

User Guide

Forensics Analysis 7.4.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



November 18, 2025

Forensics Analysis 7.4.3 User Guide

04-743-1083817-20241118

TABLE OF CONTENTS

Introduction	4
License	5
Requesting forensic analysis on an endpoint	6
Change log	13

Introduction

You can request forensic analysis on a suspected device from EMS. The Fortinet forensics team investigates the logs and provides a detailed report with their verdict. You can download the report from EMS.

You can use this feature with on-premise EMS or FortiClient Cloud.

For on-premise EMS, you can only request forensic analysis for Windows or macOS endpoints. FortiClient (macOS) 7.4.1 and later versions support forensic analysis.

You need to apply the Forensics license to EMS to access this feature. The following assumes that you have acquired and applied the license as necessary.

License

The Forensics analysis feature requires the following licensing:

License name	Description
FortiGuard Endpoint Forensics Analysis	<p>The forensic service provides remote endpoint analysis to help endpoint customers respond to and recover from cyber incidents. For each engagement, forensic analysts from Fortinet's FortiGuard Labs remotely assist in the collection, examination, and presentation of digital evidence, including a final detailed report.</p> <p>This is an add-on license that you can apply to per-endpoint and per-user endpoint protection platform, zero trust network access, and FortiSASE licensing.</p> <p>On-premise EMS only supports this feature for Windows endpoints.</p>

For details on EMS licensing, see [Windows, macOS, and Linux licenses](#).

Requesting forensic analysis on an endpoint

You can request forensic analysis on a suspected device from EMS. The Fortinet forensics team investigates the logs and provides a detailed report with their verdict. You can download the report from EMS.

You can only request forensic analysis for Windows or macOS endpoints. FortiClient (macOS) 7.4.1 and later versions support forensic analysis.

You must apply the Forensics license to EMS to access this feature. The following assumes that you have acquired and applied the license as necessary.

To request forensic analysis for an endpoint:

1. Enable the forensic analysis feature:
 - a. In EMS, go to *System Settings > Feature Select*.
 - b. Enable *FortiGuard Forensics Analysis*.
 - c. Click *Save*.
2. Configure forensic analysis in a profile:
 - a. Go to *Endpoint Profiles > System Settings*.
 - b. Create a new profile or edit an existing one.
 - c. Under *Endpoint Control*, toggle *Enable Forensics Feature* on.
 - d. Click *Save*.
 - e. Include this profile in a policy, and apply the policy to the desired endpoint.
3. Request analysis:
 - a. Go to *Endpoints > All Endpoints*.
 - b. Select the desired endpoint.
 - c. Under *Forensics Analysis*, click *Request Analysis*.
4. Complete the questionnaire:
 - a. In the *Summary of the Issue* field, enter a description of the issue that you are observing on the endpoint.
 - b. In the *Reason of Escalation* field, select the reason that you are escalating this issue to the forensics team. If you are submitting a request to test that the forensics feature is functioning correctly on your EMS or FortiClient Cloud instance, select *Test Request*.

Request Forensics Analysis ✕

0 / 5 Request(s) in Progress

Summary of the Issue

Required

Reason of Escalation

- High Risk Application
- Malware Detection
- Intrusion Attempt
- Malicious Email
- High Risk Traffic
- Lateral Movement
- Test Request !

No real device info will be submitted, and a sample report will be available for download

Optional

First Identified Activity

Required

Actions Taken to Date

- Reboot of computer
- AV Scan
- Uninstall/Removal of any application
- Cleaning of browser data

Other

Supplementary Logs

Please Input log path

Finish

- c. In the *First Identified Activity* field, enter the date that you first observed the issue.
- d. In the *Actions Taken to Date* field, select any actions you took to resolve this issue.
- e. In the *Supplementary Logs* field, enter the path to logs that you would like the analyst to review.
- f. If desired, provide details in the *Comment* field.

