious files. These files are on the Comodo blacklist of known malware and should not be allowed to run on your network.

- Click the funnel icon to filter scans by status:



Results are shown when the scan finishes:



Scan Completed
(Files: 2099 | Computers: 2 of 3)

Name	Size	Verdict
DESKTOP-E0HU211 (10.108.57.37) Completed: Total files scanned: 1321. Unknown: 0. Maliciou...		Completed
c:\program files\windowsapps\microsoft.windows.photos_2018.18041.15530.0_x64__8wekyb...	64 MB	Clean
C:\Python27\python.exe	27 KB	Clean
c:\program files\windowsapps\microsoft.windows.photos_2018.18041.15530.0_x64__8wekyb...	852 KB	Clean
WIN-PC (10.108.57.118) Completed: Total files scanned: 778. Unknown: 0. Malicious: 0.		Completed
DESKTOP_JKLMNOP This computer is not accessible.		Offline

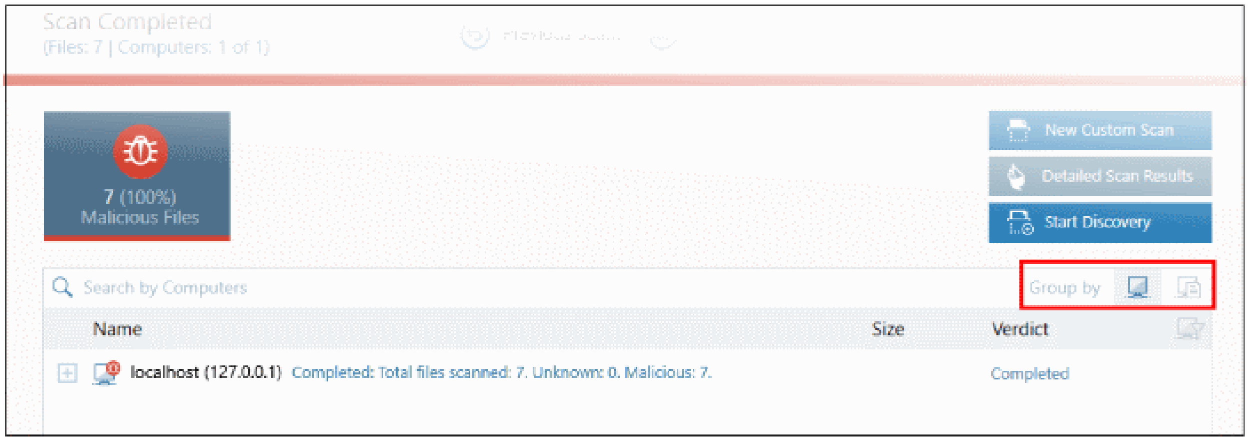
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

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	Status of the file. The possible values are: • In Progress – Unknown file which is queued for upload to Valkyrie, Comodo's file analysis system • Uploading – Unknown file which is currently being submitted to Valkyrie • In Analysis – Unknown file which is currently being tested by Valkyrie • Clean – Valkyrie tests found the file is safe to run • Malicious – Valkyrie tests found the file is harmful and should not be allowed to run • 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.

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

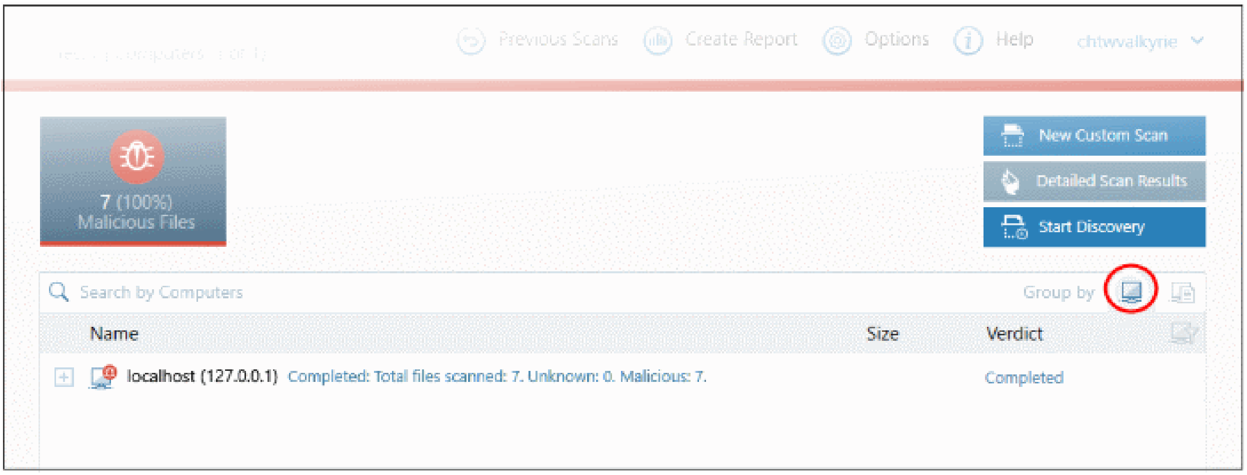
- 'Clean' - Unknown files that have been analyzed by Valkyrie and found safe.
- Click the 'Group By' icons on the right to change how results are displayed:
  - **Group by Computer:** Lists all computers scanned. Expand any computer to view the unknown / malicious files on those computers.
  - **Group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



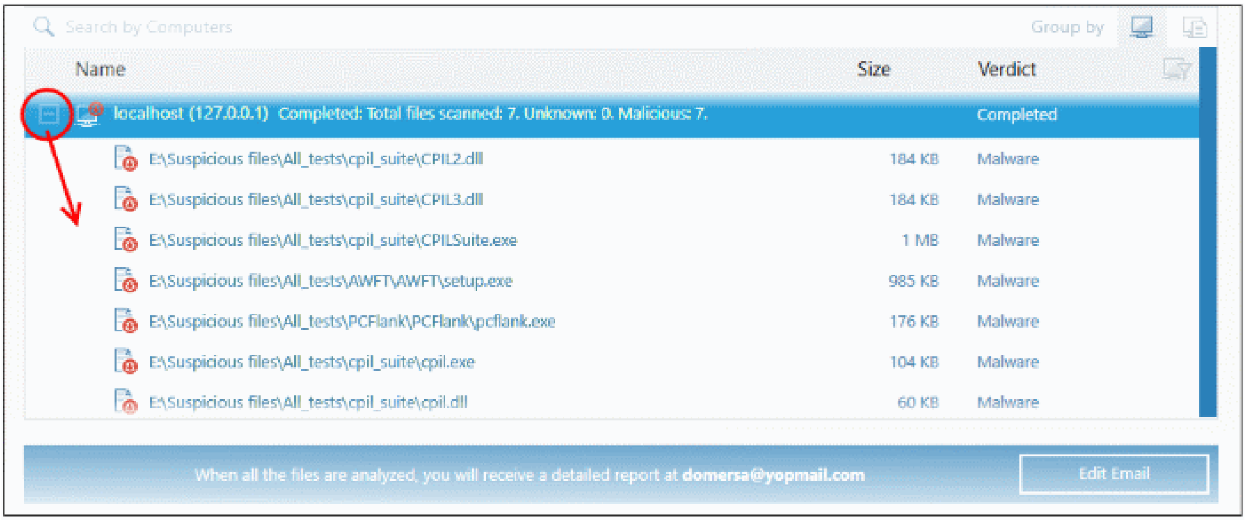
localhost (127.0.0.1) Completed: Total files scanned: 7. Unknown: 0. Malicious: 7. Completed

- Click the computer icon to view results by computer:



localhost (127.0.0.1) Completed: Total files scanned: 7. Unknown: 0. Malicious: 7. Completed

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

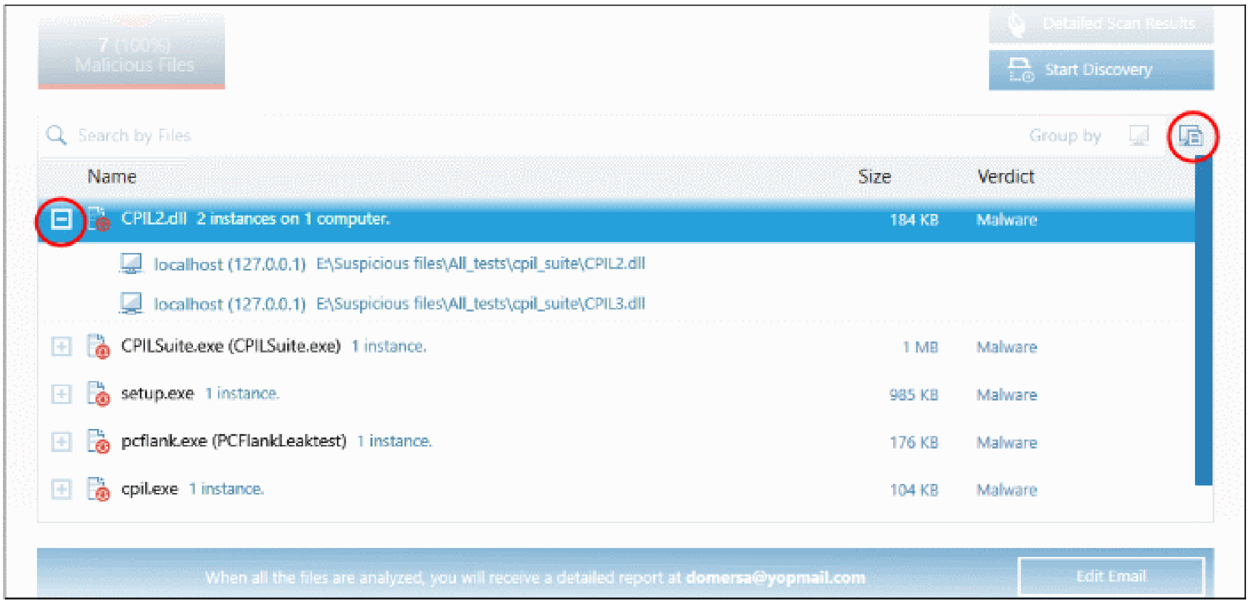


Name	Size	Verdict
localhost (127.0.0.1) Completed: Total files scanned: 7. Unknown: 0. Malicious: 7.		Completed
E:\Suspicious files\All_tests\cpil_suite\CPIL2.dll	184 KB	Malware
E:\Suspicious files\All_tests\cpil_suite\CPIL3.dll	184 KB	Malware
E:\Suspicious files\All_tests\cpil_suite\CPILSuite.exe	1 MB	Malware
E:\Suspicious files\All_tests\AWFT\AWFT\setup.exe	985 KB	Malware
E:\Suspicious files\All_tests\PCFlank\PCFlank\pcflank.exe	176 KB	Malware
E:\Suspicious files\All_tests\cpil_suite\cpil.exe	104 KB	Malware
E:\Suspicious files\All_tests\cpil_suite\cpil.dll	60 KB	Malware

When all the files are analyzed, you will receive a detailed report at **domersa@yopmail.com**

Group by File

- Click the computer with file icon on the right



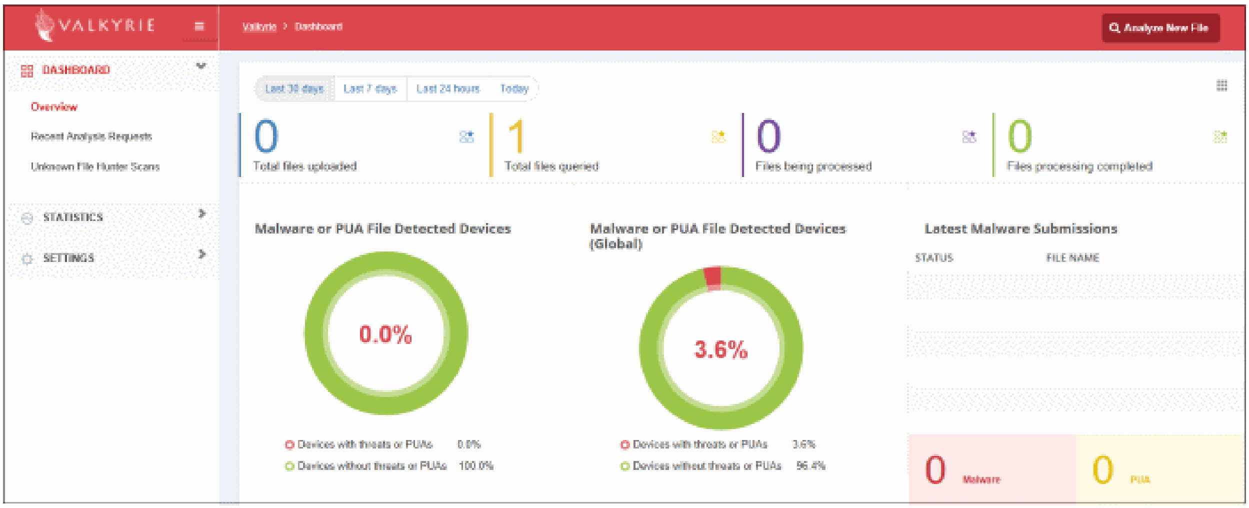
Name	Size	Verdict
CPIL2.dll 2 instances on 1 computer.	184 KB	Malware
localhost (127.0.0.1) E:\Suspicious files\All_tests\cpil_suite\CPIL2.dll		
localhost (127.0.0.1) E:\Suspicious files\All_tests\cpil_suite\CPIL3.dll		
CPILSuite.exe (CPILSuite.exe) 1 instance.	1 MB	Malware
setup.exe 1 instance.	985 KB	Malware
pcflank.exe (PCFlankLeaktest) 1 instance.	176 KB	Malware
cpil.exe 1 instance.	104 KB	Malware

When all the files are analyzed, you will receive a detailed report at **domersa@yopmail.com**

- 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:

