



# Comodo Unknown File Hunter

Software Version 5.0

# Administrator Guide

Guide Version 5.0.091619

Comodo Security Solutions 1255 Broad Street Clifton, NJ 07013



### **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	
4.1 Comodo Unknown File Hunter Scan Results	29
4.2 Valkyrie Analysis Results	
5 Reports	
5.1 Executive Report	
5.2 Device Report	
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.



#### 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:

COMODO

#### 🔄 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\UnknownFileHunte	er	
	OK	Cancel

 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.

🖶 Com	nodo Unknown File Hunter 100%	×
Ð	Starting	
	Cancel	

• 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 H	lunter
	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
	Cancel I ACCEPT

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

COMODO

ting Trust Online					_ U
0% Searching for Available Devices	Previous Scans	(III) Create Report	Options	(i) Help	
4 Devices Found				j	iscovery
Computers					
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	

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

COMODO Creating Trust Online Unknown File Hunter				_ 🗆 ×
Discovery Completed	Previous Scans	🐽 Create Report	Options (i)	Help Login
4 Devices Found				Scan Now Custom Scan Restart Discovery
Q Search by Computers				
Name			IP	
10.0.2.2			10.0.2.2	
II. 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 po	ortfolio of security solution	s. Visit <u>one.comodo.com</u> (	to learn how Comodo can f	help protect your environment.

## 2.1 The Main Interface

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

COMODO Unknown File Hur	nter V	_ 0
Discovery Completed	Previous Scans Create Report	Options () Help Login
4	Controls	🔚 Scan Now
Q Search by Computers Name		Restart Discovery
10.0.2.2	Main Display Area	10.0.2.2
10.0.2.3		10.0.2.3
10.0.2.4		10.0.2.4
DESKTOP-HI9508N.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.

Options				×
FLS	TCP Port	80		
FLS	UDP Part	53		
	Ca	ncel	Save	

Help – Contains 'About' and 'Agent Requirements'

COMODO

'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.

COMODO Creating Trust Online Unknown File Hunter					_ 🗆 ×
Scan Completed (Files: 9   Computers: 1 of 1)	Previous Scans	(h) Create Report	Options	(i) Help	Login
2 (22.22%) Clean Files 7 (77.78%) Malicious Files				Detailed S	iom Scan ican Results iovery
Watch out! Malware Is Detect Comodo Unknow File Hunter has scann that you reconsider your current security <u>Comodo Advanced Endpoint Protection</u> and reporting capabilities. It follows "Do unknown files inside a secure container use such unknown files with no impact t	ted! In your environment and dete posture to eliminate the dan keeps your endpoints free frr fault Deny' posture which allo until a definitive verdict of 'ge to the usability and yet no han	sted malware on one or ger of infecting your end om malware now and in t ws known files to freely is ded' or "bad" is delivered m to the system.	more of the system points. he future and provi un, blocks bad files . Comodo Auto-Cor	s. We recommend des essential manage and automatically lau ntainment <sup>74</sup> feature al	ment inches lows to
When all the files are analyzed, Comodo Unknown File Hunter is part of the Comodo ONI	you will receive a detailed rep	ort at <b>domersa@yopma</b> s. Visit one.comodo.com	<b>il.com</b> to learn how Como	Edit t	Email our environment.

COMODO

## 2.2 Login to UFH

• Open the UFH executable to start the application.

COMODO Creating Trust Online Unknown File Hunter					_ 🗆 ×
Discovery Completed	Previous Scans	🐽 Create Report	Options	(i) Help	Login
				i≡ so	an Now
					istom Scan
A Devices Found					start Discovery
Q English by Computers					

- 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.