Click *Finish*. Once you submit the request, EMS notifies FortiClient and the forensics agent on the endpoint starts collecting forensics logs. FortiClient uploads the logs to the cloud and shares a link with the analyst. In EMS, you can see status of the analysis request in the endpoint summary:

Status	Description
Ticket Status	Status of the ticket. Possible statuses are: <ul style="list-style-type: none"> • Request Submitted: EMS is creating the forensics analysis request and sending the information to the team. • Pending: Forensic analysis request has been initiated. The Forensics team has not yet assigned it to an analyst.

Status	Description
	<ul style="list-style-type: none"> • In Progress: Forensics team has assigned the request to an analyst, who has begun working on it. • Failed: request is in a failed state. This can be due to a variety of reasons, for example, the analyst may not be able to connect to the endpoint. The analyst may contact you regarding the reason for the failure. See the remaining steps in this procedure for how to contact the analyst. • Cancelled: indicates one of the following: <ul style="list-style-type: none"> • The analyst needed more information about the endpoint to perform the analysis. • The EMS administrator canceled the request. • Completed: analyst has completed analysis on the endpoint and shared the result in a PDF document. You can download the report from the endpoint summary's <i>Forensic Analysis</i> section.
Agent Status	<p>Status of the forensic agent collecting logs on the endpoint. Possible statuses are:</p> <ul style="list-style-type: none"> • Pending: EMS has notified FortiClient that a forensic analysis request is submitted, but the forensic agent is not running yet. • Running: forensics agent starts collecting forensics logs. • Collection Completed: forensics agent has completed collecting forensics logs. • Upload Started: FortiClient has started to upload the logs to the cloud. • Upload Completed: FortiClient has completed uploading the logs to the cloud. • Upload Failed: FortiClient failed to upload the logs to the cloud.
Task ID	Request ID in the FortiGuard forensics system.

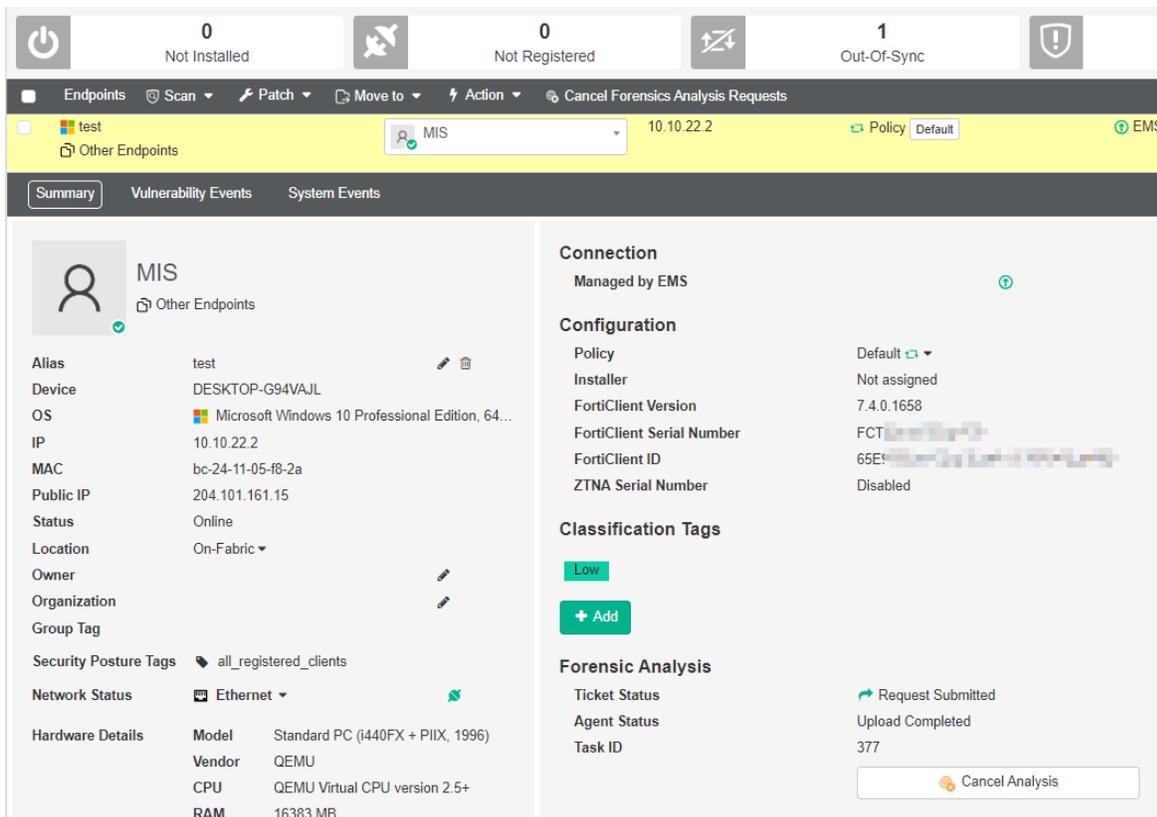
The following shows that EMS is creating the forensics analysis request and sending the information to the team. EMS has notified FortiClient that a forensic analysis request is submitted, but the forensic agent is not running yet:

Requesting forensic analysis on an endpoint

The screenshot displays the Fortinet FortiClient management interface. At the top, there are status indicators: 0 Not Installed, 0 Not Registered, and 1 Out-Of-Sync. Below this is a navigation bar with options like Endpoints, Scan, Patch, Action, and Cancel Forensics Analysis Requests. The main content area shows details for an endpoint named 'test' with IP address 10.10.22.2. The interface is divided into several sections: Summary, Vulnerability Events, and System Events. The Summary section includes fields for Alias (test), Device (DESKTOP-G94VAJL), OS (Microsoft Windows 10 Professional Edition, 64-bit), IP (10.10.22.2), MAC (bc-24-11-05-f8-2a), Public IP (204.101.161.15), Status (Online), Location (On-Fabric), Owner, Organization, Group Tag, Security Posture Tags (all_registered_clients), Network Status (Ethernet), and Hardware Details (Model: Standard PC (i440FX + PIIX, 1996), Vendor: QEMU, CPU: QEMU Virtual CPU version 2.5+, RAM: 16383 MB). The Connection section shows 'Managed by EMS'. The Configuration section lists Policy (Default), Installer (Not assigned), FortiClient Version (7.4.0.1658), FortiClient Serial Number (FCT...), FortiClient ID (65E...), and ZTNA Serial Number (Disabled). The Classification Tags section shows 'Low'. The Forensic Analysis section shows Ticket Status (Request Submitted), Agent Status (Pending), and Task ID (377). A 'Cancel Analysis' button is located at the bottom right of the Forensic Analysis section.

In the following screenshot, the *Agent Status* has updated to *Upload Completed*. FortiClient has completed uploading the logs to the cloud.

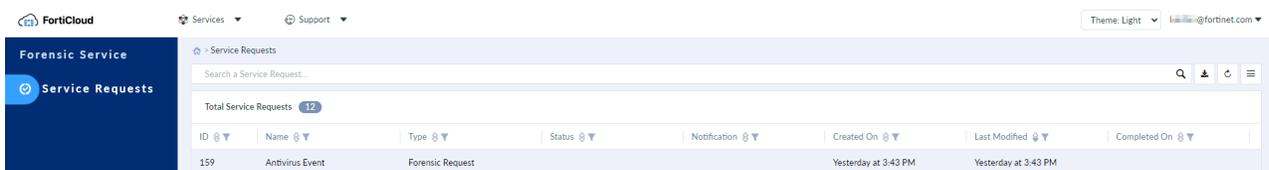
Requesting forensic analysis on an endpoint



