Blue Trace User & Policy Guide

Version 2.0.0.0

© 2024 White Hat Wes Cybersecurity

Table of Contents

About Blue Trace

Blue Trace is an advanced, modular forensic and system health analysis tool designed for Windows environments.
Developed by cybersecurity professionals, Blue Trace provides analysts, IT staff, and incident responders with the capability to collect, analyze, and report on a wide spectrum of system, network, security, and user artifacts—all in a single, streamlined workflow.

Primary Purposes

- **Digital Forensics:** Collect and review Windows system artifacts for evidence, threat hunting, or post-incident analysis.
- **Incident Response:** Gather live system data to assist in rapid triage and root cause analysis.
- **System Health Monitoring:** Assess the state and performance of endpoints for IT operations and troubleshooting.
- **Compliance Reporting:** Map current device configurations and activities to recognized frameworks (CMMC, SOC 2, ISO 27001) for audit support or internal review.

What Makes Blue Trace Different?

- Analyst-driven workflows: You choose what to collect, and how deep to go.
- All-in-one output: Easy exports (JSON, Excel, PDF, etc.)—no parsing, no scripting required.
- Visual insights: Dashboard, scan history, and report tools present results clearly, so you can take action fast.
- Privacy-first: All operations are local; your evidence never leaves your control.
- No vendor lock-in or hidden “cloud” processing—what you scan is what you keep.

Key Features

- **End-to-End Artifact Collection:** Gathers user, system, network, security, and forensic artifacts in a single automated pass.
- **Custom & Preconfigured Scans:** Choose from incident response, networking, system health, compliance, or design your own scan sets.
- **Dashboard & Scan History:** Visualize device health, review past scans, and track system changes.
- **Multiple Export Formats:** Export scan results as **JSON**, **XLSX**, **TXT**, or **CSV**. JSON scans can be converted to full PDF reports.
- **Privacy Focused:** All operations and data are local-only by default; nothing is sent to any third party.

System Requirements

- **Operating System:** Windows 10 version 1809 (build 17763) or later (64-bit/x64)
- **.NET Runtime:** .NET 8.0 Desktop Runtime (included in MSIX package)
- **Privileges:** Local Administrator rights required for most scan modules
- **Disk Space:** At least 250 MB free for installation and scan output

Installation Guide

Download Blue Trace

- Obtain the latest MSIX/installer bundle from your trusted source or official release page: BlueTrace_2.0.0.0_x64.msixbundle

Install the Application

1. Double-click the .msixbundle file to start installation with Windows App Installer.
2. Follow the prompts:
    - Click **"Install"** or **"Reinstall"** if upgrading.
    - Accept security dialogs (the publisher should be **White Hat Wes Cybersecurity**).

Note:
If blocked, right-click the installer, select **Properties**, and check **"Unblock"** if available.

Launch Blue Trace

- After installation, click **"Launch"** or open "Blue Trace" from your Start Menu.

Quick Start

1. Open Blue Trace from your Start Menu.
2. Select a scan profile (Incident Response, Networking, System Health, Compliance) or create a custom scan.
3. Click **"Start Scan"** and follow the progress bar.
4. View scan results on the dashboard, export as needed or generate a PDF report.
5. Review past scans in the Scan History tab.

Output Formats

- **JSON:** Structured data for reporting and archival
- **XLSX:** For Excel/LibreOffice analysis
- **TXT:** Plain text review
- **CSV:** Spreadsheet/database import
- **PDF:** Generated from JSON for full reports

Custom Scans & Profiles

- **Run any module individually**
- **Create custom scan profiles** with modules you choose
- **Predefined profiles:**
    - Incident Response
    - Networking
    - System Health
    - Compliance

Frequently Asked Questions

Q: What permissions does Blue Trace require?
A: Local administrator rights for complete artifact access.

Q: Are results private?
A: All scan data is stored and exported locally only unless you choose to share.

Q: Can Blue Trace be used offline?
A: Yes. All functions work without an internet connection.

Q: Does Blue Trace run in the background or at startup?
A: No. Blue Trace runs only when launched by the user.

Dashboard & History

The Dashboard

The Blue Trace dashboard serves as your control center and executive summary. It provides an at-a-glance view of:

- **Current System Information:**
  - Device name, hostname, user name, operating system, hardware specs
- **Security Posture:**
  - UAC status, BitLocker status, AV/EDR state, Windows Update, firewall configuration, encryption status
- **System Health:**
  - Disk usage, RAM utilization, CPU load, last boot time, system events
- **Live Scan Progress:**
  - Real-time scan activity, status indicators (including visual progress and failure states), and module-by-module results as they are collected

Scan History

- **Automatic Logging:**
  Every scan (preconfigured or custom) is automatically logged and accessible in the Scan History view.
- **Comprehensive Metadata:**
  Track scan type, timestamp, operator, scan outcome, and export history for each run.
- **One-Click Access:**
  Instantly open previous scan results, re-export in your preferred format, or generate new reports from past JSON data.
- **Audit Support:**
  The Scan History provides a reliable audit trail for compliance and internal investigations.