Comodo ONE login	×
Please sign in with Comodo License Account credentials to analyze files with Valkyrie	Please sign up to Comodo ONE if you don't have a Comodo ONE account yet
Enter User Name	Valkyrie which is a service provided in <u>Comodo ONE</u> is a cloud-based file analysis service for submitted known and unknown files with a range of static and
Enter Password	dynamic detectors including file lookup, heuristics and real-time behaviour analysis
Enter LICENSE	
OK <u>Continue a</u>	s Guest User Sign Up

- 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.

COMODO Unknown File Hunter		_ 🗆 ×
Discovery Completed	Servious Scans (III) Create Report	Ø Options         (i) Help         Guest          ✓
4 Devices Found		Scan Now Custom Scan Restart Discovery
Q Search by Computers		
Name		IP
		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 p	ortfolio of security solutions. Visit <u>one.comodo.com</u>	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

COMODO

### 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		_ 🗆 ×
Start Scan Wizard	×	(j) Help Login
Select Scan Targets + + + + + + + + + + + + + + + + + + +	Network Addresses Scan computers with specified IP addresses or endpoint names	Scan Now Custom Scan
Workgroup Scan computers selected from Workgroups	This Computer Scan This Computer	
Comodo Unknown File Hunter is part of the Comodo ONE port	Cancel	do can help protect your environment

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

COMODO

Start Scan Wiz	ard		×
Ŷ	Active Directory Creden	tials	
	Domain Name	Enter Domain Name	
	Domain Administrator	Enter Domain\Administrator	
	Password	Enter Password	10
Back			Next

- 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.

COMODO

Start Scan Wiz	ard	×
	Select Computers	
	<ul> <li>mike</li> <li>Computers</li> <li>Domain Controllers</li> </ul>	
Back	Next	

- 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

8% Scan In Progress iles: 1738   Computers: 1 of 3)	🕞 Previous Scans 🏾 ᆒ Create Report	: 🍥 Options 🌔	Help chtv		
(99.88%) <b>1736</b> (99.88%) Clean Files In Analysis			Stop Scan		
2 Search by Computers			Group by		<u>.</u>
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) Complete	d: Total files scanned: 778. Unknown: 0. Malicious: 0.		Completed		
DESKTOP JKLMNOP This compute	r is not accessible.		Offline		
When all the files are analyzed,	you will receive a detailed report at <b>chrisgaylec1operatio</b>	ns@gmail.com	Edit E	mail	X9.10

- '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:

(99.88%) 1736 (99.88%) Clean Files	Safe files. These files are on the Comodo whitelist are OK to run.
<b>3</b> (0.14%) In Analysis	<ul> <li>Unknown, potentially malicious files.</li> <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 https://valkyrie.comodo.com/login</li> <li>You also can sign into Valkyrie with your Comodo Dragon / Comodo One username and password.</li> <li>See 'Valkyrie Analysis Results' for more information.</li> </ul>

COMODO



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:

		1		
Grou	p by		<u>F</u>	
Verdict			(Ly	)
In Progres		n Prog	ress	]
In Progres		Cancele Comple	ed eted	
Offline		Failed		
		Offline		
	C	lear Filt	er	]

Results are shown when the scan finishes:

COMODO

COMODO Creating Trust Online Unknown File Hunter		_ 0	×
Scan Completed (Files: 2099   Computers: 2 of 3)	Options (	i) Help chtwvalkyrie v	~
<b>2099</b> (100%) Clean Files		Back to Previous Scans     Detailed Scan Results	
Q Search by Computers		Group by	
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_x648wekyb	64 MB	Clean	
C\Python27\python.exe	27 KB	Clean	
c:\program files\windowsapps\microsoft.windows.photos_2018.18041.15530.0_x648wekyb	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 <u>one.comodo.com</u> to lea	am how Comode	o can help protect your environm	nent.

