COMODO
Creating Trust Online®

Comodo Forensic Analysis

Software Version 4.0

Quick Start Guide

Guide Version 4.0.030119

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

How to Use Comodo Forensic Analysis

- Comodo Forensic Analysis (CFA) lets you scan domains, workgroups and IP ranges to discover the trust level of every file on a network.
- 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** tests. The results of the Valkyrie tests are reported back to the CFA software for administrator review.

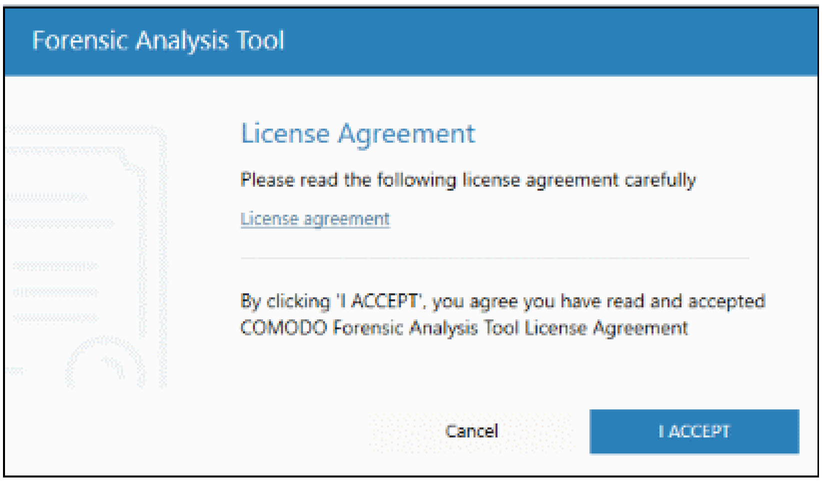
This tutorial briefly explains how to set up and run a scan:

- **Step 1 - Download, install and discover computers**
- **Step 2 – Specify targets and run a scan**
- **Step 3 – View scan results and reports**

Step 1 - Download, install and discover computers

- Please download the utility from: **https://enterprise.comodo.com/freeforensicanalysis/**

CFA does not require installation and can be started by simply opening 'ForensicAnalysisTool.exe'. You need to agree to the terms and conditions before using the application:



Forensic Analysis Tool

License Agreement

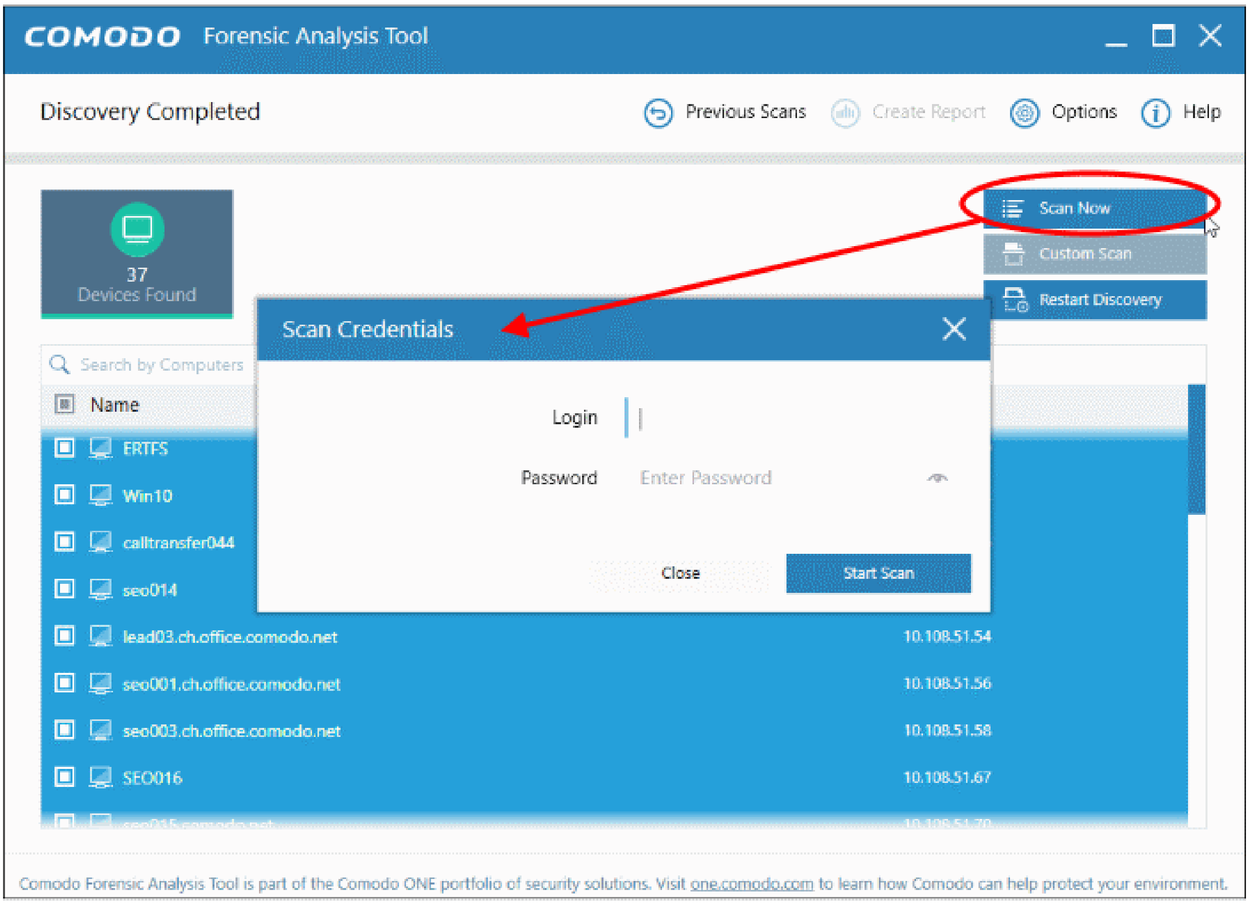
Please read the following license agreement carefully