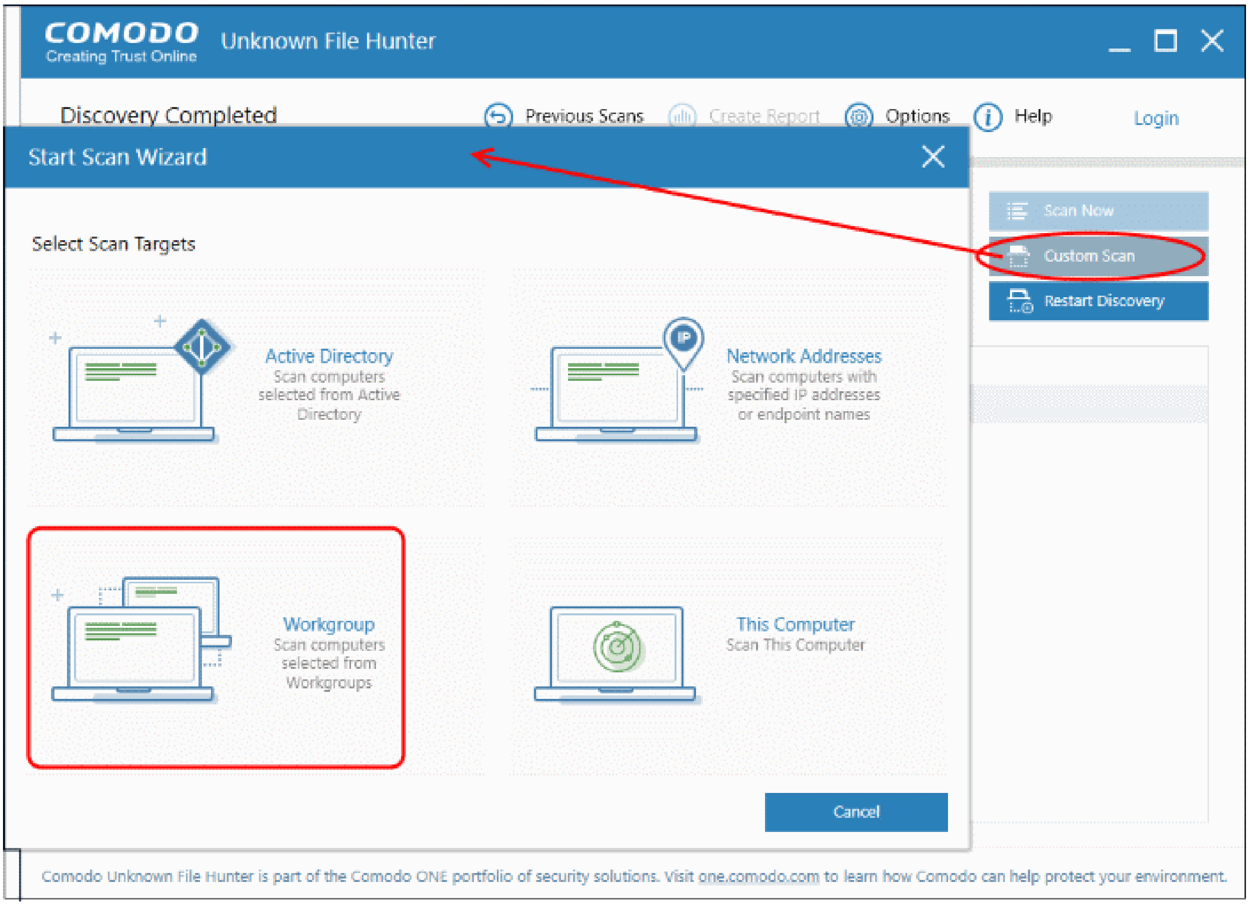

VALKYRIE
Valkyrie > Dashboard
Analyze New File
DASHBOARD
Overview
Recent Analysis Requests
Unknown File Hunter Scans
STATISTICS
SETTINGS
Last 30 days
Last 7 days
Last 24 hours
Today
0
Total files uploaded
1
Total files queried
0
Files being processed
0
Files processing completed
Malware or PUA File Detected Devices
0.0%
Devices with threats or PUAs 0.0%
Devices without threats or PUAs 100.0%
Malware or PUA File Detected Devices (Global)
3.6%
Devices with threats or PUAs 3.6%
Devices without threats or PUAs 96.4%
Latest Malware Submissions
STATUS
FILE NAME
0 Malware
0 PUA

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

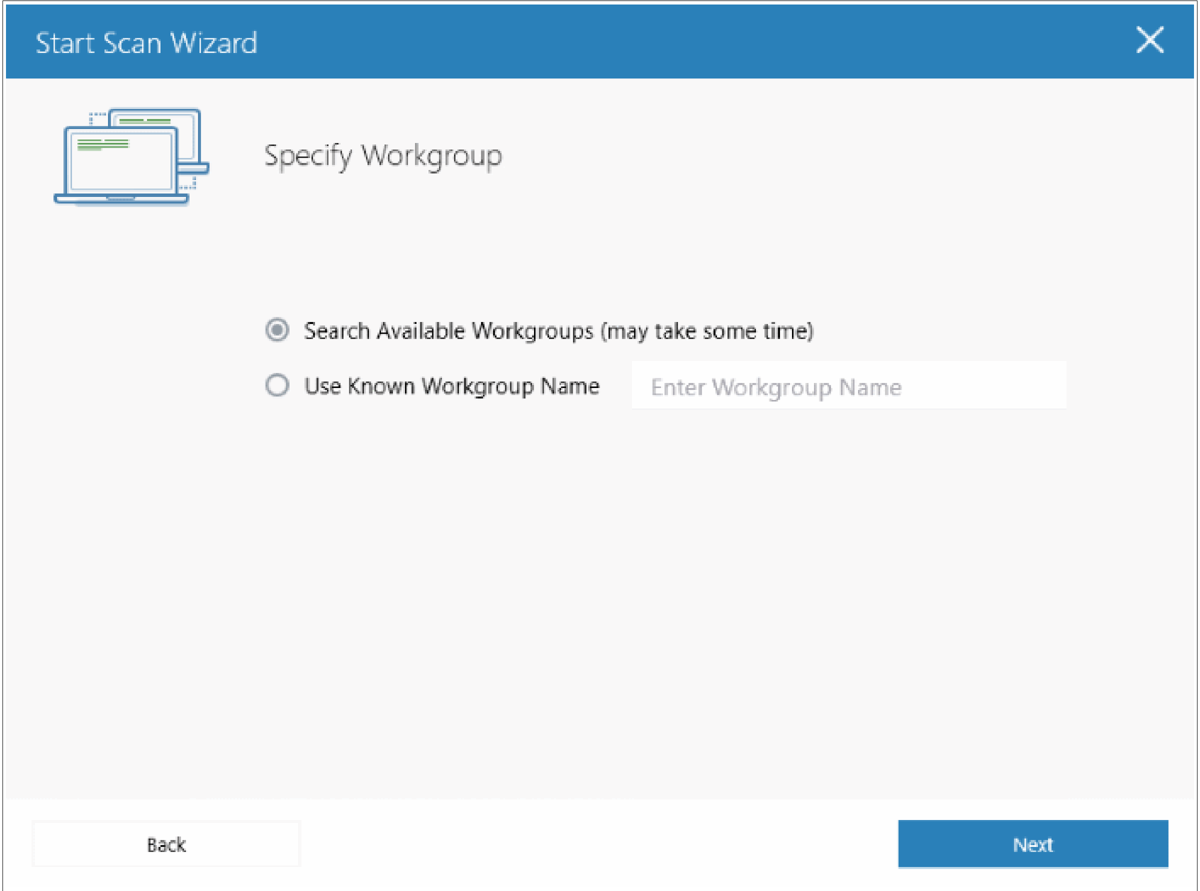
3.2 Scan Computers by Workgroup

To scan all or selected computers in a Workgroup:

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


COMODO
Creating Trust Online
Unknown File Hunter
Discovery Completed
Previous Scans
Create Report
Options
Help
Login
Start Scan Wizard
Select Scan Targets
Active Directory
Scan computers selected from Active Directory
Network Addresses
Scan computers with specified IP addresses or endpoint names
Workgroup
Scan computers selected from Workgroups
This Computer
Scan This Computer
Cancel
Scan Now
Custom Scan
Restart Discovery
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

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



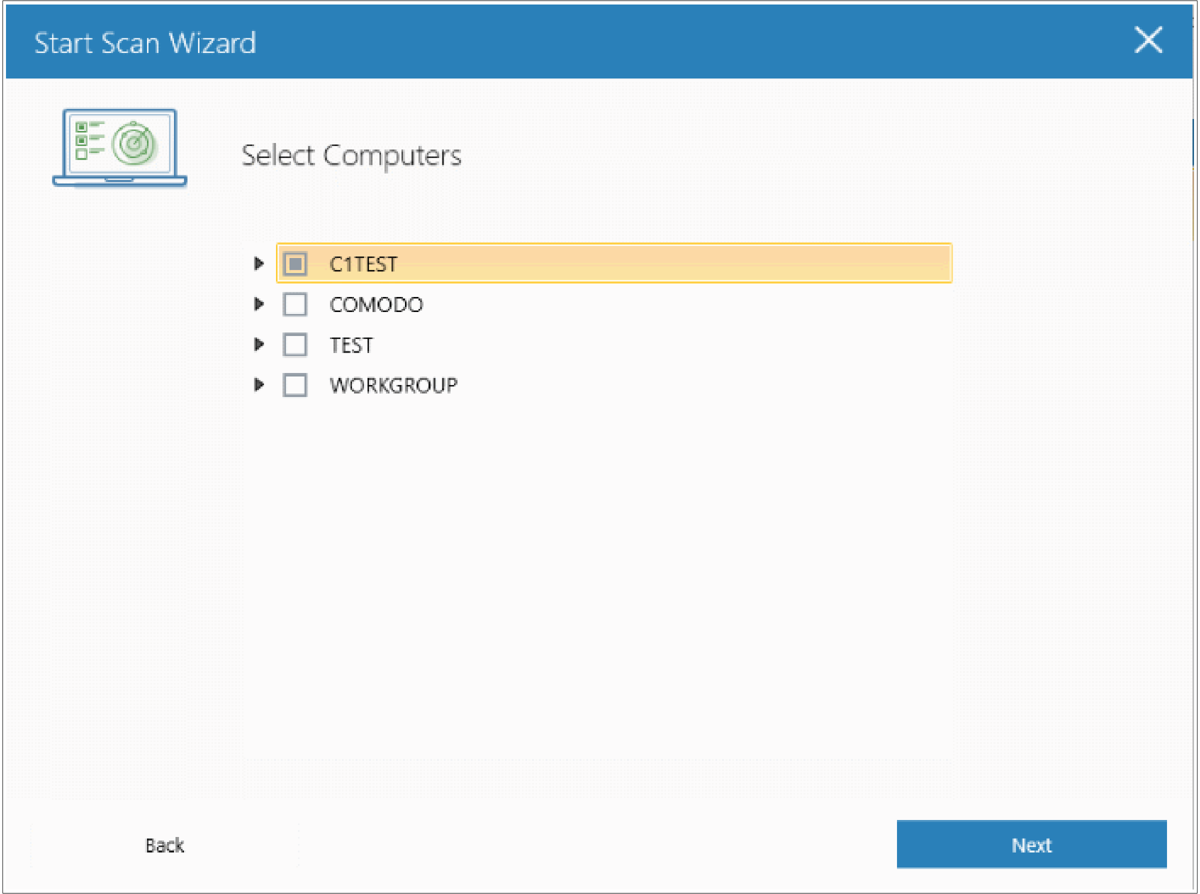
Start Scan Wizard

Specify Workgroup

● Search Available Workgroups (may take some time)