	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:
	<ul> <li>In Progress – Unknown file which is queued for upload to Valkyrie, Comodo's file analysis system</li> </ul>
	<ul> <li>Uploading – Unknown file which is currently being submitted to Valkyrie</li> </ul>
	<ul> <li>In Analysis – Unknown file which is currently being tested by Valkyrie</li> </ul>
	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
	<ul> <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

		New Custom Se	
7 (100%)		🔌 Detailed Scan R	tesults
Malicious Files		Start Discovery	
🔍 Search by Computers		Group by	
	E	Mandlet	100

· Click the computer icon to view results by computer:

			Options	(j) Help ch	twvalkyrie 💙
7 (100%) Malicious Files				New Cus Detailed	stom Scan Scan Results covery
Q Search by Computers				Group by	
Name			Size	Verdict	⊑r⁄
Iocalhost (127.0.0.1) Completed:	Total files scanned: 7. Unknown: 0. Malicious: 7	τ.		Completed	

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

COMODO

Name	Size	Verdict
Iocalhost (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
C\Suspicious files\All_tests\cpil_suite\cpil.dll	60 KB	Malware

#### Group by File

· Click the computer with file icon on the right

7 (100%) Malicious Files		Detailed Scan Results
Search by Files		Group by 🗔 🚺
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		
Iocalhost (127.0.0.1) E\Suspicious files\All_tests\cpil_suite\CPIL3.dll		
EPILSuite.exe (CPILSuite.exe) 1 instance.	1 M8	Malware
🗄 🛅 setup.exe 1 instance.	985 KB	Malware
🗄 🐻 pcflank.exe (PCFlankLeaktest) 1 instance.	176 KB	Malware
cpil.exe 1 instance.	104 KB	Malware

• 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:

COMODO

<b>VALKYRIE</b>	=	Vallorie > Dashboard							Q, Analyze New File
EE DASHBOARD	٣	Last 30 days Last 7 days Last 24	hours Too	tay)					
Recent Analysis Requests Unknown file Hunter Scans		O Total files uploaded	88 <b>*</b> Te	tal files queried	88	O Files being processed	25	O Files processing co	88
😔 STATISTICS O: SETTINGS	>	Malware or PUA File Detected	Devices	Malwa (Globa	re or PUA File Do	etected Devices	Latest Ma status	Iware Submission FILE NAME	5
		0.0%			3.6%				
		<ul> <li>Devices with threats or PUAs</li> <li>Devices without threats or PUAs</li> </ul>	0.0% 100.0%	01	Devices with threats or I Devices without threats	PUAs 3.6% or PUAs 96.4%	O Matwa	. 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 Start Scan Wizard	Previous Scans (In) Create Report (In) Options	(i) Help Login
Select Scan Targets  + + + + + + + + + + + + + + + + + +	Network Addresses Scan computers with specified IP addresses or endpoint names	E Scan Now Custom Scan
+ :	This Computer Scan This Computer Cancel	
Comodo Unknown File Hunter is part of the Comodo ONE p	ortfolio of security solutions. Visit one.comodo.com to learn how Como	do can help protect your environment.

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

COMODO

Start Scan Wizard	l i i i i i i i i i i i i i i i i i i i			×
	Specify Workgroup			
	Search Available Workgroups (m	ay take some time)		
	<ul> <li>Use Known Workgroup Name</li> </ul>	Enter Workgroup Nam	e	
Back			Next	

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

Start Scan Wizard	×
Select Computers	
C1TEST	
Back	Next

COMODO

Start Scan Wiza	ard			×
XXX	Scan Credentials			
	Login	Enter Login		
	Password	Enter Password	1	
Back		Quick Scan	F	ull 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:

COMODO

				_ [	
4% Scan In Progress iles: 1680   Computers: 0 of 4)	🕤 Previous Scans 🔟 Create Report	i Options	(i) Help	Guest	: <b>~</b>
1680 (100%) Clean Files			Stop Sca	an	
2 Search by Computers			Group by		P
Name		Size	Verdict		
C1TWIN8132 (10.8.64.174) 360 files sc	anned (24.73%). Unknown: 0. Malicious: 0.		In Progress		
C1TWIN8164 (10.8.64.225) 720 files sc	anned (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@enterpr	ise.com	Su	bmit	

