MEFF
M3 PRO

Complete User Manual

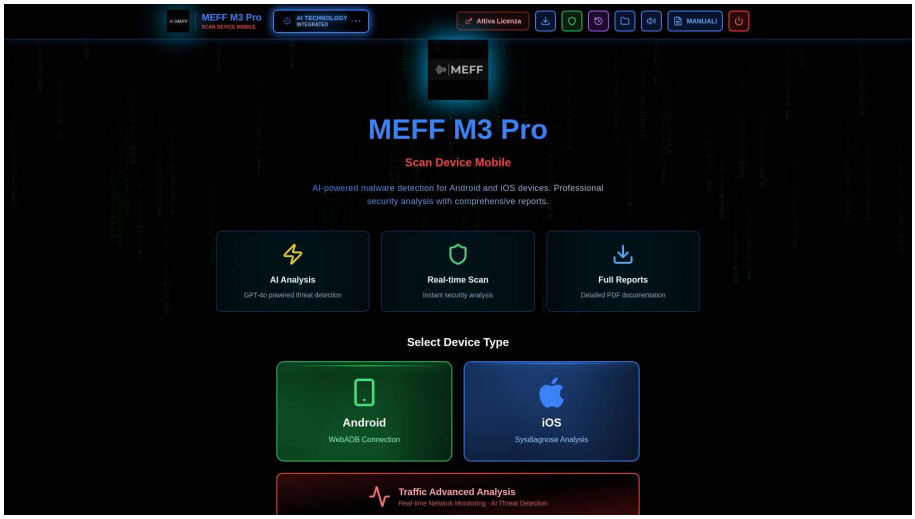
Version 2.0.0 - Professional Mobile Malware Scanner

November 2025

Securcomitaly

TABLE OF CONTENTS

1. INTRODUCTION



What is MEFF M3 PRO

MEFF M3 PRO is a professional solution for security analysis of Android and iOS mobile devices, with advanced network traffic analysis capabilities. It uses AI technologies to detect malware, government spyware and suspicious behaviors.

Main Features

■ Android Scanner with WebUSB

■ iOS Scanner with Sysdiagnose

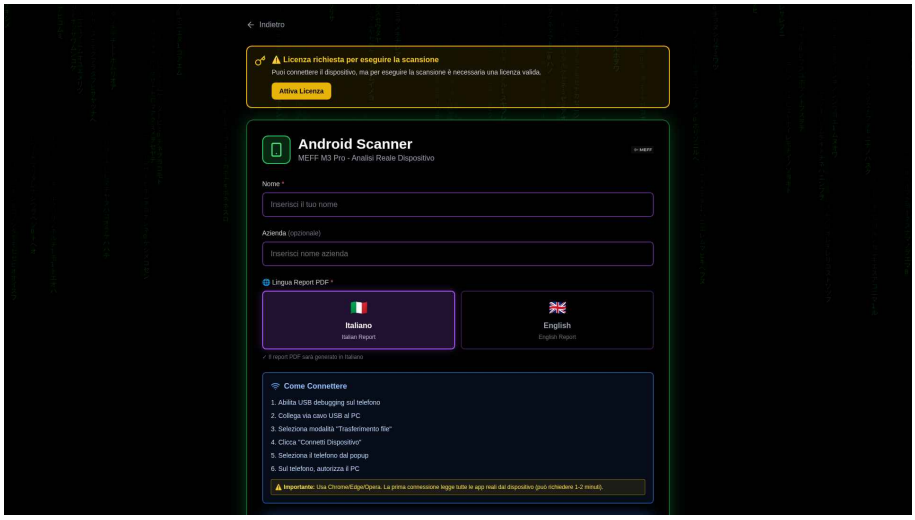
■ Traffic Analyzer with Hotspot

■ AI Analysis with OpenAI GPT-4o

■ Professional PDF Reports

■ Multilingual (IT/EN/FR)

2. ANDROID SCANNER



The Android Scanner module allows real-time analysis of Android devices through direct USB connection using WebUSB technology.

Android Device Preparation

Before connecting the Android device, you need to enable USB Debugging in the phone's Developer Options.

Steps to Enable USB Debugging:

1. Go to Settings > About phone
2. Tap "Build number" 7 times
3. Go back and open "Developer options"
4. Enable "USB debugging"
5. Connect phone to PC with USB cable
6. Authorize PC when prompted on phone

Device Connection

Once USB Debugging is enabled, click the "Connect Android Device" button and select the device from the browser popup.