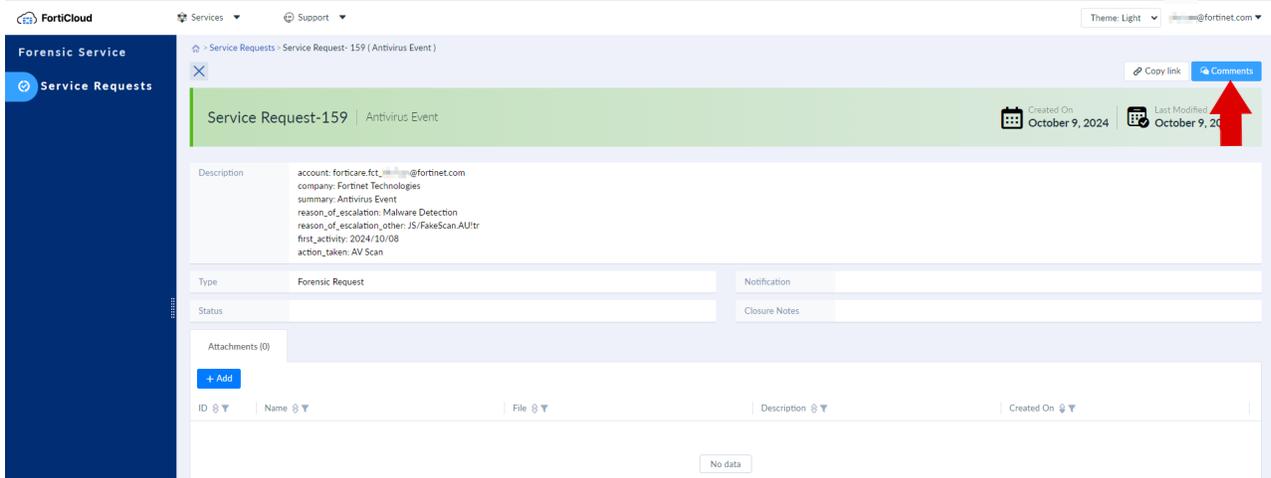
5. Do one of the following:

- Log in to the [Forensic Service portal](#) using your FortiCloud credentials.
- If using FortiClient Cloud, go to the *Forensics Analysis* tab on the left, then click the link to the Forensics Service portal. The link may not be available if the analyst has not created a service request for your analysis request.

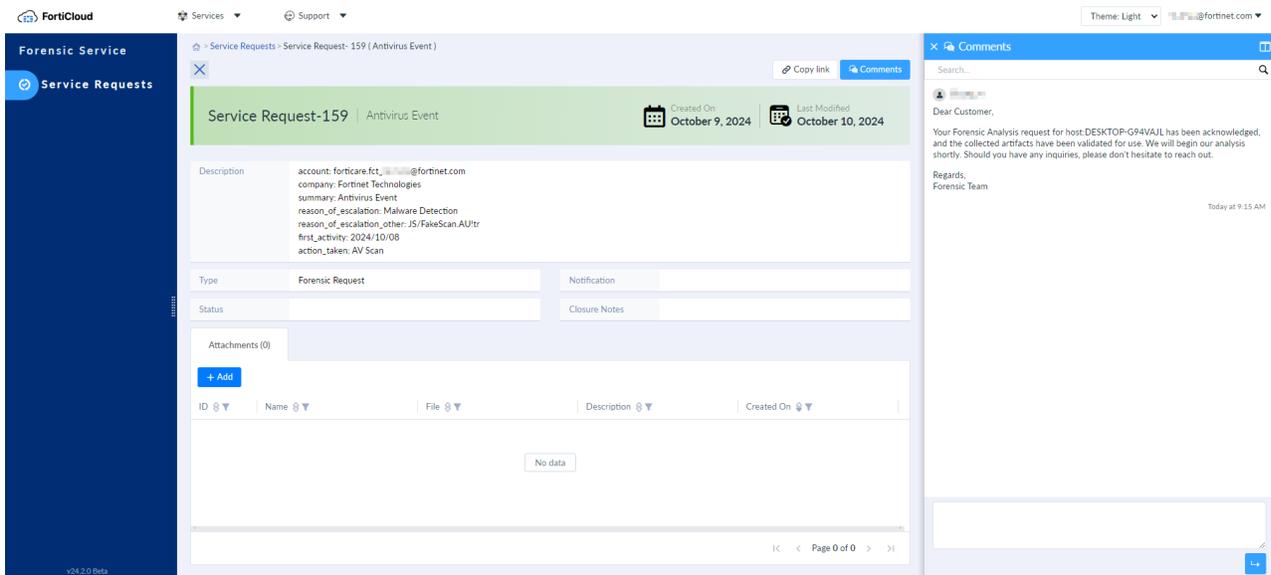
6. The *Service Requests* dashboard shows your service requests. Select the current request, in this example, *Antivirus Event*.