○ Use Known Workgroup Name Enter Workgroup Name

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

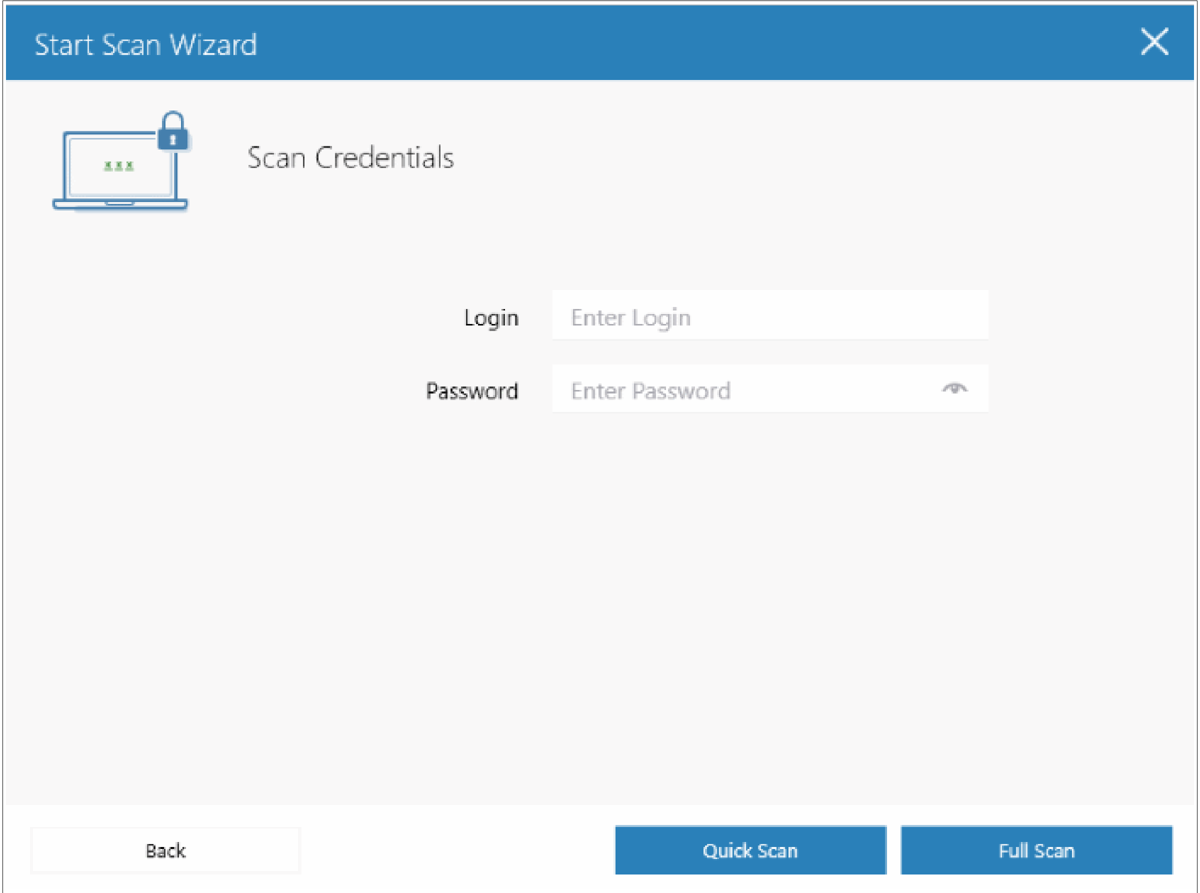


Start Scan Wizard

Select Computers

- ▸ ▣ C1TEST
- ▸ □ COMODO
- ▸ □ TEST
- ▸ □ WORKGROUP

- Enter the administrator's credentials



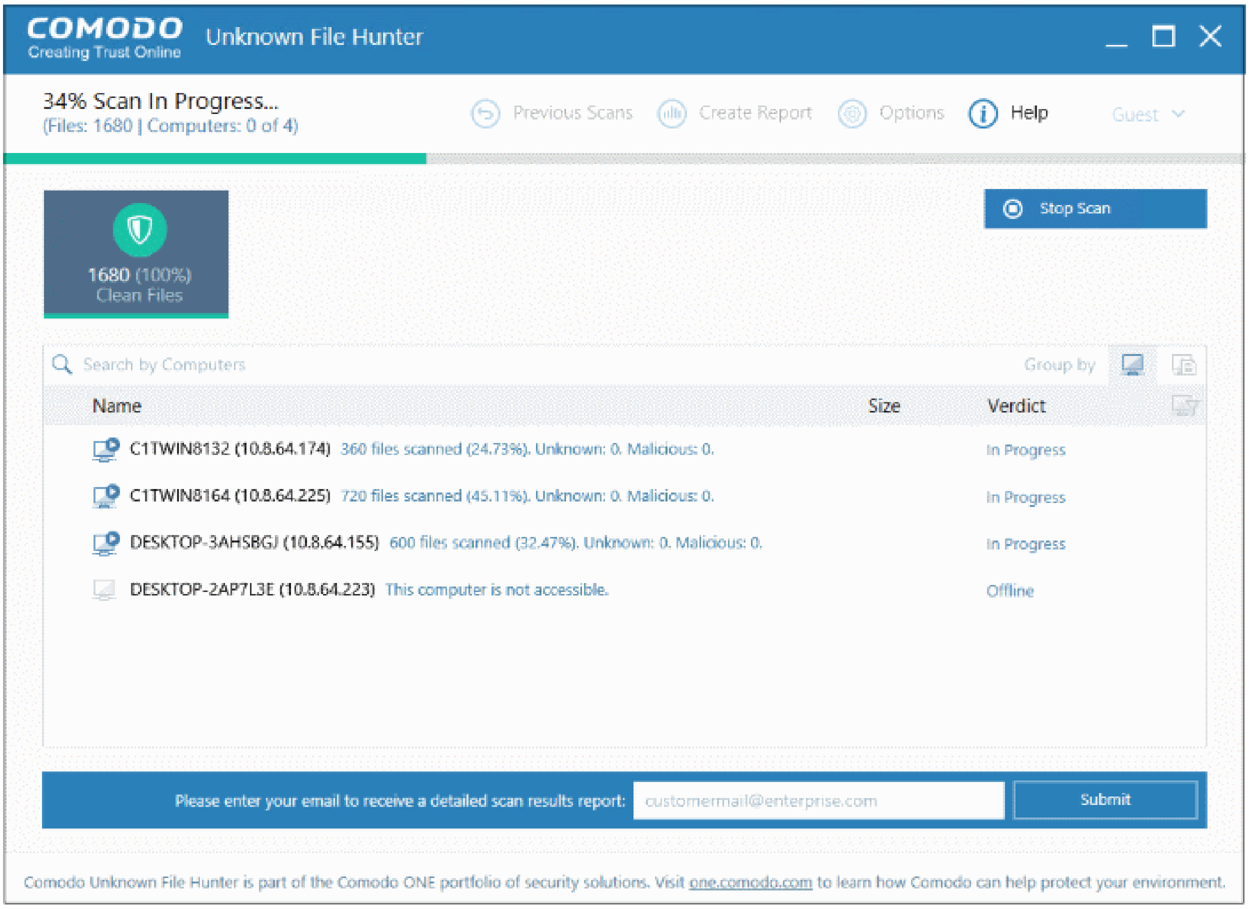
Login: Enter Login

Password: Enter Password

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:



34% Scan In Progress...
(Files: 1680 | Computers: 0 of 4)

1680 (100%) Clean Files

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

Please enter your email to receive a detailed scan results report: customermail@enterprise.com

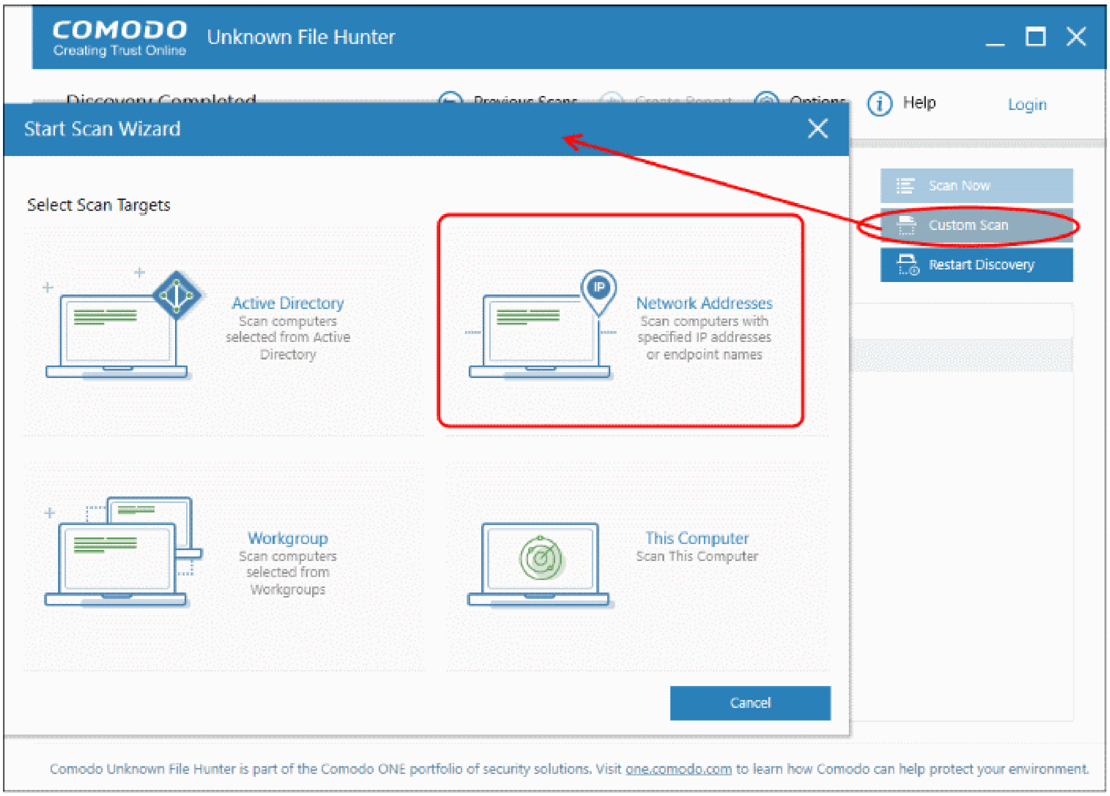
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

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

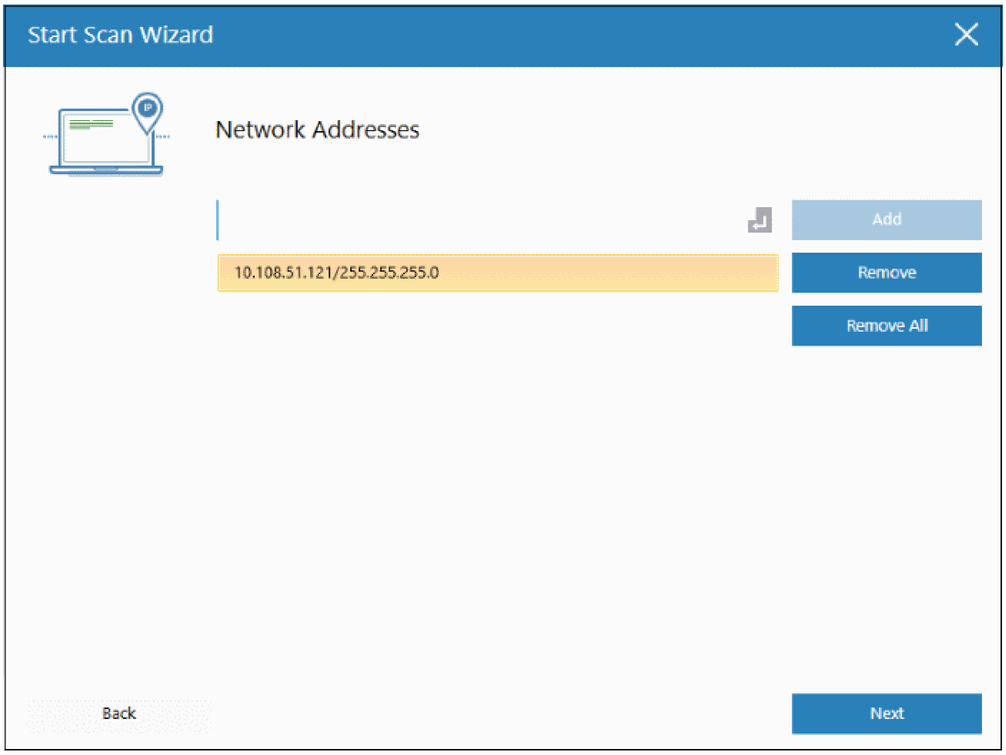
To scan computers by specifying their IP address or hostname:

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


COMODO Creating Trust Online
Unknown File Hunter
Discovery Completed
Previous Scans
Create Report
Options
Help
Login
Start Scan Wizard
Select Scan Targets
Active Directory
Scan computers selected from Active Directory
Network Addresses
Scan computers with specified IP addresses or endpoint names
Workgroup
Scan computers selected from Workgroups
This Computer
Scan This Computer
Cancel
Scan Now
Custom Scan
Restart Discovery
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

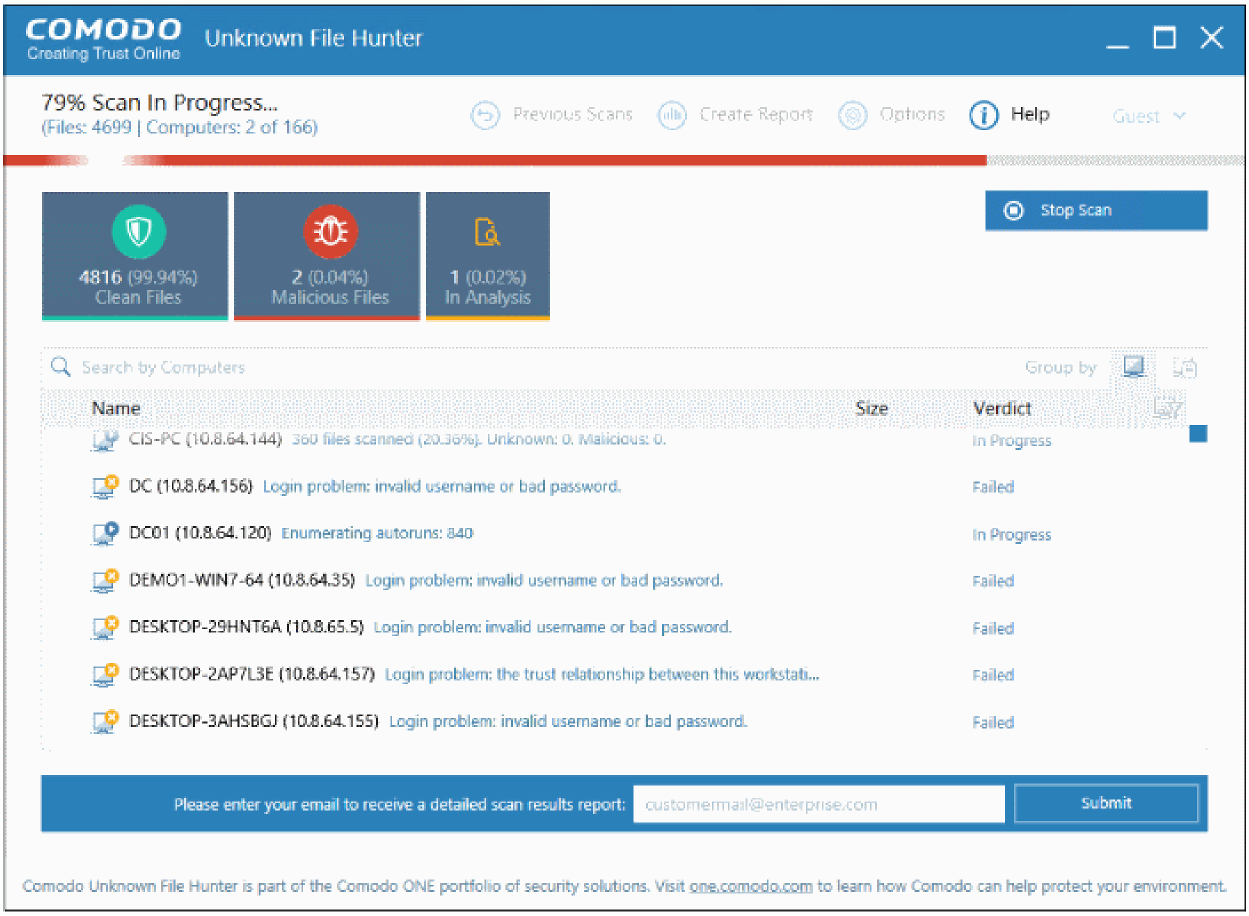
Next, enter the addresses you want to scan. You can add addresses in the following format:

- 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'



10.108.51.121/255.255.255.0

- 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.