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	Draviour Scone (D) Croste Report (D) Optioner	i Help Login
Start Scan Wizard Select Scan Targets           +         +         Active Directory           Scan computers         Selected from Active           Directory         Directory	Network Addresses Scan computers with specified IP addresses or endpoint names	Eustorn Scan
Workgroup Scan computers selected from Workgroups	This Computer Scan This Computer	
Consolo Unknown Silo Hunter is not of the Course in 20	Cancel	en hele antest vers an in-

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'

Start Scan Wizar	d		×
	Network Addresses		
		5	Add
	10.108.51.121/255.255.255.0		Remove
			Remove All
Back		- I	Next



- 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.

9% Scan In Progress Files: 4699   Computers: 2 of 166)	🕤 Previous Scans 🍈 Create Report 🌘	Options (i) Help Guest >
(0.04%) <b>4816</b> (99.94%) Clean Files <b>2</b> (0.04%) Malicious Files	1 (0.02%) In Analysis	Stop Scan
Q Search by Computers		Group by
Name	2	Size Verdict
CIS-PC (10.8.64.144) 360 files scan	ned (20.36%). Unknown: 0. Malicious: 0.	in Prógress
DC (10.8.64.156) Login problem: in	valid username or bad password.	Failed
DC01 (10.8.64.120) Enumerating at Enumerating at the second se	utoruns: 840	In Progress
DEMO1-WIN7-64 (10.8.64.35) Log	Failed	
DESKTOP-29HNT6A (10.8.65.5) Lo	gin problem: invalid username or bad password.	Failed
P DESKTOP-2AP7L3E (10.8.64.157)	ogin problem: the trust relationship between this workstati	Failed
DESKTOP-3AHSBGJ (10.8.64.155)	Login problem: invalid username or bad password.	Failed
Diase enter your email to rece	aive a detailed scan results report:	Submit

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

COMODO Creating Trust Online Unknown File Hunter		_ 🗆 ×
Start Scan Wizard	×	(j) Help Login
Select Scan Targets + + + + + + + + + + + + + + + + + + +	Network Addresses Scan computers with specified IP addresses or endpoint names	E Scan Now Custom Scan
+	This Computer         Scan This Computer	
Comodo Unknown File Hunter is part of the Comodo ONE po	rtfolio of security solutions. Visit one.comodo.com to learn how Comoc	do can help protect your environment.

• Choose the type of scan you want to run:

Start Scan Wizard		×
Select Scan Type		DESKTOP-HI950BN
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:

COMODO

Start Scan Wizard	×
Select Directories	
<ul> <li>C:\</li> <li>\$Recycle.Bin</li> <li>\$WINDOWS.~BT</li> <li>Documents and Settings</li> <li>inetpub</li> <li>OpenSSL-Win32</li> <li>PerfLogs</li> <li>Program Files</li> <li>Program Files (x86)</li> <li>ProgramData</li> <li>Recovery</li> </ul>	
Back 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.

COMODO

ating Trust Online	er		
0% Scan In Progress iles: 120   Computers: 0 of 1)	🕤 Previous Scans 🐽 Create Report 🍥 Options 🧃	i) Help	
(5%) Clean Files (5%) Clean Files		Stop Scan	
Q Search by Computers		Group by	
News		Mandat	
Name	d (40%), Unknown: 0, Malicious: 6.	In Progress	
Iocalhost (127.0.0.1) 120 files scanned	Size	In Progress	
Name Iocalhost (127.0.0.1) 120 files scanned When all the files are analyz	d (40%). Unknown: 0. Malicious: 6. ed, you will receive a detailed report at <b>domersa@yopmail.com</b>	Uerdict In Progress Edit E	imail