License agreement

By clicking 'I ACCEPT', you agree you have read and accepted COMODO Forensic Analysis Tool License Agreement

Step 2 – Specify targets and run a scan

- On startup, Comodo Forensic Analysis runs a scan to discover all endpoints on the local network.
- Local discovery is designed for users who want to scan their immediate environment. At the end of discovery, you can select local endpoints then click 'Scan Now'.

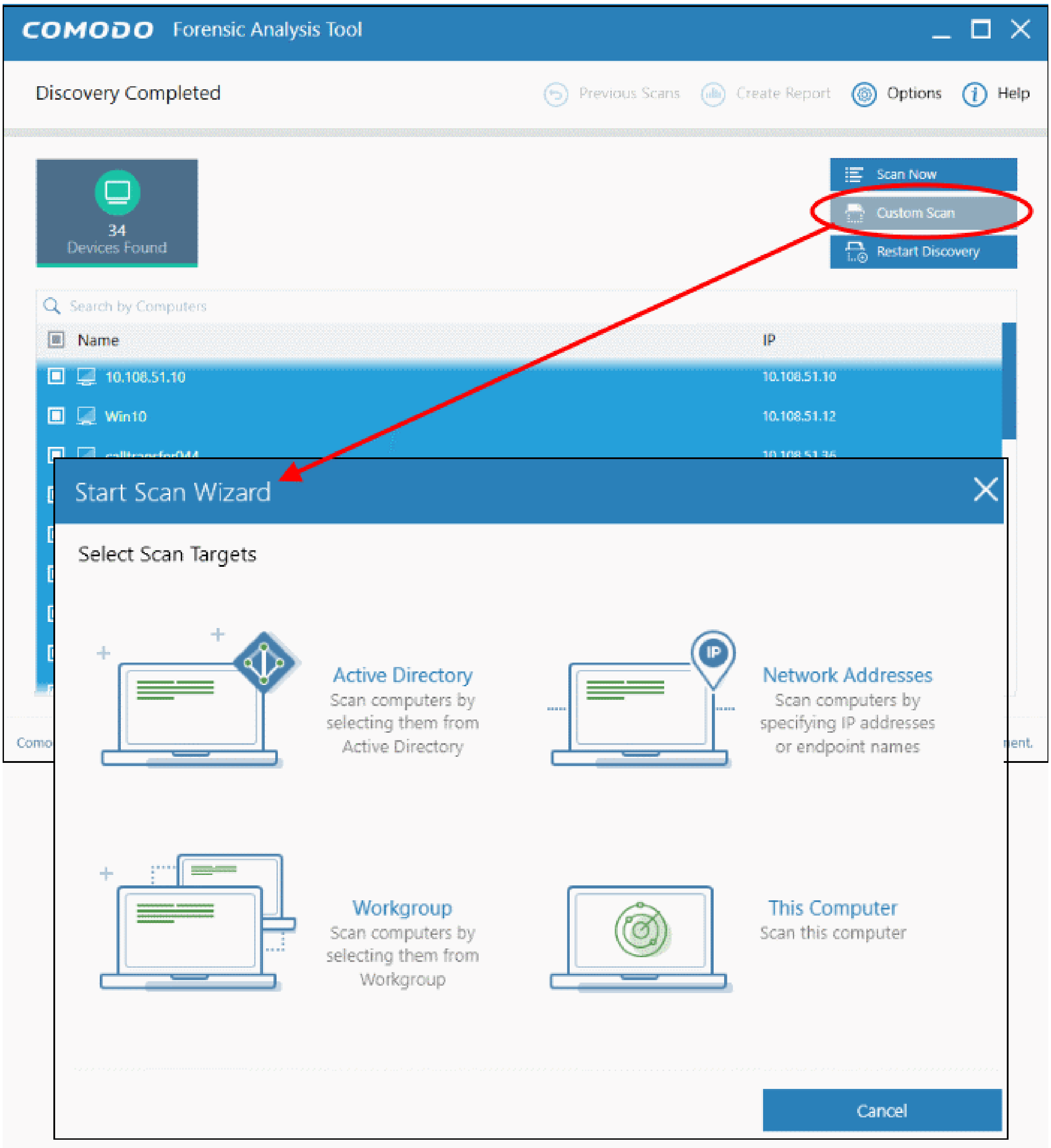


Name	
ERTFS	
Win10	
calltransfer044	
seo014	
lead03.ch.office.comodo.net	10.108.51.54
seo001.ch.office.comodo.net	10.108.51.56
seo003.ch.office.comodo.net	10.108.51.58
SEO016	10.108.51.67

Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

- Enter an admin username and password for the endpoints you wish to scan
- Choose a scan type:
  - **Quick Scan**: Scans critical and commonly infected areas of target endpoints