79% Scan In Progress...
(Files: 4699 | Computers: 2 of 166)

4816 (99.94%) Clean Files

2 (0.04%) Malicious Files

1 (0.02%) In Analysis

Name	Size	Verdict
CIS-PC (10.8.64.144) 360 files scanned (20.36%). Unknown: 0. Malicious: 0.		In Progress
DC (10.8.64.156) Login problem: invalid username or bad password.		Failed
DC01 (10.8.64.120) Enumerating autoruns: 840		In Progress
DEMO1-WIN7-64 (10.8.64.35) Login problem: invalid username or bad password.		Failed
DESKTOP-29HNT6A (10.8.65.5) Login problem: invalid username or bad password.		Failed
DESKTOP-2AP7L3E (10.8.64.157) Login problem: the trust relationship between this workstati...		Failed
DESKTOP-3AHSBGJ (10.8.64.155) Login problem: invalid username or bad password.		Failed

Please enter your email to receive a detailed scan results report: customermail@enterprise.com

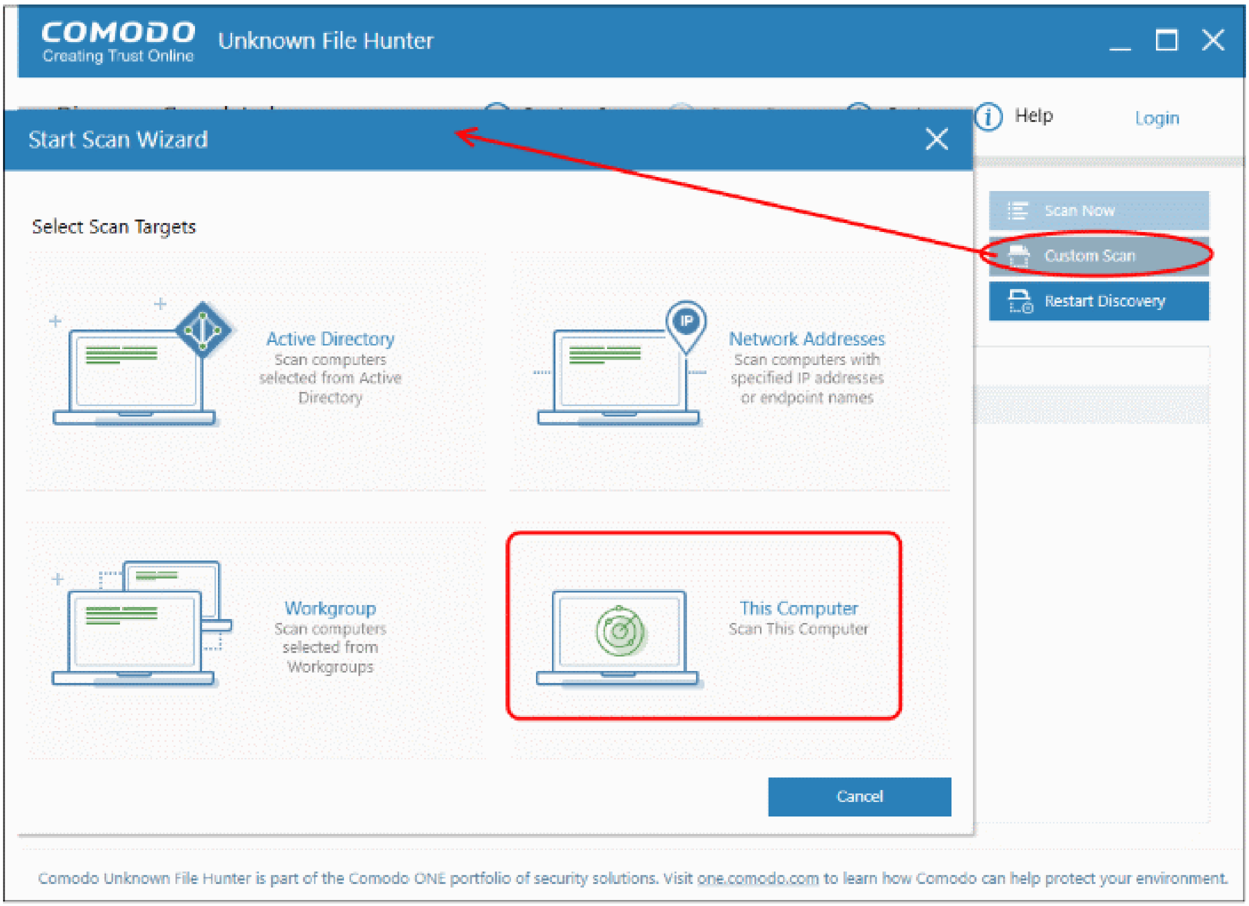
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

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.

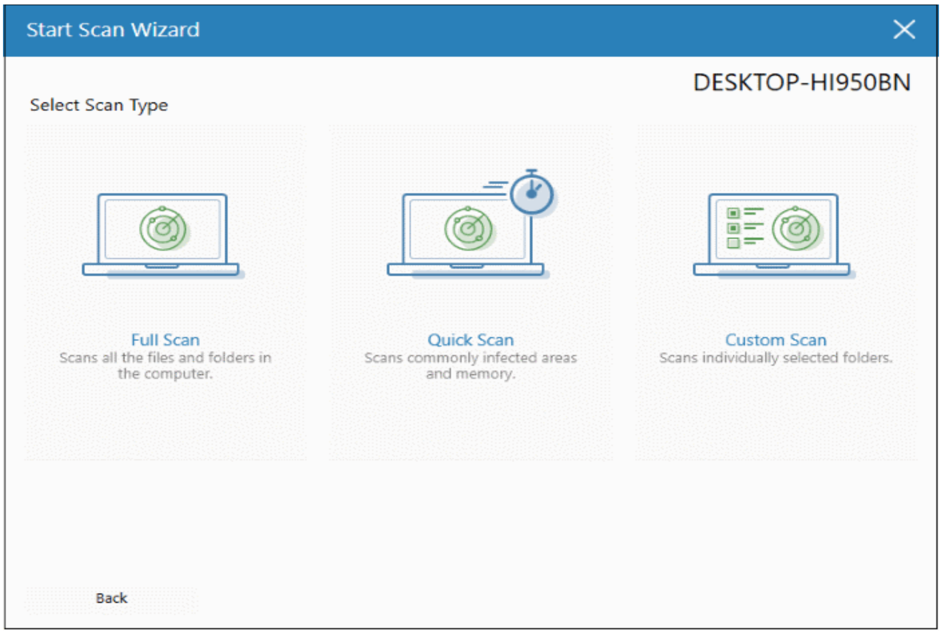
3.4 Scan Local Computer

To scan the computer you are currently using:

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


COMODO Creating Trust Online
Unknown File Hunter
Help
Login
Start Scan Wizard
Select Scan Targets
Active Directory
Scan computers selected from Active Directory
Network Addresses
Scan computers with specified IP addresses or endpoint names
Workgroup
Scan computers selected from Workgroups
This Computer
Scan This Computer
Cancel
Scan Now
Custom Scan
Restart Discovery
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

- Choose the type of scan you want to run:

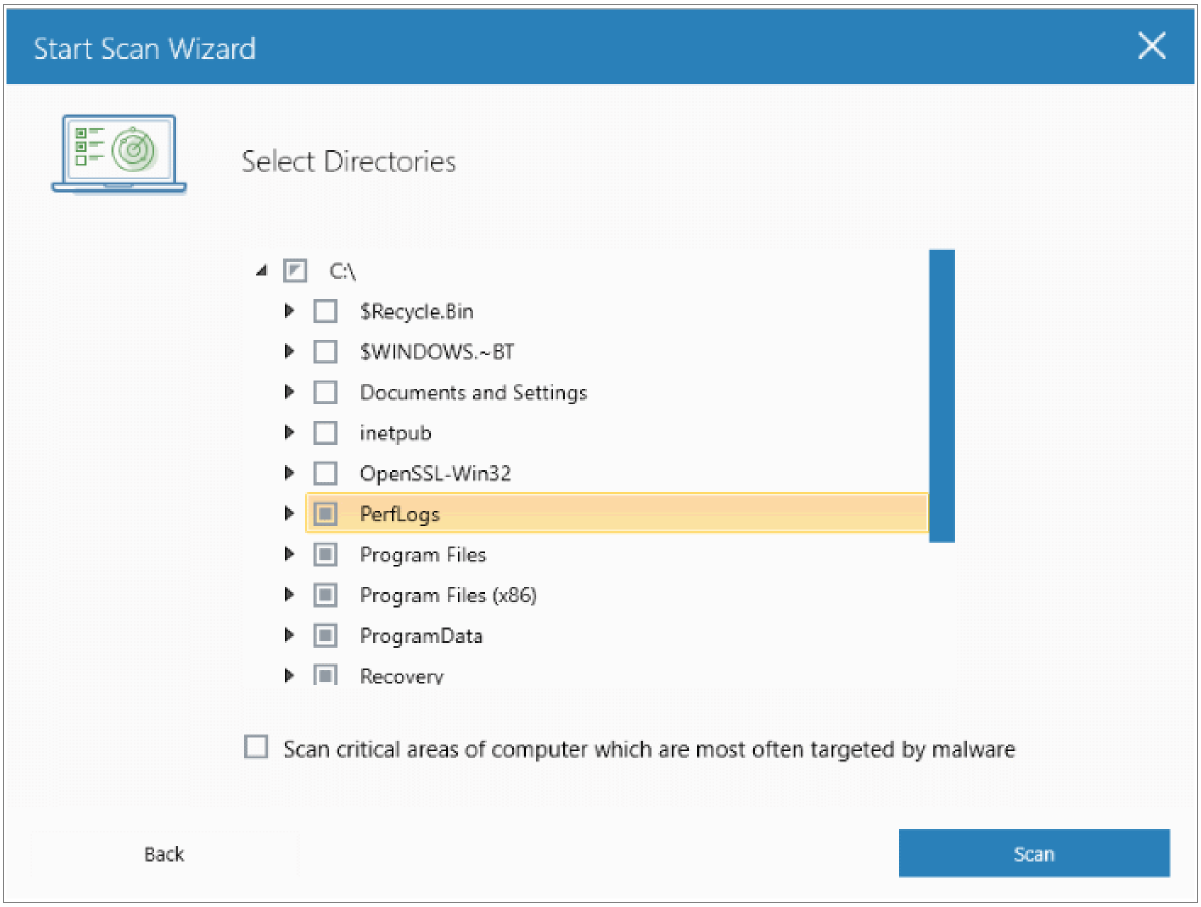

Start Scan Wizard
DESKTOP-HI950BN
Select Scan Type
Full Scan
Scans all the files and folders in the computer.
Quick Scan
Scans commonly infected areas and memory.
Custom Scan
Scans individually selected folders.
Back

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

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

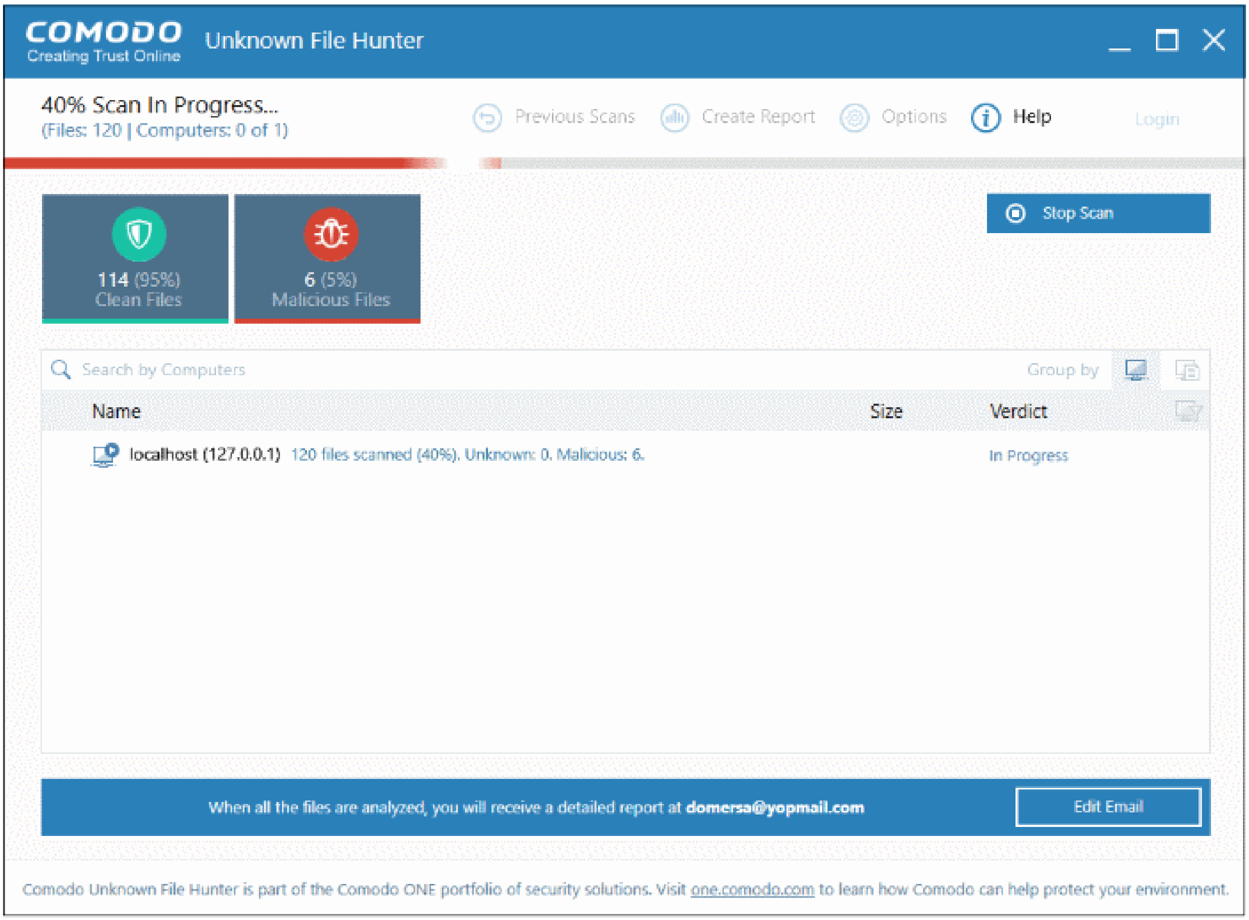
Custom Scan: Scan selected files or folders on the local computer

- 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 of computer which are most often targeted by malware

- '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.



40% Scan In Progress...
(Files: 120 | Computers: 0 of 1)

114 (95%) Clean Files

6 (5%) Malicious Files

Name	Size	Verdict
localhost (127.0.0.1) 120 files scanned (40%). Unknown: 0. Malicious: 6.		In Progress

When all the files are analyzed, you will receive a detailed report at **domersa@yopmail.com**

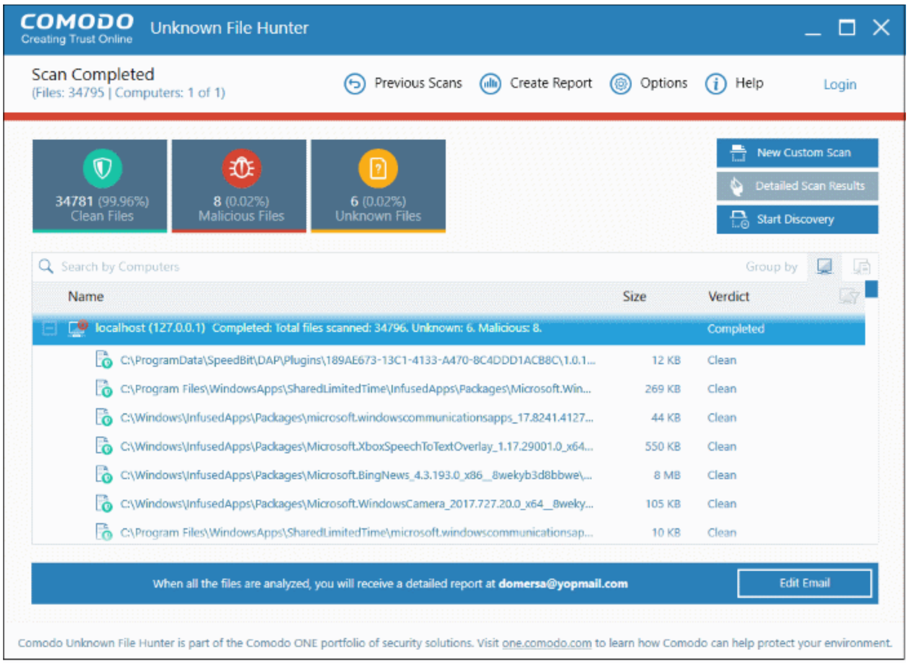
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

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.

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.



