COMODO
CYBERSECURITY

Comodo
Unknown File Hunter

Software Version 5.0

Quick Start Guide

Guide Version 5.0.071119

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

How to Use Comodo Unknown File Hunter (UFH)

Comodo UFH lets you scan your entire network to discover the trust levels of all files on your endpoints. The tool classifies files as 'safe' (whitelisted / no threat), 'malicious' (blacklisted / malware) or 'unknown' (neither blacklisted nor whitelisted). Unknown files are automatically submitted to Comodo Valkyrie for static and **dynamic analysis**. The results of the Valkyrie tests are reported back to UFH for your review.

This tutorial briefly explains how to set up and run a scan.

Step 1 - Download, install and run the tool

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:

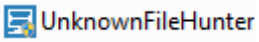
- Login to your Comodo Dragon / Comodo One account at **https://platform.comodo.com/app/login** / **https://one.comodo.com/app/login**
- Click 'Tools' > Click 'Download' in the Unknown File Hunter tile
  - You can sign up for a free Comodo Dragon / Comodo One account at **https://platform.comodo.com/signup** / **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

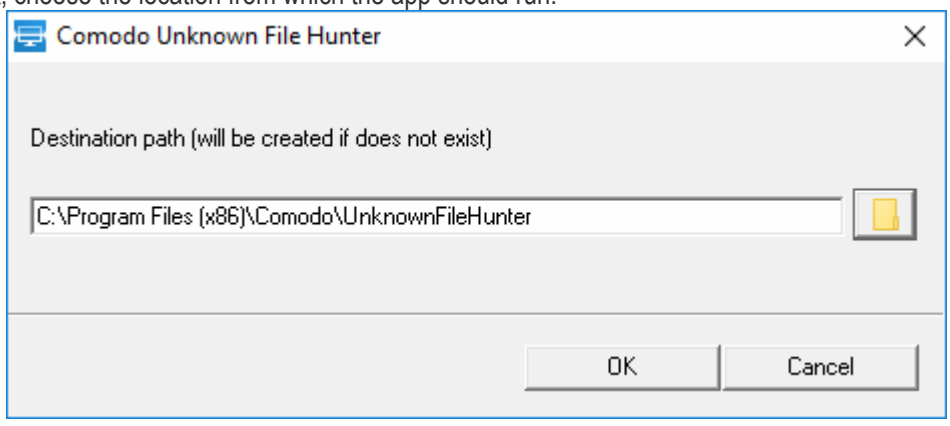
- Go to **https://valkyrie.comodo.com/**
- Click 'Download Unknown File Hunter'
  - You can create a Valkyrie account at **https://valkyrie.comodo.com**
- Please visit **https://valkyrie.comodo.com/apt_tool/download/UnknownFileHunter.exe**

Run Unknown File Hunter

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



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



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

different locations as you prefer.

- You will need to agree to the EULA when you first run UFH on a new computer.
- Click the 'License agreement' link, read the agreement and click 'I Accept'.

Step 2 – Specify targets and run a scan

The are four ways to scan endpoints:

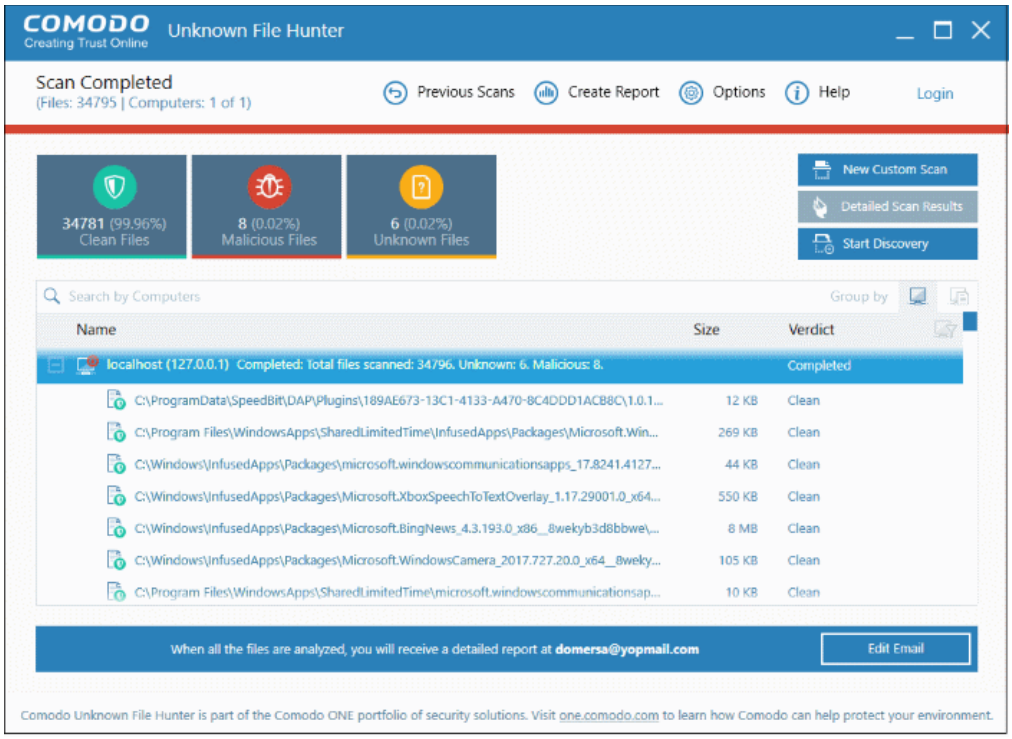
- **Active Directory** - Import computers from an active directory domain.
- **Workgroup** - Add computers that belong to a particular workgroup.
- **Network Address** - Specify individual host names, IP addresses or IP ranges.
- **This Computer** – Scan the local device.

If you need more help to specify targets, refer to our online guide at **https://help.comodo.com/topic-400-1-794-10428-Scanning-Computers.html**.

- Click 'Custom Scan' and select a method to begin a scan.

Step 3 – View results

Detailed results are shown at the end of every scan.

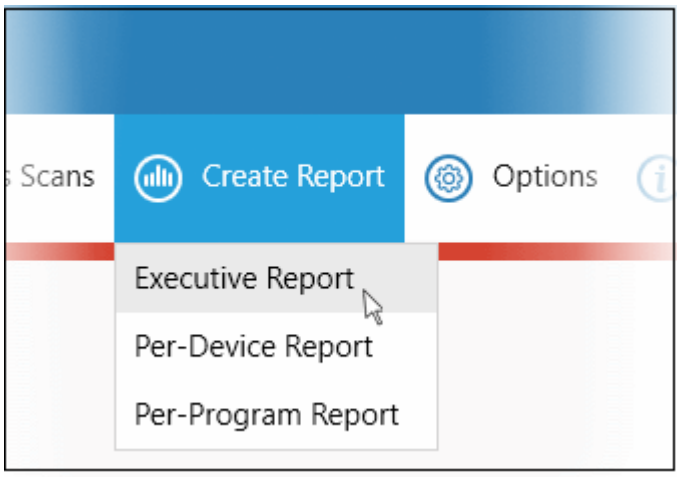


- Click '+' beside a hostname to view all files analyzed on the endpoint. Double-click any file to view scan details on the file.
- The tiles above the table show the total number of unknown, malicious and clean files on all endpoints covered by the scan.
  - 'Unknown' means no trust rating is available for the file.
  - Unknown files are uploaded to Valkyrie, Comodo's file analysis service, where they will be tested to find out whether or not they are malicious.
  - After analysis, they will be re-categorized as either 'Safe' or 'Malicious'.
- Click 'Detailed Scan Results' to login to Valkyrie and view a breakdown of the tests on your files.
  - Login at **https://valkyrie.comodo.com/** with your Comodo Dragon, Comodo One or Valkyrie

username and password.

See '**Scan Results**' if you need more help with this.

- You also can view detailed scan results in the 'Reports' section:



- Executive Report - Top level summary of scan results.
- Per Device Report – Results grouped by device.
- Per Program Report – Results grouped by filename.

For more details about reports, see **https://help.comodo.com/topic-400-1-794-10430-Reports.html**

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**