  - **Full Scan**: Scans all files and folders on target endpoints.

Custom scan: Scan specific Active Directory domains, Workgroups or IP ranges. You can also scan your local machine:



Name	IP
10.108.51.10	10.108.51.10
Win10	10.108.51.12

Start Scan Wizard
Select Scan Targets
Active Directory
Scan computers by selecting them from Active Directory
Network Addresses
Scan computers by specifying IP addresses or endpoint names
IP
Workgroup
Scan computers by selecting them from Workgroup
This Computer
Scan this computer
Cancel

You can use any of the following methods to add endpoints to a custom scan:

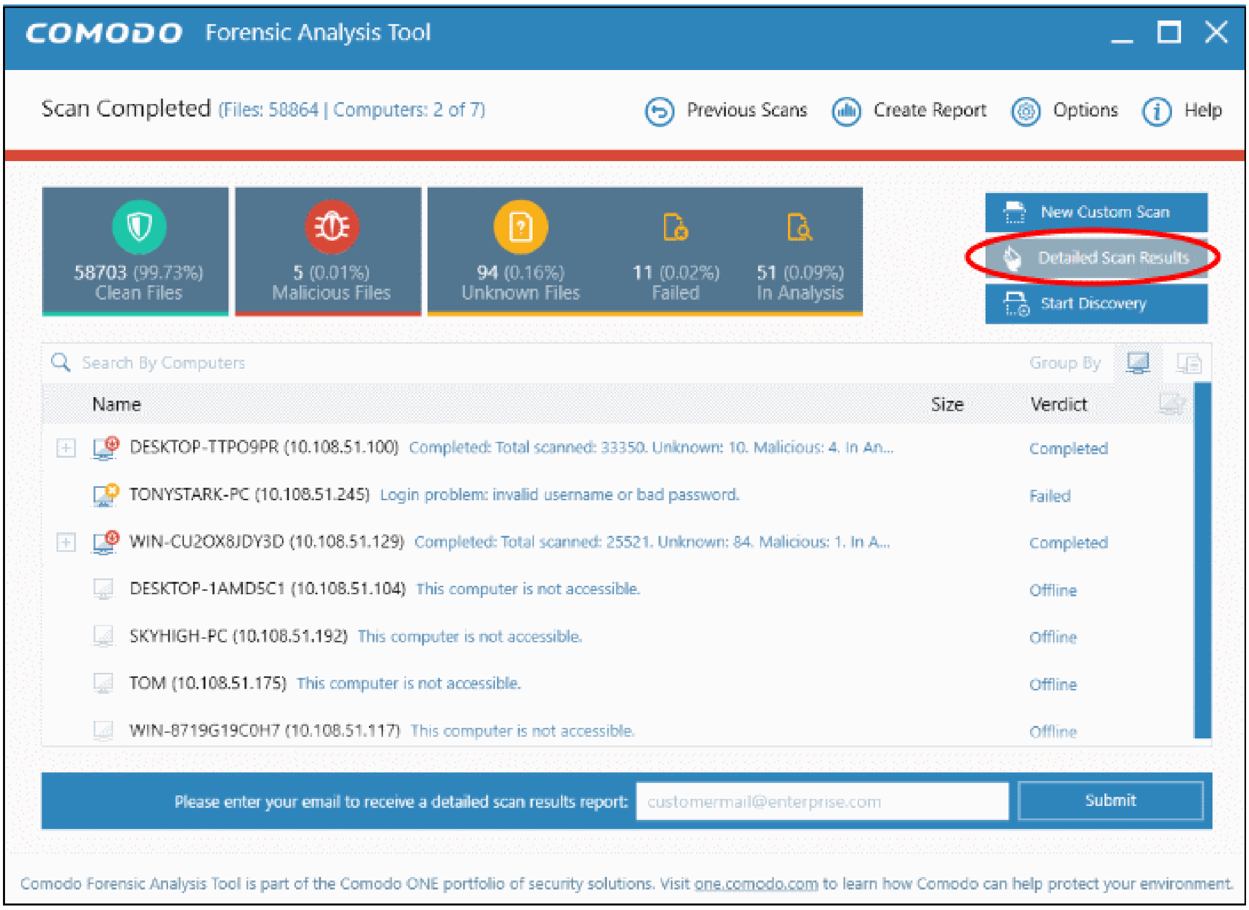
- **Active Directory** - Scan computers which belong to an Active Directory domain.
- **Workgroup** - Scan computers that belong to a local work group
- **Network Address** - Specify target endpoints by host name, IP address, or IP range
- **This Computer** - Run a scan on your local device.