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					_ □
Scan Completed (Files: 34795   Computers: 1 of 1)	Previous Scans	🐽 Create Report	Options	(i) Help	Login
34781 (99.96%)         8 (0.02%)           Clean Files         Malicious Files	(0.02%) 6 (0.02%) Unknown Files			Image: New Cl       Image: New Cl	ustom Scan d Scan Results iscovery
Q Search by Computers					/ 🖳 🕼
Name			Size	Verdict	47
Completed: local nost (127.00.1) Completed: local files	scanned: 34/96. Unknown:	6. Malicious: 8.		Completed	
C:\ProgramData\SpeedBit\DAP\Plugins'	189AE673-13C1-4133-A470	-8C4DDD1AC88C\1.0.1	12 KB	Clean	
C:\Program Files\WindowsApps\Shared	LimitedTime\InfusedApps\P	ackages\Microsoft.Win	269 KB	Clean	
C:\Windows\InfusedApps\Packages\mic	crosoft.windowscommunicat	ionsapps_17.8241.4127	44 KB	Clean	
C\Windows\InfusedApps\Packages\Mic	rosoft.XboxSpeechToTextOv	verlay_1.17.29001.0_x64	550 KB	Clean	
C:\Windows\InfusedApps\Packages\Mic	crosoft.BingNews_4.3.193.0_3	x868wekyb3d8bbwe\	8 MB	Clean	
C:\Windows\InfusedApps\Packages\Mic	xosoft.WindowsCamera_201	17.727.20.0_x648weky	105 KB	Clean	
C:\Program Files\WindowsApps\Shared	LimitedTime\microsoft.wind	owscommunicationsap	10 KB	Clean	
When all the files are analyzed, ye	ou will receive a detailed rep	ort at <b>domersa@yopmai</b> l	.com	Ed	it Email

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:

1)	Previous Scans	s 🐽 Create Report	Options	(i) Help	Login
(0.02%) licious Files	6 (0.02%) Unknown Files			L Start I	Custom Scan ed Scan Result Discovery
				Group	y 💶 🛛
			Size	Verdict	
ompleted: Total fi	iles scanned: 34796. Unknown	: 6. Malicious: 8.		Completed	
/eedBit\DAP\Plugi	ins\189AE673-13C1-4133-A47	70-8C4DDD1AC88C\1.0.1	12 KB	Clean	
lindowsApps\Shar	redLimitedTime\InfusedApps\	Packages\Microsoft.Win	269 KB	Clean	
dApps\//ackages\/	Microsoft.Windowscommunica	https://www.action.com/action/	44 KB	Clean	
dApps(Packages)	Microsoft RingNews 4 3 193.0	venay_1.17.29001.0_x04	S MR	Clean	
dApos\Packages\	Microsoft WindowsCamera 20	17.727.20.0 x64 Bweky	105 KB	Clean	
and that a ground safe			100.00		
	y (0.02%) icious Files ompleted: Total fi teedBit\DAP\Plugi indowsApps\Shar dApps\Packages\ dApps\Packages\ dApps\Packages\	eedBit\DAP\Plugins\189AE673-13C1-4133-A47 indowsApps\SharedLimitedTime\InfusedApps\ dApps\Packages\Microsoft.windowscommunica dApps\Packages\Microsoft.bingNews_4.3.193.0	Image: State of the second state of	Image: Size         Size         Completed: Total files scanned: 34796. Unknown: 6. Malicious: 8.         reedBit\DAP\Plugins\189AE673-13C1-4133-A470-8C4DDD1AC88C\1.0.1       12 KB         tindowsApps\SharedLimitedTime\InfusedApps\Packages\Microsoft.Win       269 KB         dApps\Packages\Microsoft.Windowscommunicationsapps_17.8241.4127       44 KB         dApps\Packages\Microsoft.XboxSpeechToTextOverlay_1.17.29001.0_x64       550 KB         dApps\Packages\Microsoft.BingNews_4.3.193.0_x868wekyb3d8bbwe\       8 MB	Image: Start I         Image