7. The service request page displays information about your request. Click *Comments* in the upper right corner.



- 8. The *Comments* pane displays messages from the Fortinet forensics team. You can also send the team messages to clarify details of your request. While your forensics analysis request is in progress, ensure that you monitor panel to provide the team details of your request as needed. You will also receive an email when the forensics team sends a message via this *Comments* pane.



- 9. Once the analysis is complete, you can click *Download Report* in the endpoint summary to view the details. You can also view the verdict that the analyst arrived at. You can also filter the endpoint list based on whether the forensics service is enabled, the status, and verdict.

Requesting forensic analysis on an endpoint

The screenshot displays the Fortinet FortiGuard console interface for an endpoint named 'Bilbo'. At the top, there are five status indicators: 'Not Installed' (0), 'Not Registered' (0), 'Out-Of-Sync' (0), 'Security Risk' (0), and 'Quarantined' (0). Below this is a navigation bar with 'Endpoints', 'Scan', and 'Action' menus, along with a search bar and filters.

The main content area is divided into several sections:

- Device Information:** Device: Bilbo; OS: Microsoft Windows 10 Profession...; IP: 192.168.0.5; MAC: 00-15-5d-51-42-03; Public IP: 172.19.200.93; Status: Online; Location: On-Fabric; Owner: [edit]; Organization: [edit]; Group Tag: [edit]; Zero Trust Tags: all_registered_clients; Network Status: Ethernet; Hardware Details: Model: Virtual Machine; Vendor: Microsoft Corporation; CPU: Intel(R) Core(TM) i9-9980...; RAM: 4095 MB; S/N: [redacted]; HDD: 79 GB.
- Policy:** Policy01; Installer: Not assigned; FortiClient Version: 7.2.2.0820; FortiClient Serial Number: FCT80C...; FortiClient ID: E6576F...; ZTNA Serial Number: 5D135F...
- Classification Tags:** Low; + Add.
- Forensic Analysis:** Ticket Status: Completed; Verdict: Compromised; Task ID: 3358; Download Report; Request Analysis.
- Security Features:** Antivirus enabled; Real-Time Protection enabled; Anti-Ransomware enabled; Cloud Based Malware Outbreak Detection installed; Sandbox installed; Sandbox Cloud enabled; Web Filter enabled; Video Filter enabled; Application Firewall enabled; Remote Access enabled; Vulnerability Scan installed; SSOMA installed; User Verification supported; ZTNA enabled; Privilege Access Management installed.
- Third Party Features:** Virus & Threat Protection: None.

Change log

Date	Change description
2024-10-11	Initial release.
2024-11-18	Updated: <ul style="list-style-type: none"><li data-bbox="418 531 737 562">• Introduction on page 4<li data-bbox="418 569 1149 600">• Requesting forensic analysis on an endpoint on page 6



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.