If you need help to specify additional targets using the methods above, please refer to our online guide at https://help.comodo.com/topic-400-1-794-10428-Scanning-Computers.html.

- Click 'Scan Now' to begin your scan.

Step 3 – View scan results and reports

Unknown files are automatically submitted to Valkyrie for analysis after the scan finishes. Click 'Detailed Scan Results' to view the results of the analysis:



Scan Completed (Files: 58864 | Computers: 2 of 7)

58703 (99.73%) Clean Files	5 (0.01%) Malicious Files	94 (0.16%) Unknown Files	11 (0.02%) Failed	51 (0.09%) In Analysis

Name	Size	Verdict
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total scanned: 33350. Unknown: 10. Malicious: 4. In An...		Completed
TONYSTARK-PC (10.108.51.245) Login problem: invalid username or bad password.		Failed
WIN-CU2OX8JDY3D (10.108.51.129) Completed: Total scanned: 25521. Unknown: 84. Malicious: 1. In A...		Completed
DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible.		Offline
SKYHIGH-PC (10.108.51.192) This computer is not accessible.		Offline
TOM (10.108.51.175) This computer is not accessible.		Offline
WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible.		Offline

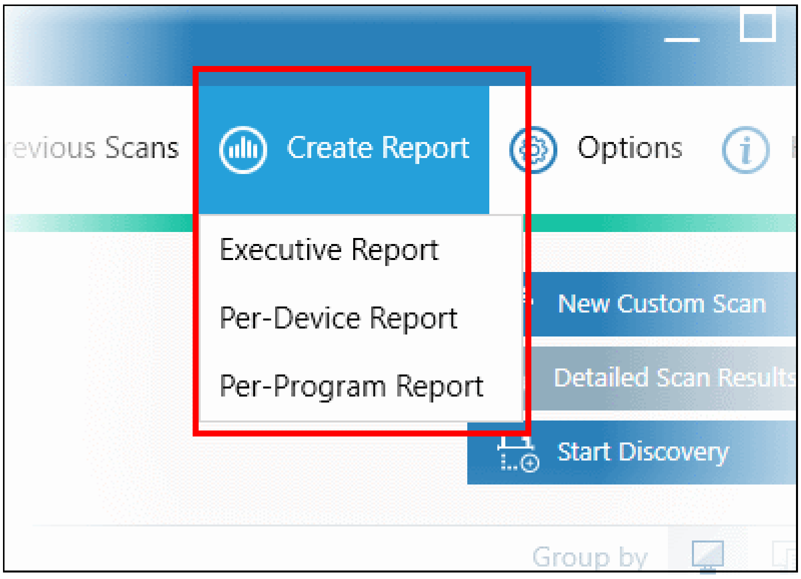
Please enter your email to receive a detailed scan results report: customermail@enterprise.com

Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

- Click 'Detailed Scan Results' to view all scan results analyzed by Valkyrie. Valkyrie is an automated, cloud-based behavior analysis system which subjects unknown files to a battery of static and dynamic tests to try and discover malicious or anomalous behavior.
- After the scan completes, you can enter your email id and click 'Submit' to get a detailed scan result report.
- You can view a more detailed version of these results by creating an account at the Valkyrie website. To do so, click 'Please click here to see the detailed results' and select 'Create an Account' at **https://valkyrie.comodo.com/login**

For more details on using Valkyrie, see **https://help.comodo.com/topic-400-1-794-10439-Valkyrie-Analysis-Results.html**

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



- **Executive report -** An overall report which shows the scope of the scan, the number of devices scanned, the number of unknown programs found and more.
- **Per device report -** Groups results by computer. Expand any row to see the unknown, safe and malicious files found on that specific machine.
- **Per program report -** Groups results by file to show the footprint of a specific file on your network. Expand any row to see the names and addresses of all devices on which the file was found.

For more details about reports, see **https://help.comodo.com/topic-442-1-890-11317-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**