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

34781 (99.96%) Clean Files

8 (0.02%) Malicious Files

6 (0.02%) Unknown Files

Name	Size	Verdict
localhost (127.0.0.1) Completed: Total files scanned: 34796. Unknown: 6. Malicious: 8.		Completed
C:\ProgramData\SpeedBit\DAP\Plugins\189AE673-13C1-4133-A470-8C4DDD1ACB8C\1.0.1...	12 KB	Clean
C:\Program Files\WindowsApps\SharedLimitedTime\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\SharedLimitedTime\microsoft.windowscommunicationsap...	10 KB	Clean

When all the files are analyzed, you will receive a detailed report at **domersa@yopmail.com**

Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit 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.

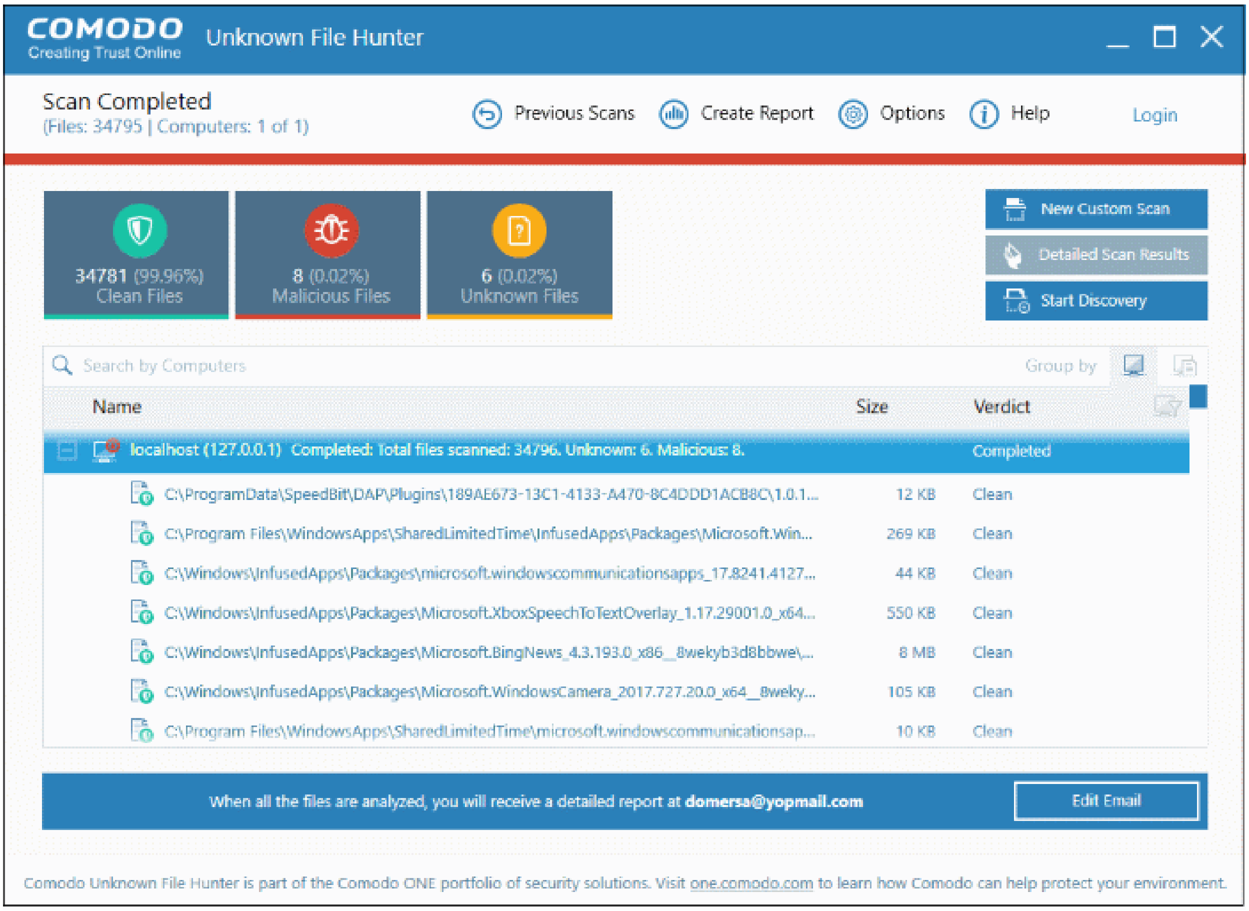
- **Current Scan interface** – Full results of the most recent scan.
- **Previous Scan interface** – A list of all previously run scans. Expand any scan to view per-endpoint results.

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

Previous Scans	Current Scan

Current Scan Results

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



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

34781 (99.96%) Clean Files

8 (0.02%) Malicious Files

6 (0.02%) Unknown Files

Name	Size	Verdict
localhost (127.0.0.1) Completed: Total files scanned: 34796. Unknown: 6. Malicious: 8.		Completed
C:\ProgramData\SpeedBit\DAP\Plugins\189AE673-13C1-4133-A470-8C4DDD1ACB8C\1.0.1...	12 KB	Clean
C:\Program Files\WindowsApps\SharedLimitedTime\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\SharedLimitedTime\microsoft.windowscommunicationsap...	10 KB	Clean

When all the files are analyzed, you will receive a detailed report at **domersa@yopmail.com**

Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

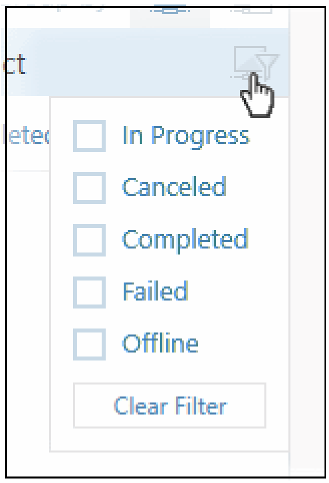
- Click '+' beside a hostname to view all files analyzed on the endpoint. Double-click on any file to view file details.
- The tiles above the results table show the total number of unknown, malicious and clean files.
  - 'Unknown' means no trust rating is available for the file. After expert analysis 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	The trust rating of the file. The possible values are: • Completed – Unknown file which has been successfully uploaded to Valkyrie for analysis. • In Analysis – Unknown file which is currently being tested by Valkyrie • Clean – Files found to be safe after Valkyrie analysis • Malicious – Files found to be unsafe after FLS and Valkyrie analysis • 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.

Searching, sorting and filtering Options

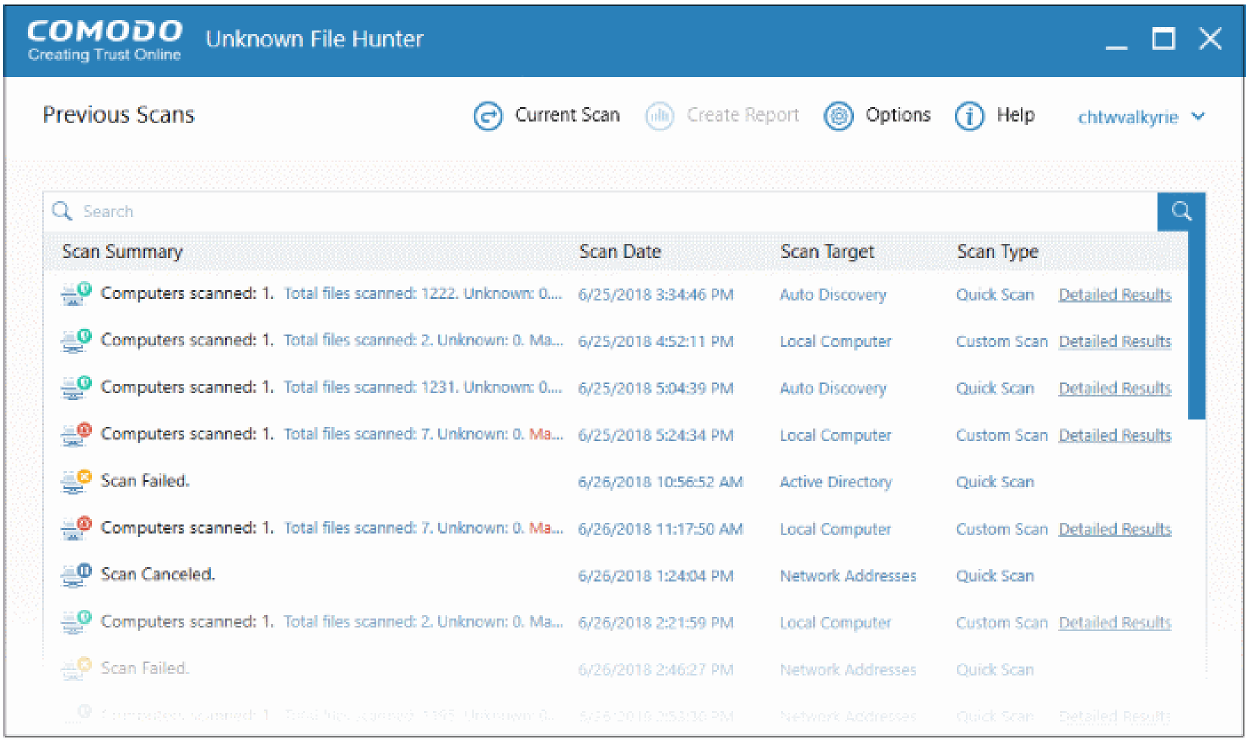
- Use the search box to look for endpoints by name or IP address. Clear the search box to display all endpoints again.
- Click the column headers to sort results by name, size and verdict.
- Click the funnel icon at the end of 'Name' column to choose result filters:



Previous Scans Results

- Click 'Previous Scans' at the top

The results of the previous scans will be shown:

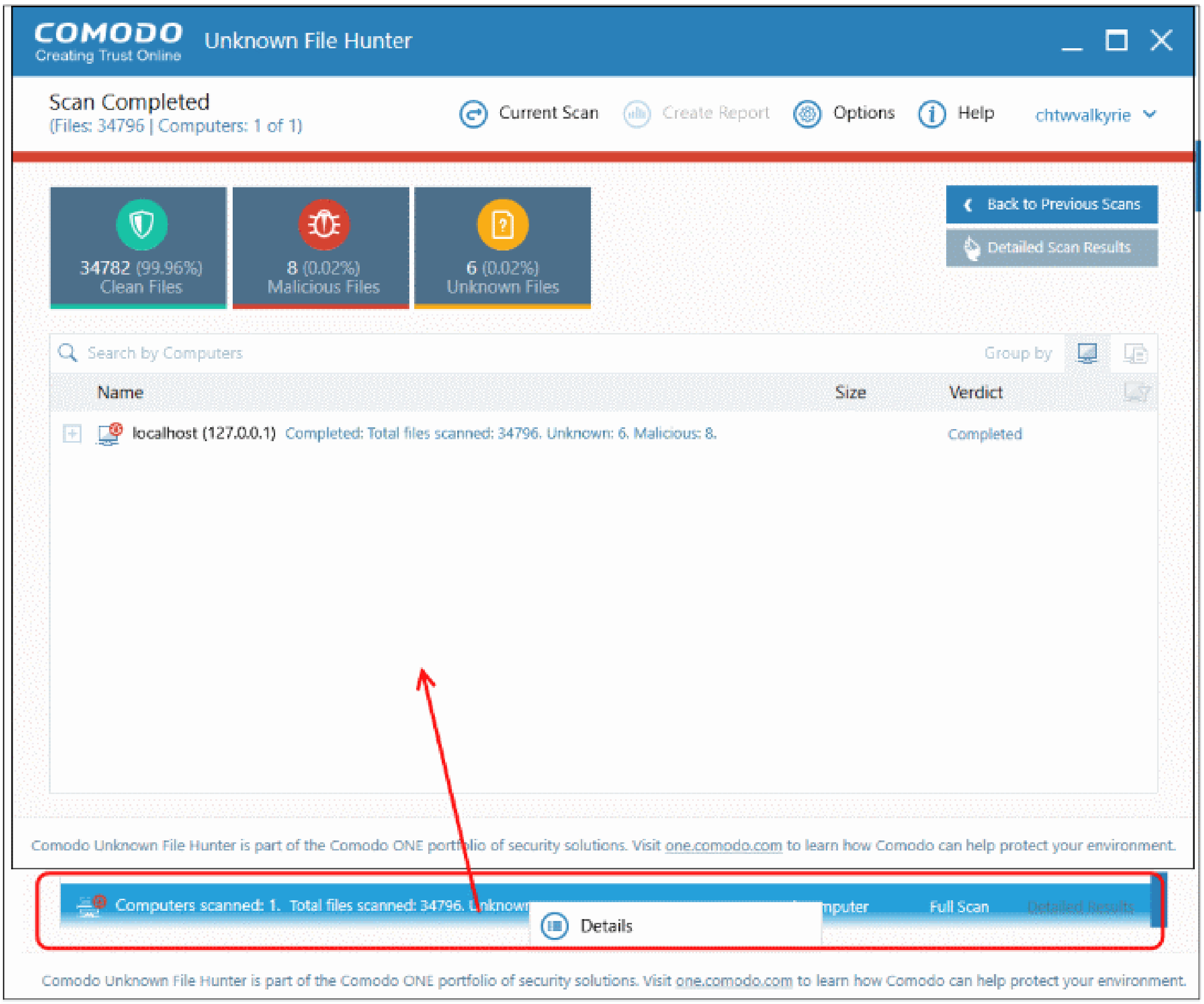


Scan Summary		Scan Date	Scan Target	Scan Type	
Computers scanned: 1.	Total files scanned: 1222. Unknown: 0....	6/25/2018 3:34:46 PM	Auto Discovery	Quick Scan	Detailed Results
Computers scanned: 1.	Total files scanned: 2. Unknown: 0. Ma...	6/25/2018 4:52:11 PM	Local Computer	Custom Scan	Detailed Results
Computers scanned: 1.	Total files scanned: 1231. Unknown: 0....	6/25/2018 5:04:39 PM	Auto Discovery	Quick Scan	Detailed Results
Computers scanned: 1.	Total files scanned: 7. Unknown: 0. Ma...	6/25/2018 5:24:34 PM	Local Computer	Custom Scan	Detailed Results
Scan Failed.		6/26/2018 10:56:52 AM	Active Directory	Quick Scan	
Computers scanned: 1.	Total files scanned: 7. Unknown: 0. Ma...	6/26/2018 11:17:50 AM	Local Computer	Custom Scan	Detailed Results
Scan Canceled.		6/26/2018 1:24:04 PM	Network Addresses	Quick Scan	
Computers scanned: 1.	Total files scanned: 2. Unknown: 0. Ma...	6/26/2018 2:21:59 PM	Local Computer	Custom Scan	Detailed Results
Scan Failed.		6/26/2018 2:46:27 PM	Network Addresses	Quick Scan	
Computers scanned: 1.	Total files scanned: 1395. Unknown: 0....	6/26/2018 2:53:30 PM	Network Addresses	Quick Scan	Detailed Results