- 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:
	<ul> <li>Completed – Unknown file which has been successfully uploaded to Valkyrie for analysis.</li> </ul>
	<ul> <li>In Analysis – Unknown file which is currently being tested by Valkyrie</li> </ul>
	Clean – Files found to be safe after Valkyrie analysis
	<ul> <li>Malicious – Files found to be unsafe after FLS and Valkyrie analysis</li> </ul>
	<ul> <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:

COMODO

COMODO Creating Trust Online Unknown Fi	ile Hunter				_ 🗆 ×
Previous Scans	Current	t Scan 🐽 Create Rep	ort 🎯 Options	(i) Help	chtwvalkyrie 💙
Q Search					Q
Scan Summary		Scan Date	Scan Target	Scan Type	
😔 Computers scanned: 1. Total f	files scanned: 1222. Unknown: 0	6/25/2018 3:34:46 PM	Auto Discovery	Quick Scan	Detailed Results
실 Computers scanned: 1. Total f	files scanned: 2. Unknown: 0. Ma	6/25/2018 4:52:11 PM	Local Computer	Custom Scan	Detailed Results
Computers scanned: 1. Total f	iles scanned: 1231. Unknown: 0	6/25/2018 5:04:39 PM	Auto Discovery	Quick Scan	Detailed Results
🚐 Computers scanned: 1. Total f	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 f	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 f	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	

	Previous Scan Results Interface - Table of Column Descriptions
Column Header	Description
Scan Summary	<ul> <li>Indicates the status of scans.</li> <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	<ul> <li>Indicates the type of scan:</li> <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 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

COMODO Unknown File Hunter					_ C	
Scan Completed (Files: 34796   Computers: 1 of 1)	Current Scan	illi Create Report	Options	(i) Help	chtwvalkyri	ie 🗸
Image: Weight of the second system         Image: Weight of the second system	(0.02%) 0 (0.02%) Unknown Files			🕻 Back tr	o Previous Sca ed Scan Resul	ans ts
Q Search by Computers				Group	by 📮	
Name			Size	Verdict		
modo Unknown File Hunter is part of the Comodo ON	E portfylio of security solutio	ons. Visit <u>one.comodo.con</u>	n to learn how Com	nodo can help prote	ect your envir	ronme
modo Unknown File Hunter is part of the Comodo ON	E portfolio of security solutio	ons. Visit <u>one.comodo.con</u> tails	n to learn how Com	nodo can help prote Full Scan	ect your envir Oktailed Auso	ronm

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.

### COMODO

# Comodo Unknown File Hunter - Admin Guide

### 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:

	÷.	ALKYRIE						IGN IN 🔶		
U	nknown File Hunte	r Scan Results								
	UNKNOWN FILE HUNTER	R SCAN SESSION DETA	illS				Se	arch:		
	File Name 👻	Path 6	SHA1 0	Last Activity 🔅	Final Verdict 6	Human Expert Verdict	Human Expert Analysis Status	Request Type 9	÷	
	setup.exe	EASuspicious files/All_t	2ec4e0011001a27882	2018-07-02 13:31:56	PUA			Queried	8	
	pcflank.exe	E:Suspicious files/All_t	3437369e6b75021157d	2018-07-02 13:31:55	PUA			Queried	8	
	illvid-download-manager.exe	CNUsers/RathDownloa	88e20914dcae99feaad	2018-07-02 13:31:22	PÜÄ	PUA	Completed	Queried	8	
	CPLSubs.exe			2014-07-02 13:31:55	6174				211	