Custom Scans & Profiles

- **Run any module individually**
- **Create custom scan profiles** with modules you choose
- **Predefined profiles:**
    - Incident Response
    - Networking
    - System Health
    - Compliance

Report Generation

Requirements

- **Reports can only be generated from scan results saved in JSON format.**
- JSON files **must be located in a folder named BlueTraceReports**.

Preconfigured Scans

- The BlueTraceReports folder is **created automatically**.
- All scan results are saved in the correct location for report generation.

User-Created (Custom) Scans

- **You must manually create a folder named BlueTraceReports** in your output location.
- Save your custom scan JSON files in this folder.
- Only these JSON files will be available for PDF report generation.

Generating a Report

1. Save your scan as JSON.
2. Ensure the file is in the BlueTraceReports folder.
3. Go to the Reports section in Blue Trace.
4. Select your scan and click **“Generate Report”**.

Only .json scan files in BlueTraceReports will appear in the report list.

Data Privacy Statement

Blue Trace was designed with privacy as a core requirement. Your data stays in your hands—always.

- **Local-Only Operation:**
  All scan operations, artifact collection, report generation, and data exports occur entirely on your local device. **Nothing is ever sent or uploaded to White Hat Wes Cybersecurity or any third party.**
- **No Telemetry:**
  Blue Trace does not phone home, collect analytics, or transmit telemetry of any kind.
- **User-Directed Data Management:**
  - Only you decide if, when, and how to export, share, or delete your scan data and reports.
  - All exported files remain on your device unless you manually send them elsewhere.
- **No Hidden Data Collection:**
  Blue Trace does not embed, encrypt, or otherwise hide any data transfer functions.
- **Data Security is Your Security:**
  Your trust is our reputation. We encourage you to review the output directory and application logs at any time to confirm these statements.
- **Enterprise Use:**
  Blue Trace can be deployed in sensitive or regulated environments (e.g., legal, healthcare, government) with confidence—your data never leaves your organization unless you choose to share it.

Security Policy

We take the security of Blue Trace and your environment seriously. If you believe you have found a security issue, please read and follow our disclosure process:

Reporting Security Issues or Vulnerabilities

- **Contact us directly and privately:**
  Email: Info@whitehatwes.com

Do not disclose security issues publicly or in GitHub issues. This is to protect all users.

What to Include in Your Report

- A description of the vulnerability or security concern
- Steps to reproduce the issue, including relevant system details
- Any logs, screenshots, or code snippets (plain text only)
- Your contact information for follow-up

For security reasons, do not send executable files (.exe, .dll, .bat, .ps1, etc.). Emails containing executables will not be reviewed or opened.

Responsible Disclosure Process

- **Private reporting:**
  Please report vulnerabilities to us privately, allowing time to investigate and address them.
- **Coordinated response:**
  We may coordinate with you for additional details, clarification, or confirmation.
- **Public disclosure:**
  We ask that you give us reasonable time to resolve the issue before any public announcement or disclosure.
- **Acknowledgment:**
  Valid reports will be acknowledged and tracked through resolution.

Follow-Up and Compensation

- We may reach out to you for further information or clarification regarding the reported issue.
- If you provide a solution or recommendation that helps resolve the issue, please note that **financial compensation is not required or guaranteed**.

License

Copyright (c) 2024 White Hat Wes Cybersecurity. All rights reserved.

This software and its associated files ("Blue Trace") are the exclusive property of White Hat Wes Cybersecurity.

Permission is granted to the original licensee for personal or internal business use only, subject to these restrictions:

1. **No Modification:**
   You may not modify, adapt, reverse engineer, decompile, or create derivative works.
2. **No Sale or Redistribution:**
   You may not sell, resell, lease, rent, sublicense, distribute, or otherwise transfer this software or any derivative works.
3. **No Commercial Use Beyond Original Licensee:**
   Use is restricted solely to the original licensee and may not be provided as a service or included in any commercial offering.
4. **Proprietary Notices:**
   Do not remove or obscure copyright, trademark, or other proprietary notices.
5. **No Warranty:**
   Provided "as is", without warranty of any kind. White Hat Wes Cybersecurity is not liable for any damages from use.

Contact & Support

For installation help, bug reports, security issues, or questions about your license, contact:
Email: Info@whitehatwes.com
Website: https://whitehatwes.com

Thank you for choosing Blue Trace. Your security, privacy, and operational clarity are our top priorities.

Full Name (Print): ____________________________ **Date: ________________________**

Signature: ____________________________________ **Date: ________________________**

Blue Trace Signature: __________________________ **Date: ________________________**