Previous Scan Results Interface - Table of Column Descriptions

Column Header	Description
Scan Summary	Indicates the status of scans. • Scan Failed – The scan was unsuccessful. • Scan Canceled – The scan was canceled by the admin. • Computer scanned – The number beside it indicates the number of endpoints that were scanned for that scan.
Scan Date	The date and time the scan was run.
Scan Target	Indicates the type of scan: • Auto Discovery – Scan run on discovered endpoints on the network • Active Directory – Scan run on endpoints which belong to an Active Directory domain • Network Addresses – Scan executed by specifying their host name/IP address, or scan all endpoints on an IP range • Local Computer – Scan run on the local device
Scan Type	Indicates whether it is a quick or full scan
Detailed Results	Click this link to open **https://valkyrie.comodo.com** 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


COMODO Creating Trust Online
Unknown File Hunter
Scan Completed
(Files: 34796 | Computers: 1 of 1)
Current Scan
Create Report
Options
Help
chtwvalkyrie
34782 (99.96%) Clean Files
8 (0.02%) Malicious Files
6 (0.02%) Unknown Files
Back to Previous Scans
Detailed Scan Results
Search by Computers
Group by
Name
Size
Verdict
localhost (127.0.0.1) Completed: Total files scanned: 34796. Unknown: 6. Malicious: 8.
Completed
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.
Computers scanned: 1. Total files scanned: 34796. Unknown
mputer
Full Scan
Detailed Results
Details
Comodo Unknown File Hunter is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

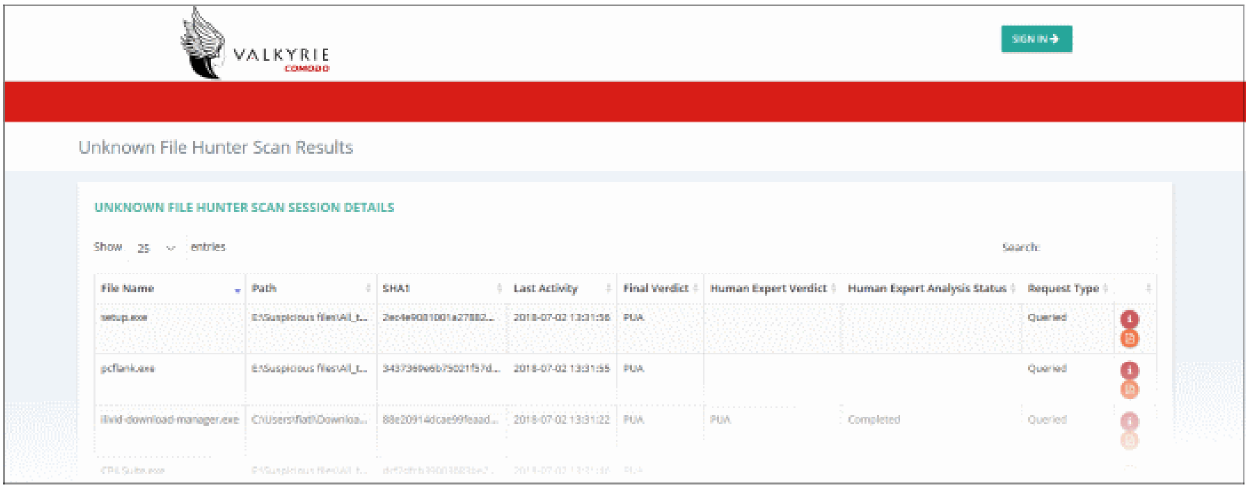
The interface is similar to current scan results explained above.

- 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, 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:



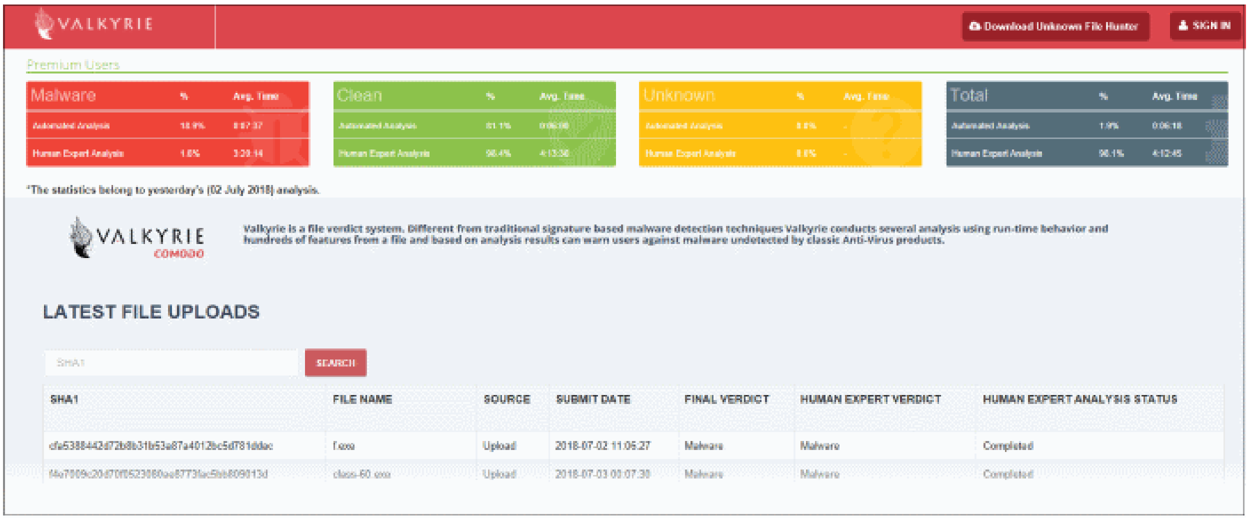
Unknown File Hunter Scan Results

UNKNOWN FILE HUNTER SCAN SESSION DETAILS

Show 25 entries Search:

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Request Type	
setup.exe	E:\Suspicious files\All_t...	2ec4e9081001a27882...	2018-07-02 13:31:56	PUA			Queried	
pcflank.exe	E:\Suspicious files\All_t...	3437369e6b75021f57d...	2018-07-02 13:31:55	PUA			Queried	
ilivid-download-manager.exe	C:\Users\fat\Downloa...	88e20914dcae99feaad...	2018-07-02 13:31:22	PUA	PUA	Completed	Queried	
CPLSuite.exe	E:\Suspicious files\All_t...	[illegible]	2018-07-02 13:31:[illegible]	PUA				

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



Malware	%	Avg. Time
Automated Analysis	18.9%	0:07:37
Human Expert Analysis	1.6%	3:20:14

Clean	%	Avg. Time
Automated Analysis	81.1%	0:06:30
Human Expert Analysis	98.4%	4:13:30

Unknown	%	Avg. Time
Automated Analysis	0.0%	-
Human Expert Analysis	0.0%	-

Total	%	Avg. Time
Automated Analysis	1.9%	0:06:18
Human Expert Analysis	98.1%	4:12:45

*The statistics belong to yesterday's (02 July 2018) analysis.

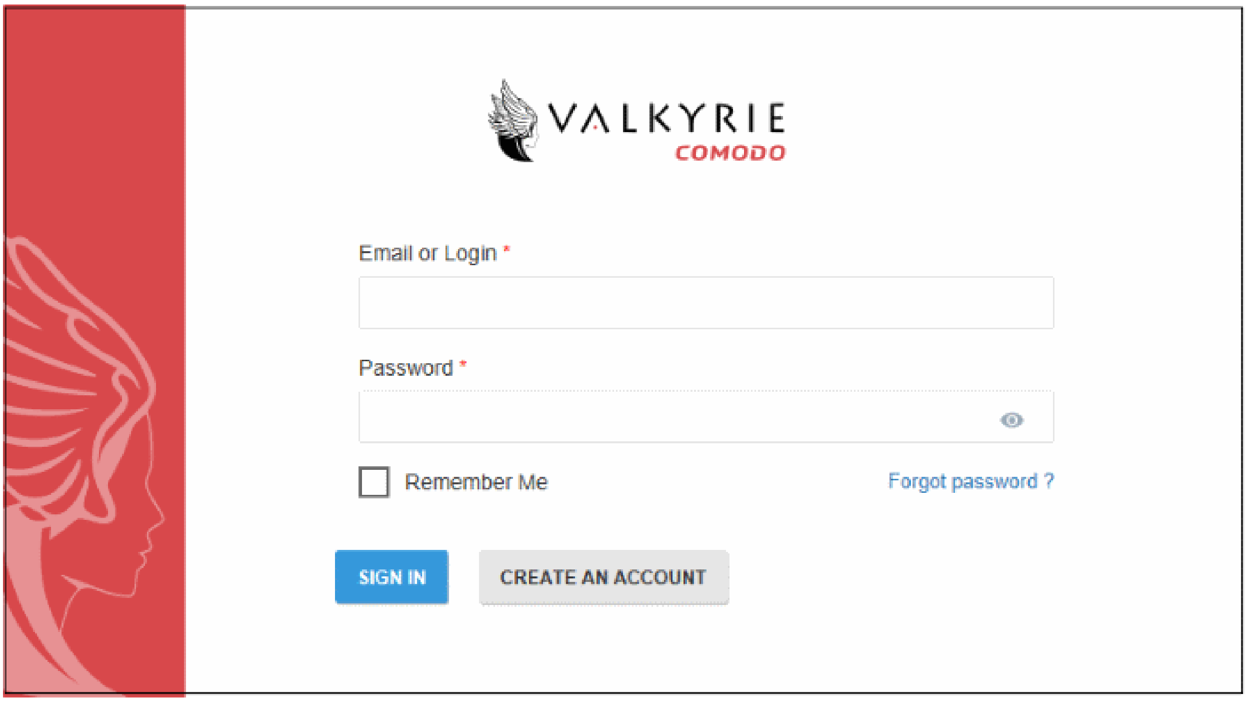
Valkyrie is a file verdict system. Different from traditional signature based malware detection techniques Valkyrie conducts several analysis using run-time behavior and hundreds of features from a file and based on analysis results can warn users against malware undetected by classic Anti-Virus products.

LATEST FILE UPLOADS

SHA1

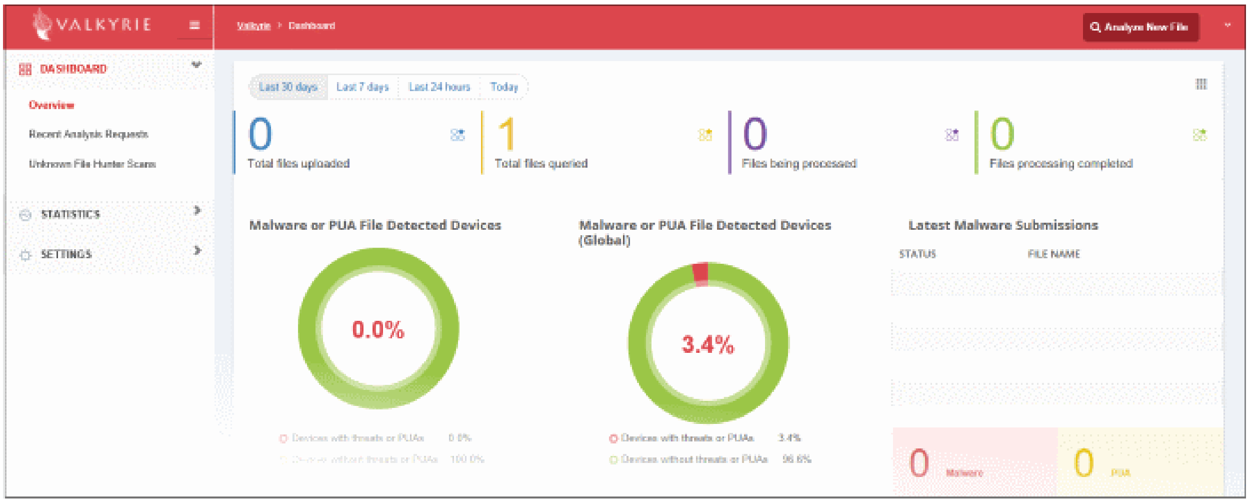
SHA1	FILE NAME	SOURCE	SUBMIT DATE	FINAL VERDICT	HUMAN EXPERT VERDICT	HUMAN EXPERT ANALYSIS STATUS
cfa5388442d72b8b31b53a87a4012bc5d781ddac	f.exe	Upload	2018-07-02 11:06:27	Malware	Malware	Completed
f4a7009c20d70f0523080aa8773facf5bb809013d	class-60.exe	Upload	2018-07-03 00:07:30	Malware	Malware	Completed

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

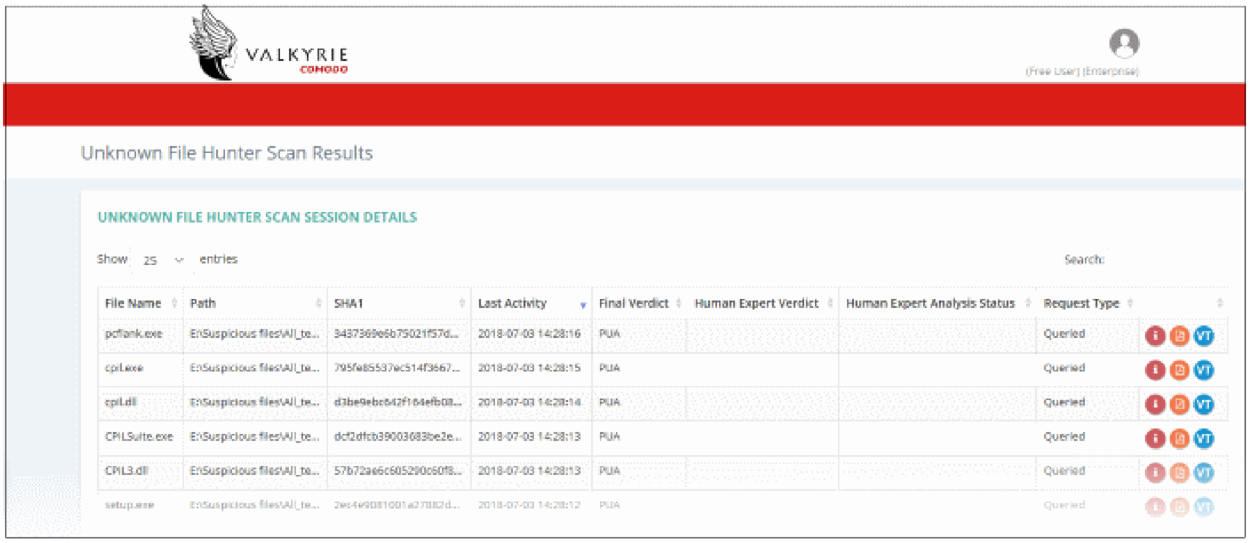


- C1 customers can use their C1 credentials to login.
- If you do not have an account, click the 'Create an account' link, provide the required details and sign up for an account, which is free.
- If you already have an Valkyrie account, enter the credentials and click the 'Sign In' button.