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

- VALKYRIE									Download Unknow	m File Hunter		SIGN IN
Premium Users												
Malware	5	Avg. Time	Clean	8	Avg. Tane.	hknown	- N - A	wg. fime	Total	5	Avg. Tim	•
Automated Analysis	11.9%	11237	Automated Analysis		00608				Automated Analysis	1,9%	0.06:18	1
Human Expert Analysis		3:29:14	Human Expert Analysis		41336				Human Expert Analysis			
LATEST FILE	E UPLO	ADS	SEARCH									
SHA1			FILE NAME	SOURCE	SUBMIT DATE	FINAL VERDICT	HUMAN E	EXPERT VERDIC	T HUMAN EXPERT	ANALYSIS S	TATUS	
dia5388442d72b8b31b9	53a87a4012b	c5d781ddac	f.exe	Upload	2018-07-02 11:05:27	Malware.	Malware		Completed			
14a7009c20d70f052308	0ae8773fac5f	y6809013d	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

COMODO

	Α ΚΥ ΚΙΕ <u> <u> </u> <u> </u> <i> </i></u>
$\mathcal{A}$	Email or Login *
	Password *
	Remember Me Forgot password ?
	SIGN IN CREATE AN ACCOUNT

- 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 an Valkyrie account, enter the credentials and click the 'Sign In' button.

The 'Dashboard' page will be displayed by default.

VALKYRIE =	Valigate > Deshiosed		Q, Analyze New File *
88 DASHDOARD *	Last 30 days Last 7 days Last 24 hours Today 0 Total files uploaded	gueried Bits being processed	III 82 O St Files processing completed
<ul> <li>STATISTICS</li> <li>SETTINGS</li> </ul>	Malware or PUA File Detected Devices	Mahware or PUA File Detected Devices (Global) 3.4% O Sexicas with threat or PUA 24% O Sexicas with threat or PUA 25%	Latest Malware Submissions STATUS FILE NAME

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.

COMODO

	VALKYR	LIE 000				a a a a a a a a a a a a a a a a a a a	Ree User] (Enterprise	
Unknown F	ile Hunter Scan R	esults						
UNKNOWN	FILE HUNTER SCAN SES	SION DETAILS						
Show 25	<ul> <li>entries</li> </ul>						Search:	
Show 25	v entries Path ₫	SHA1 0	Last Activity 💡	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Search: Request Type 0	
Show 25 File Name 0	Path 0 ErSuspicious files VAI_te	SHA1 0 3437369e6b75021f57d	Last Activity ¥ 2018-07-03 14:28:16	Final Verdict +	Human Expert Verdict 💧	Human Expert Analysis Status	Search: Request Type 1 Queried	000
Show 25 · File Name 0 poffank.exe cpiLexe	entries     Path     EnSuspicious filesWil_te EnSuspicious filesWil_te	SHA1 0 3437369e6675021f57d 795fe85537ec514f3667	Last Activity 2018-07-03 14:28:16 2018-07-03 14:28:15	Final Verdict + PUA PUA	Human Expert Verdict	Human Expert Analysis Status	Search: Request Type ( Queried	<b>800</b> <b>800</b>
Show 25 Show 2	Path     Path     Path     C     EnSuspicious files/All_te EnSuspicious files/All_te EnSuspicious files/All_te	SHA1         0           3487369e6b750211576         795fe85537ec514f3667           d3be9ebc642f164efb03         64efb03	Lest Activity 2018-07-03 14:28:16 2018-07-03 14:28:15 2018-07-03 14:28:14	Final Verdict 0 PUA PUA PUA	Human Expert Verdict	Human Expert Analysis Status	Search: Request Type 1 Queried Queried Queried	
Show 25 x File Name 0 pottank.exe opil.exe opil.exe CPILSutte.exe	entries      Path          Path	SHA1         0           3437369e6b75021f57d         7           795fe85537ec514f3667         d3be9ebc642f164efb01           d3be9ebc642f164efb01         dcf2dftcb39003683be2e	Last Activity 2018-07-03 14:28:16 2018-07-03 14:28:15 2018-07-03 14:28:14 2018-07-03 14:28:13	Final Verdict 0 PUA PUA PUA PUA	Human Expert Verdict	Human Expert Analysis Status	Search: Request Type ( Queried Queried Queried Queried	
Show 25 Show 2	entries     Path       Path           EnSuspicious files/Wijte     EnSuspicious files/Wijte     EnSuspicious files/Wijte     EnSuspicious files/Wijte     EnSuspicious files/Wijte	SHA1         0           348756966b75021f57d         795fe85537ec514f3667           d3be9ebc642f164efb08         dcf2dfcb39003683be2e           57b72ae6c605290c60f8         57b72ae6c605290c60f8	Last Activity 2018-07-03 14:28:16 2018-07-03 14:28:15 2018-07-03 14:28:14 2018-07-03 14:28:13 2018-07-03 14:28:13	Final Verdict © PUA PUA PUA PUA PUA	Human Expert Verdict	Human Expert Analysis Status	Search: Request Type () Queried Queried Queried Queried 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:

COMODO



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

COMODO Creating Trust Online Unknown File Hunter					_ 🗆 ×
Scan Completed (Files: 150   Computers: 1 of 1)	Previous Scans	Create Report	Options	(i) Help cht	wvalkyrie 💙
143 (95.33%)         7 (4.67%)           Clean Files         Malicious Files		Executive Report Per-Device Report Per-Program Report		Lini New Cus Detailed : Ling Start Disc	tom Scan Scan Results covery
Q Search by Computers				Group by	
Name			Size	Verdict	Car .
E Generation (127.0.0.1) Completed: Total files	scanned: 150. Unknown: 0	). Malicious: 7.		Completed	
E:\Suspicious files\All_tests\AWFT\AWF	P\setup.exe		985 KB	Malware	
E\Suspicious files\All_tests\cpil_suite\C				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'

COMODO



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:

Per-Device Report			$\Box \times$
🖬 👼 🕆 🖡 1 /4		Search	1
сом	ספס	Unknown File Hunter	
Per-Devic	e Report	7/4/2018 12:06:04 PM	
Summary	Chart erable Devices		
100 10 10	T		
localhost			

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).

Per-Program Report		$\Box \times$
🖬 👼 🕆 🖡 1 /8	🔎 Search	
сомодо	Unknown File Hunter	
Per-Program Report	7/4/2018 12:39:58 PM	
Summary Chart		
Top 10 Unknown/Malicious Files		
CPIL3.dll -		
cpil.dll —		
cpil.exe -		
CPILSuite.exe		
ocflank.exe -		8.

COMODO

# Comodo Unknown File Hunter - Admin Guide

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.

- сомодо  $\Box \times$ **Unknown File Hunter** Scan Completed (iii) Create Report (i) Help Previous Scans Options chtwvalkyrie 🗸 (Files: 150 | Computers: 1 of 1) About Agent Requirements  $\mathbf{O}$ art Discover Q Search by Cor About × Name Verdict 🖃 🧶 localho сомодо 🐻 E\\S Creating Trust Online 🚡 EAS Product Name: Unknown File Hunter Product Version: 5.0.0.134 Close © 2018 Comodo Security Solutions, Inc. All Rights Reserved.
- 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:

COMODO Creating Trust Online	nown File Hunter	_ 🗆 ×
Scan Completed (Files: 150   Computers: 1	of 1) () Previous Scans (iii) Create Report (ii) Options (i) Hel	P chtwvalkyrie 🗸
<b>0</b> 143 (95.33%) Clean Files	About Agent Ro 7 (4.67%) Malicious Files	Detailed Scan Results
Q Search by Computers	Agent Requirements	Group by
🖃 🦵 localhost (127.)	Check whether a target computer is turned on and connected to the network.	d
🚡 E\Suspicio	Check whether firewall on a target computer is turned Off.	
🐻 E\Suspicio	Check whether IP address of a target computer is correct.	
🐞 Et/Suspicio	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.	
	Close	

# **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