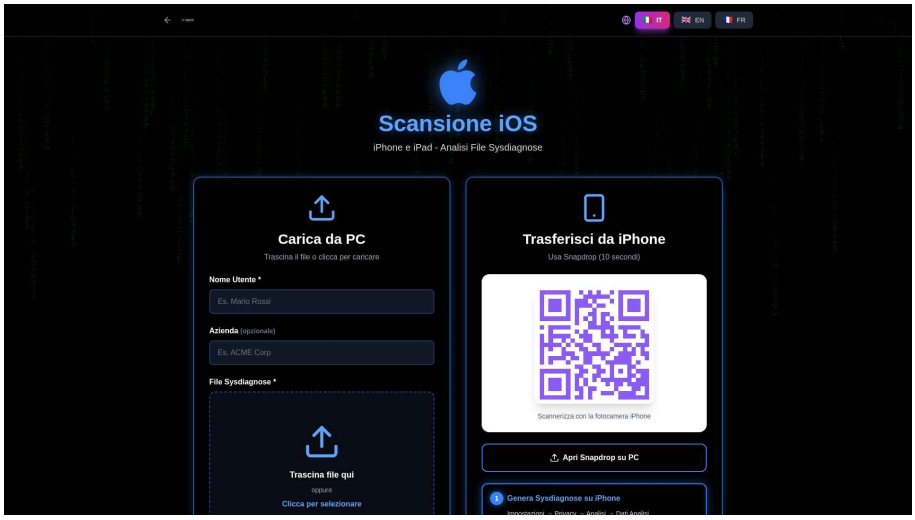
Starting Scan

After connection, enter Name and Company (optional), select report language and click "Start AI Analysis". The system will read all installed apps and permissions, then use AI to analyze risks.

Viewing Results

At the end of the scan, results will be shown with risk assessment, high-risk apps, critical permissions and recommendations. You can download the complete PDF report.

3. iOS SCANNER



The iOS Scanner module analyzes sysdiagnose files generated from iPhone and iPad devices to detect malware and suspicious behaviors.

Generating Sysdiagnose File

The sysdiagnose file contains detailed system logs. To generate it on iPhone:

1. Press simultaneously: Volume Up + Volume Down + Side Button
2. Hold for 1-2 seconds until haptic feedback
3. Wait 10 minutes (background generation)
4. Go to Settings > Privacy > Analytics & Improvements > Analytics Data
5. Find the most recent "sysdiagnose_YYYYMMDD..." file
6. Tap file > Share > Save to Files

Upload Methods

Two methods are available to upload the sysdiagnose file:

Method 1 - From PC: Transfer the file from iPhone to PC (email, AirDrop, cable) and upload via drag & drop

Method 2 - From iPhone: Scan the QR code with iPhone to open Snapdrop and transfer the file directly via local WiFi

File Scanning

After uploading the file, enter Name and Company, then click "START SCAN". Analysis takes 2-3 minutes.

iOS Analysis Results

The report shows installed apps, suspicious network connections, AI analysis and complete checklist of iOS government trojans.

4. TRAFFIC ANALYZER

The Traffic Analyzer captures and analyzes network traffic from devices connected to a Windows WiFi hotspot.

Hotspot Configuration

The hotspot is always active and automatically configured with the following credentials:

SSID: M3SCAN

Password: Meff2025!Secure

Gateway: 192.168.137.1

Device Connection

From the device to be analyzed (smartphone, tablet), connect to the M3SCAN WiFi network using the provided password. The device will automatically receive an IP in the 192.168.137.0/24 subnet.

Traffic Capture

Click "START TRAFFIC CAPTURE" to start network traffic capture. Use the device normally for 2-5 minutes browsing web, apps, social media. The system will capture all HTTP, HTTPS and DNS connections.

Traffic AI Analysis

After clicking "STOP CAPTURE", fill the form with Name and Device Type, then click "AI SCAN TECHNOLOGY". The AI will analyze traffic patterns, visited domains and detect suspicious connections.

Report Generation

Click "Generate PDF Report" to create the complete report. A progress bar with generation phases will be shown. At the end, download the PDF report with all statistics and detailed analysis.

5. SAVED REPORTS

All generated reports are saved and accessible from the Saved Reports section.

You can view, download or delete previous reports. Reports are organized by date and type (Android, iOS, Traffic).

6. TROUBLESHOOTING

Issue: Android device won't connect

Solution: Verify USB Debugging is enabled, use Chrome/Edge, authorize PC on phone.

Issue: Sysdiagnose file not accepted

Solution: Verify it's a valid .tar.gz file, size >10MB, recently generated.

Issue: No traffic captured

Solution: Verify M3SCAN WiFi connection, wait a few minutes, use apps on device.

7. APPENDIX

Ports Used:

- Backend API: 8001
- Frontend Web: 3000

Useful Commands:

- netsh wlan show hostednetwork (check hotspot)
- ipconfig /all (check network)