The 'Dashboard' page will be displayed by default.


VALKYRIE
Valkyrie > Dashboard
Analyze New File
DASHBOARD
Overview
Recent Analysis Requests
Unknown File Hunter Scans
STATISTICS
SETTINGS
Last 30 days
Last 7 days
Last 24 hours
Today
0
Total files uploaded
1
Total files queried
0
Files being processed
0
Files processing completed
Malware or PUA File Detected Devices
0.0%
Devices with threats or PUAs 0.0%
Devices without threats or PUAs 100.0%
Malware or PUA File Detected Devices (Global)
3.4%
Devices with threats or PUAs 3.4%
Devices without threats or PUAs 96.6%
Latest Malware Submissions
STATUS
FILE NAME
0 Malware
0 PUA

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.



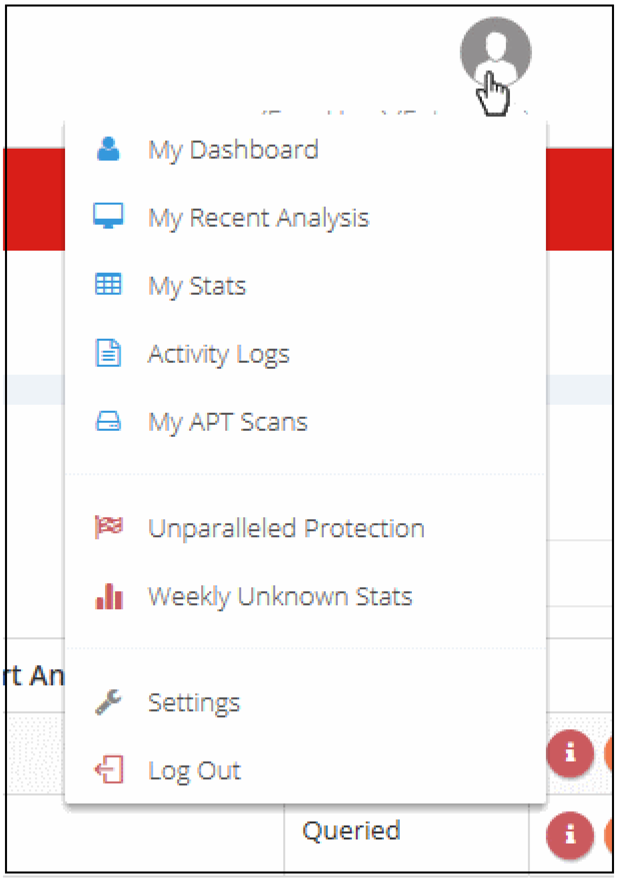
Unknown File Hunter Scan Results

UNKNOWN FILE HUNTER SCAN SESSION DETAILS

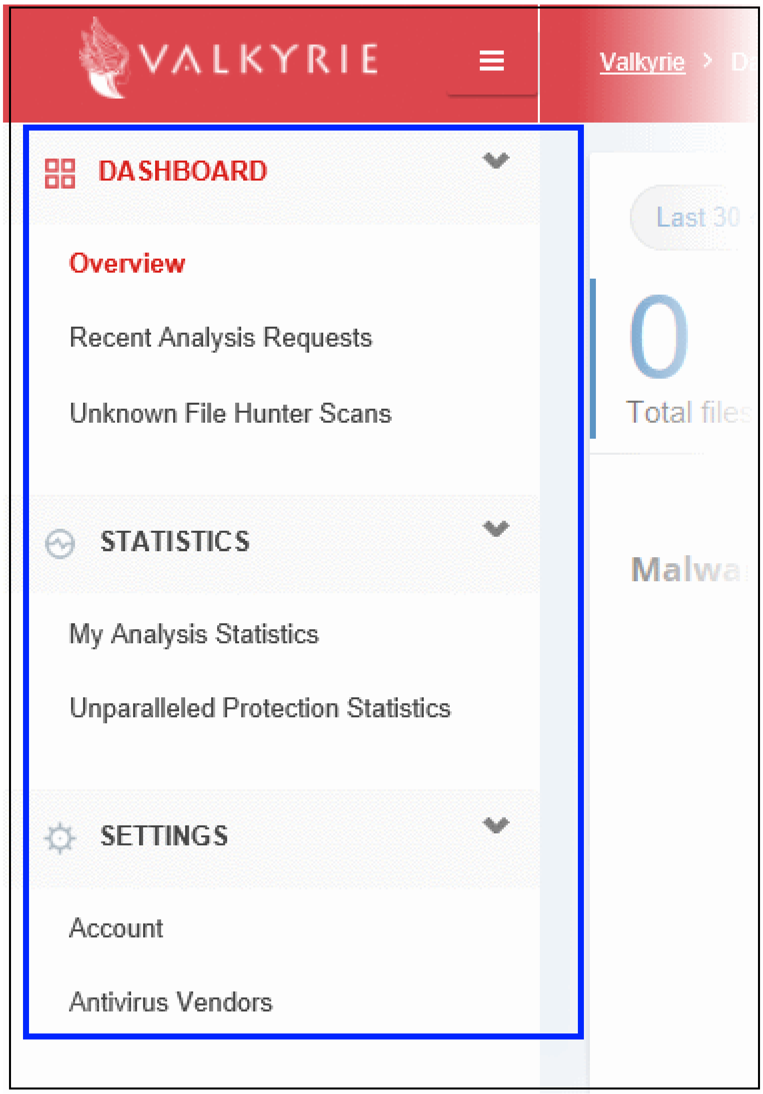
Show 25 entries Search:

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Request Type	
pcflank.exe	E:\Suspicious files\All_te...	3437369e6b75021f57d...	2018-07-03 14:28:16	PUA			Queried	i 🗎 VT
cpl.exe	E:\Suspicious files\All_te...	795fe85537ec514f3667...	2018-07-03 14:28:15	PUA			Queried	i 🗎 VT
cpl.dll	E:\Suspicious files\All_te...	d3be9ebc642f164efb08...	2018-07-03 14:28:14	PUA			Queried	i 🗎 VT
CPILSuite.exe	E:\Suspicious files\All_te...	dcf2dfcb39003683be2e...	2018-07-03 14:28:13	PUA			Queried	i 🗎 VT
CPIL3.dll	E:\Suspicious files\All_te...	57b72ae6c605290c60f8...	2018-07-03 14:28:13	PUA			Queried	i 🗎 VT
setup.exe	E:\Suspicious files\All_te...	2ec4e9081001a27882d...	2018-07-03 14:28:12	PUA			Queried	i 🗎 VT

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:



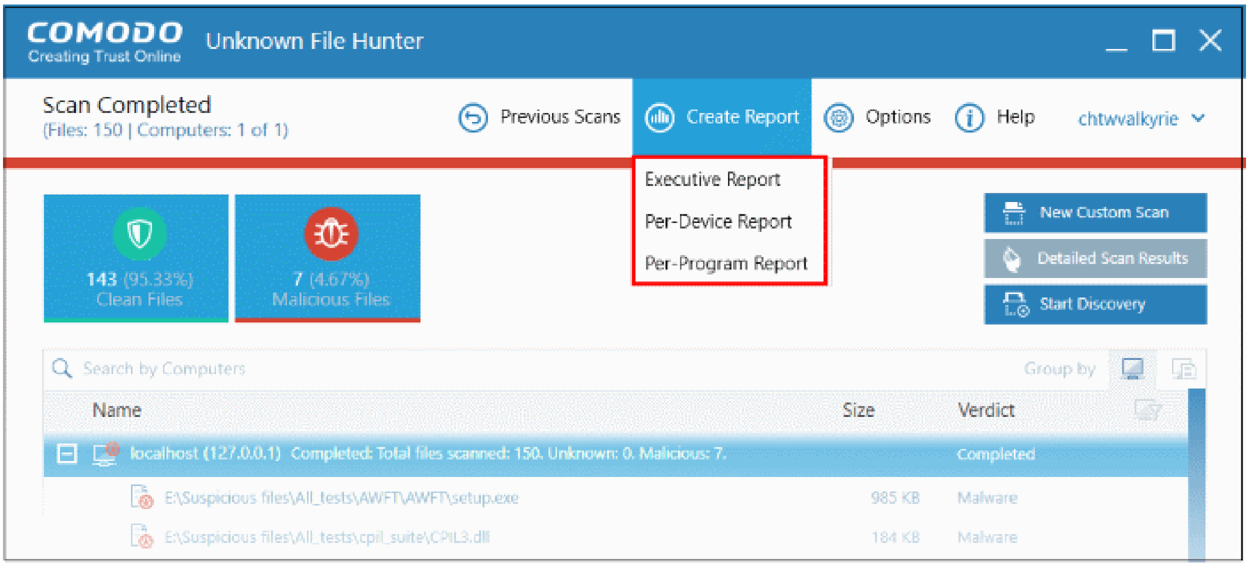
See our dedicated Valkyrie guide at **https://help.comodo.com/topic-397-1-773-9567-Valkyrie-Analysis-Results.html** for more information.

5 Reports

Report 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



Name	Size	Verdict
localhost (127.0.0.1) Completed: Total files scanned: 150. Unknown: 0. Malicious: 7.		Completed
E:\Suspicious files\All_tests\AWFT\AWFT\setup.exe	985 KB	Malware
E:\Suspicious files\All_tests\cpil_suite\CPIL3.dll	184 KB	Malware

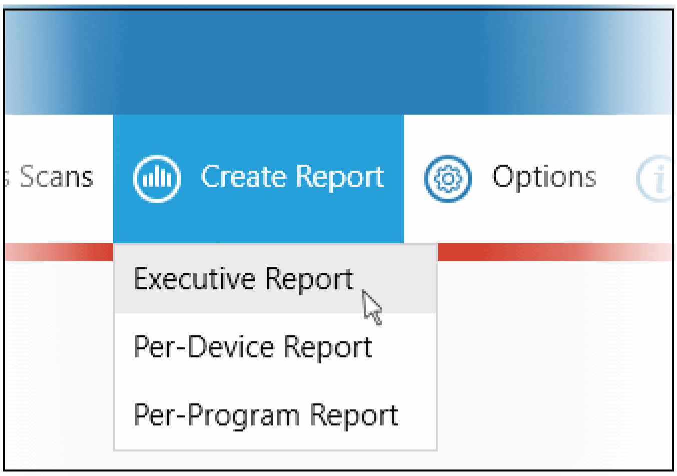
See the following sections for help on each report type:

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

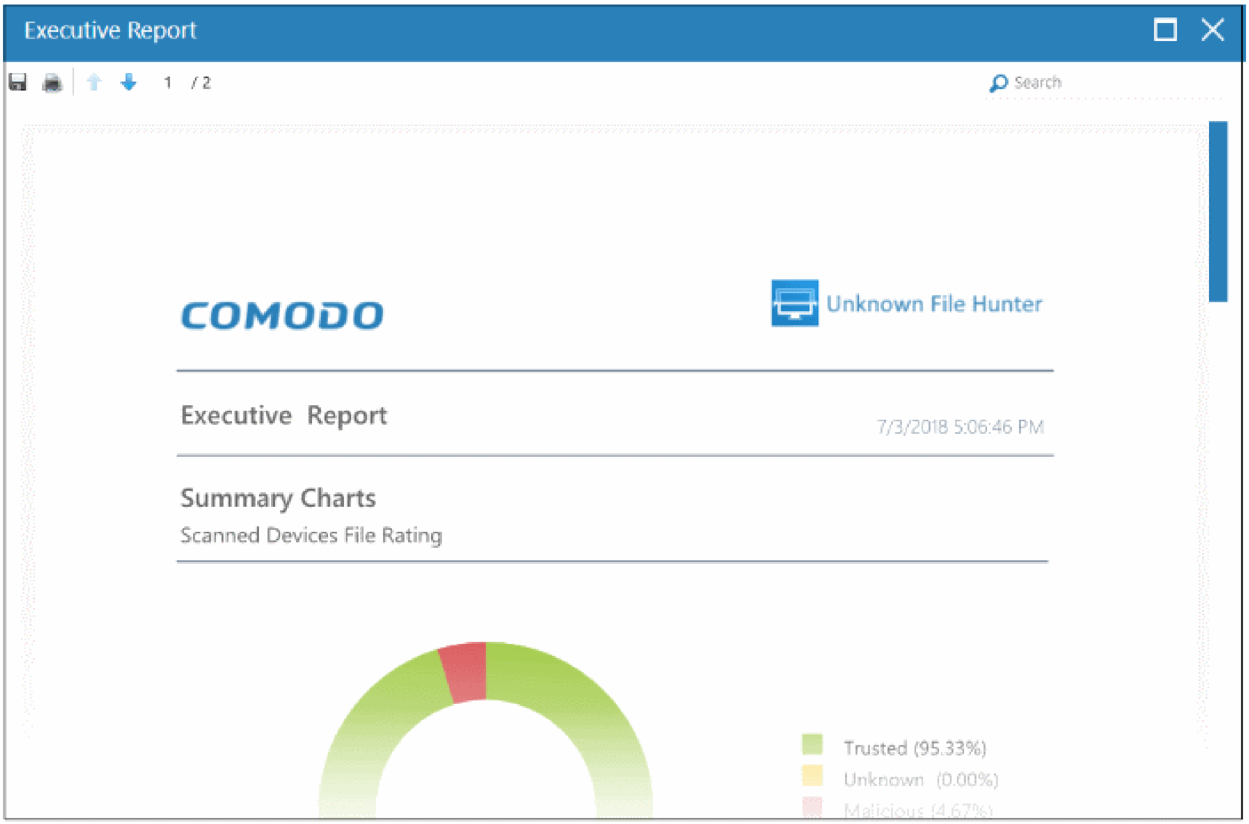
5.1 Executive Report

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:



Executive Report 7/3/2018 5:06:46 PM

Summary Charts
Scanned Devices File Rating

🟩 Trusted (95.33%)
🟨 Unknown (0.00%)
🟥 Malicious (4.67%)

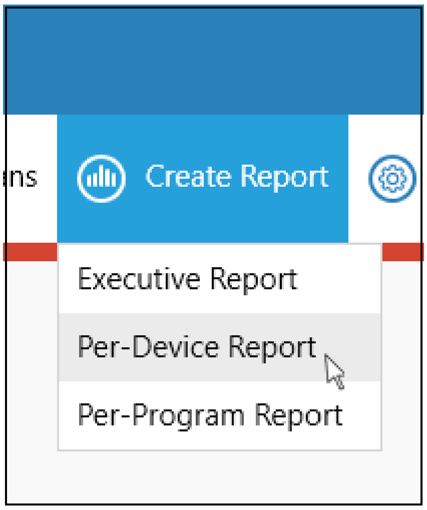
Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **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.

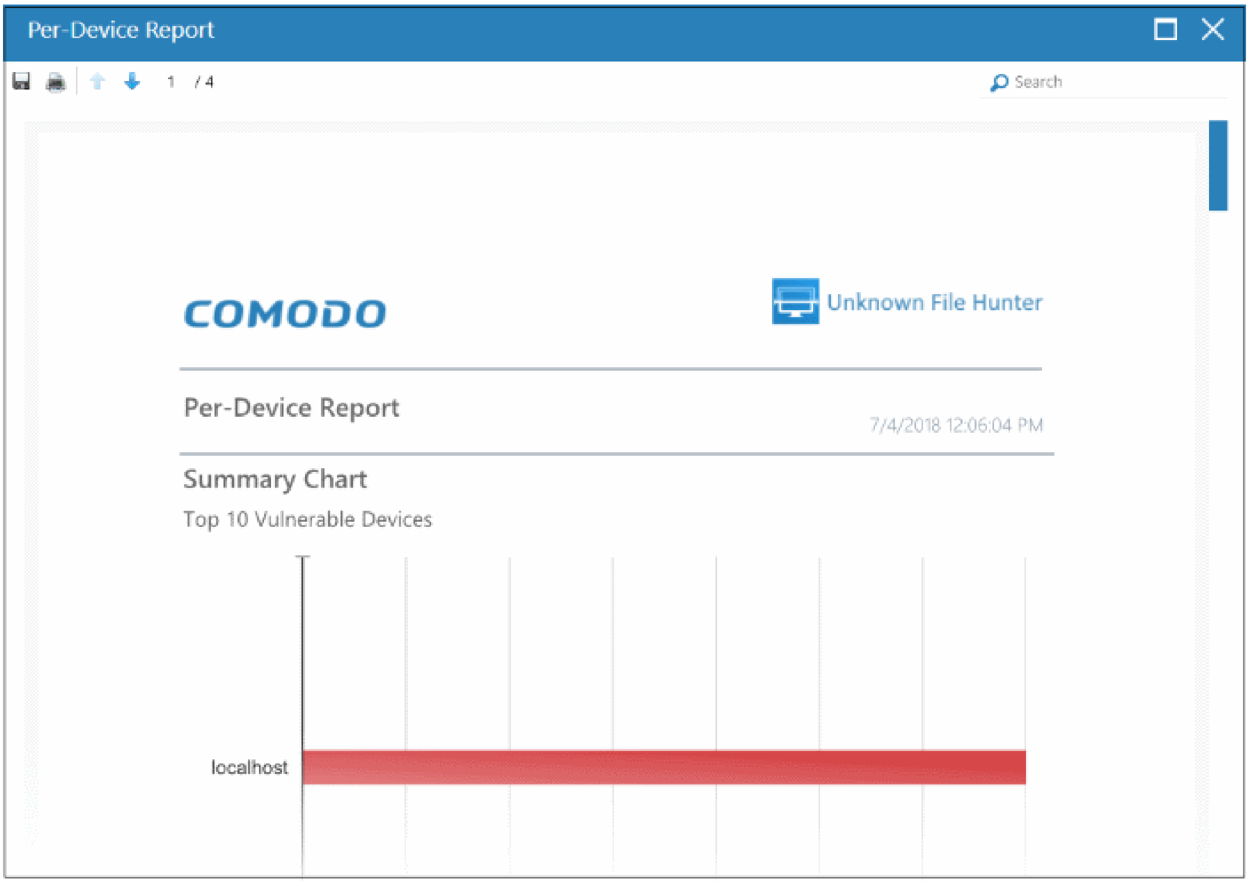
5.2 Device Report

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.

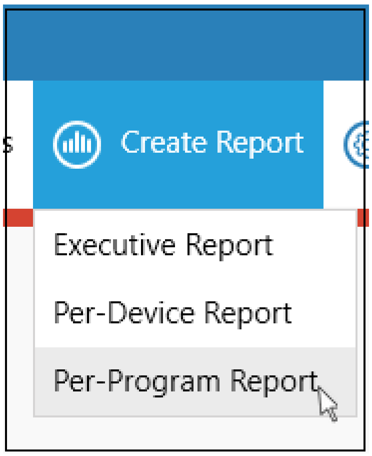
- **Summary Chart -** Provides the details in bar graph the top 10 endpoints that are detected with unknown/malware files.

- **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.

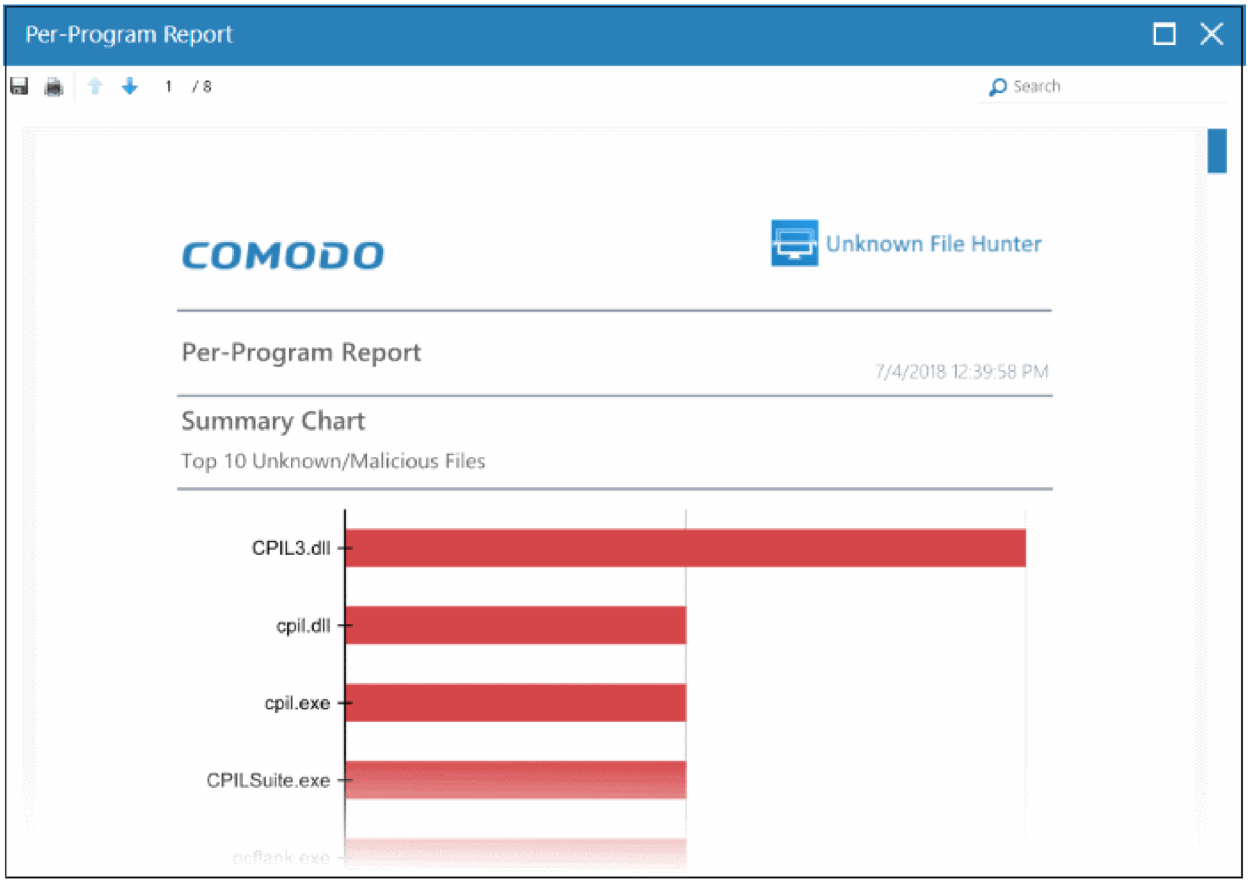
5.3 Program Report

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).



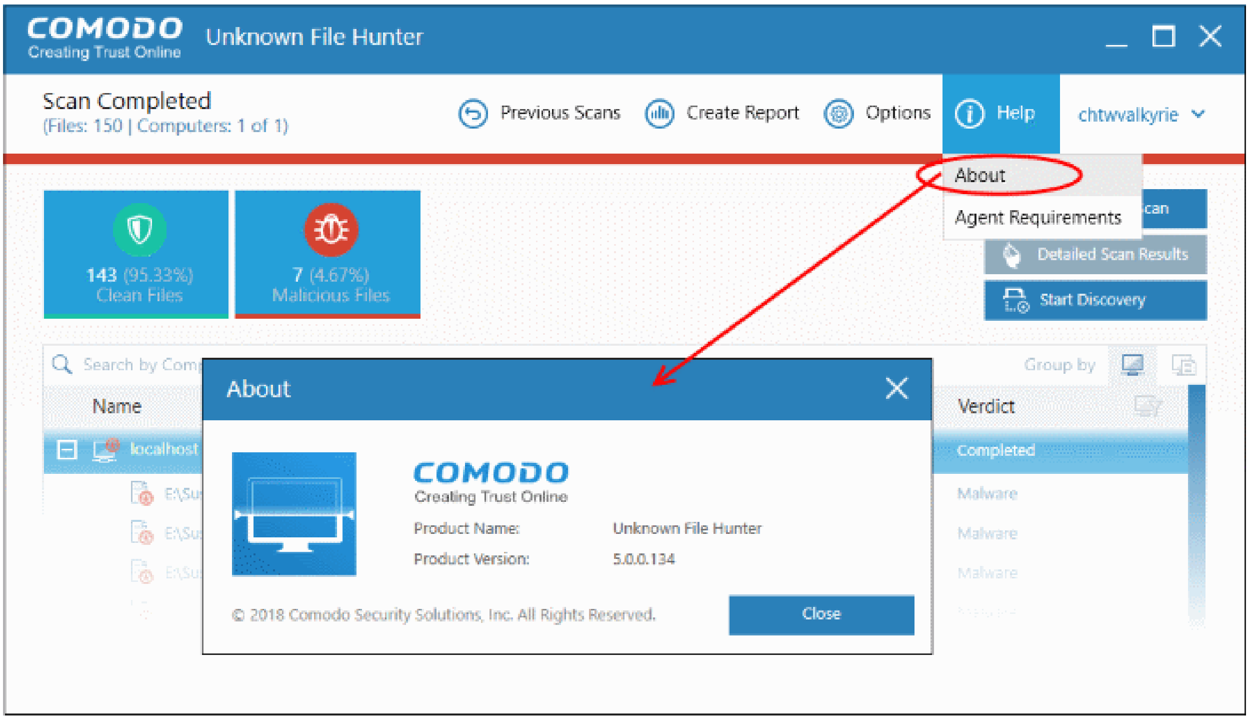
Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **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:



About

Product Name: Unknown File Hunter

Product Version: 5.0.0.134

© 2018 Comodo Security Solutions, Inc. All Rights Reserved.

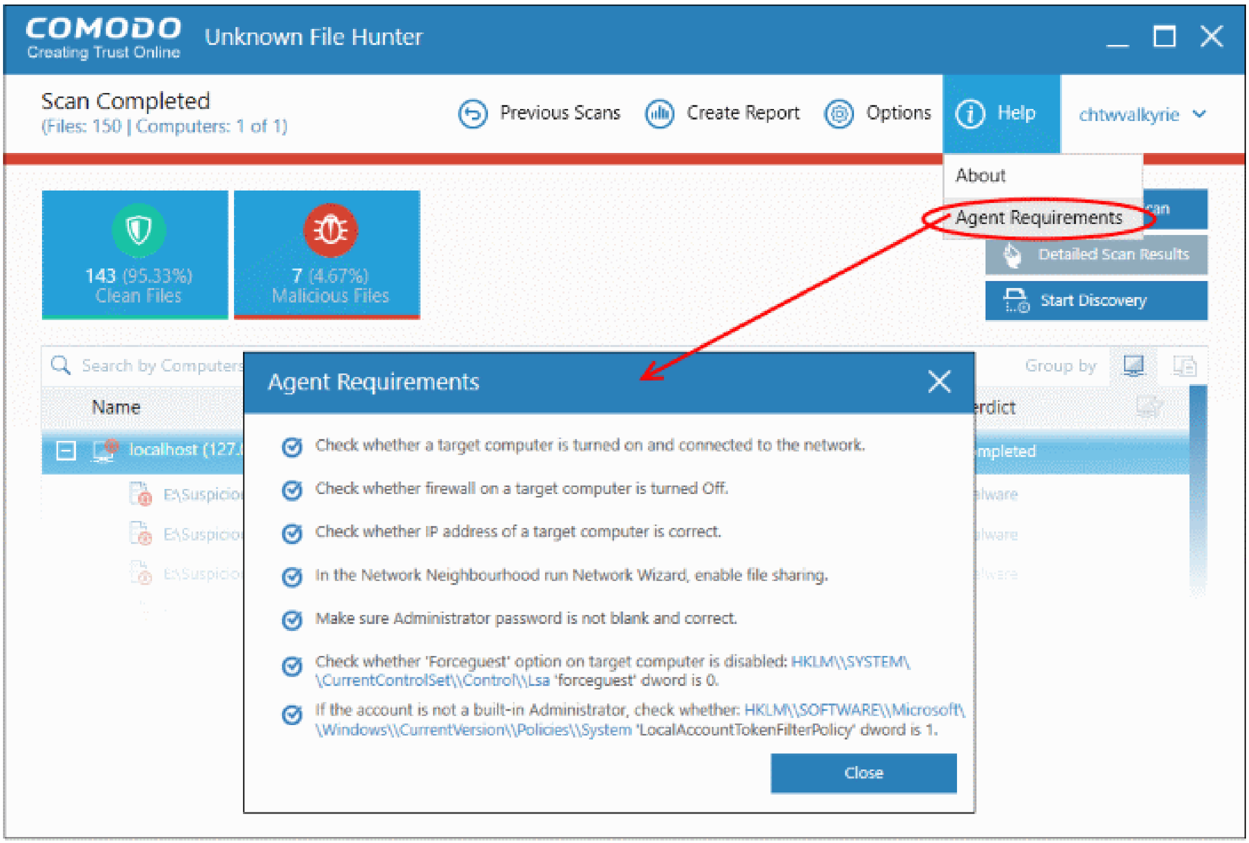
Close

- 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:



Agent Requirements

- Check whether a target computer is turned on and connected to the network.
- Check whether firewall on a target computer is turned Off.
- Check whether IP address of a target computer is correct.
- In the Network Neighbourhood run Network Wizard, enable file sharing.
- Make sure Administrator password is not blank and correct.
- Check whether 'Forceguest' option on target computer is disabled: HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa 'forceguest' dword is 0.
- If the account is not a built-in Administrator, check whether: HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System 'LocalAccountTokenFilterPolicy' dword is 1.

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.636

Tel : +1.703.581.6361

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**