# Release Notes

## FortiEndpoint 26.1.b

**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

March 06, 2026
FortiEndpoint 26.1.b Release Notes
94-261b-1258835-20260306

# TABLE OF CONTENTS


**Introduction** ..... **5**
**Special notices** ..... **6**
Changes to compatibility with FortiManager 7.4 and 7.6 ..... 6
Web filter profile import limitation ..... 6
Entra ID integration support limitation ..... 6
Split tunnel ..... 6
SAML logins ..... 6
FortiGuard Web Filtering category v10 update ..... 7
**What's new** ..... **8**
What's new for 26.1.b ..... 8
What's new for 26.1.a ..... 8
What's new for 25.3 ..... 9
What's new for 25.1 ..... 10
What's new for 24.4 ..... 11
**Product integration and support** ..... **12**
**Supported regions** ..... **14**
**Resolved issues** ..... **16**
26.1.b ..... 16
EDR ..... 16
26.1.a ..... 17
Deployment and Installers ..... 18
Endpoint Management ..... 18
Endpoint Policy and Profile ..... 18
Fabric and Connectors ..... 18
Software Inventory ..... 18
Zero Trust Telemetry (On Boarding) ..... 19
ZTNA TCP/UDP Forwarding ..... 19
FortiGuard Outbreak ..... 19
EDR ..... 19
Vulnerabilities and Exposures ..... 22
25.3 ..... 22
Administration ..... 22
Endpoint Management ..... 23
Endpoint Policy and Profile ..... 23
Endpoint control ..... 24
Fabric Devices ..... 24
GUI ..... 24
Onboarding ..... 24
Remote Access ..... 24
System Settings ..... 25
Upgrade ..... 25
License ..... 25
Web Filter and Plugin ..... 25

Zero Trust Network Access (ZTNA) Connection Rules 26
Security Posture Tags 26
Other 26
EDR 26
25.1 28
Dashboard 28
Endpoint management 28
Endpoint policy and profile 29
Fortinet Security Fabric devices 29
Onboarding 29
Performance 29
Vulnerability Scan 29
ZTNA connection rules 29
EDR 30
Vulnerabilities and Exposures 30
**Known issues 31**
Endpoint control 31
Deployment and installers 31
Endpoint control 31
Endpoint management 32
Endpoint policy and profile 32
GUI 32
EDR 32

# Introduction

FortiEndpoint is Fortinet's unified endpoint security platform that integrates secure remote access, ZTNA, EPP, EDR, and Data Protection into a single agent with centralized management and simplified licensing—providing end-to-end visibility, prevention, detection, and response for today's modern enterprise.

This document provides the following information for FortiEndpoint:


- Special notices on page 6
- What's new on page 8
- Product integration and support on page 12
- Supported regions on page 14
- Resolved issues on page 16
- Known issues on page 31


For information about FortiEndpoint, see the *FortiEndpoint Administration Guide*.

# Special notices

## Changes to compatibility with FortiManager 7.4 and 7.6

FortiEndpoint 26.1.b drops support for FortiManager 7.4.0-7.4.8 and 7.6.0-7.6.4 due to the communication protocol upgrade from HTTP/1.0 to HTTP/2. Unlike HTTP/1.x, the new HTTP/2 replies do not include a traditional "200 OK" text response and cannot be interpreted by those FortiManager versions.

## Web filter profile import limitation

FortiEndpoint 26.1.b does not support importing web filter profiles from FortiOS 7.6.4 or later.

## Entra ID integration support limitation

FortiEndpoint supports Entra ID integration with Azure commercial subscription only. Azure Government (e.g. GCC, GCC High, GCC DoD) is not supported.

## Split tunnel

In FortiEndpoint 26.1.b, you configure application split tunnel using per-tunnel configuration, not a global configuration. If you are upgrading from an older version that uses the global application split tunnel configuration, change the configuration to per-tunnel.

## SAML logins

Upon initial SAML single sign on account login, FortiEndpoint creates a standard administrator for this user in *Administration* > *Admin Users*. A standard administrator has permissions to modify endpoints, policies, and settings. Having the EMS super administrator manually assign the proper role to the newly created login is recommended.

# FortiGuard Web Filtering category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the following versions:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS: https://support.fortinet.com/Information/Bulletin.aspx

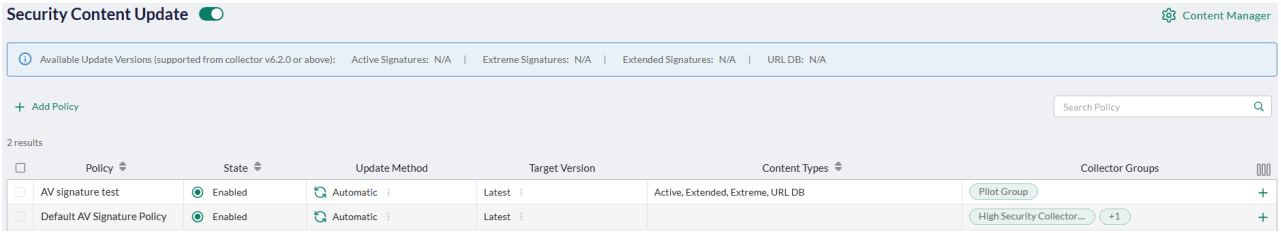
# What's new

The following sections list new features and changes for each FortiEndpoint release:


- What's new for 26.1.b on page 8
- What's new for 26.1.a on page 8
- What's new for 25.3 on page 9
- What's new for 25.1 on page 10
- What's new for 24.4 on page 11


# What's new for 26.1.b

- New EDR AV Signature policy to support OT and segmented environments that require controlled update windows (under *Profiles* > *Security* > *Security Content Update* in the EDR page). Use the AV Signature policy to define when and how EDR Collector groups download AV signatures for each type (Active, Extended, Extreme, and URL DB) based on time-based rules and time zones.




- New green color scheme of the EDR page (see above) for consistency with the EMS page.

# What's new for 26.1.a

- Windows Hello Business support for FortiGate SAML-based IPsec VPN—For FortiGate SAML-based auto-connect IPsec VPN tunnels using Microsoft Entra ID, Windows Hello for Business (key-based or certificate-based) authentication users now automatically connect to the tunnel after Windows login (using MFA with PIN or biometrics, such as fingerprint or facial recognition) without the need to re-authenticate for the VPN connection using the Entra ID username and password.
- Improve ZTNA and VPN troubleshooting process—EMS can now collect time-correlated IPsec VPN and ZTNA-related logs from FortiGate and FortiClient to help troubleshoot ZTNA and VPN integration issues between FortiGate and EMS.
- Support Referrer Host on Windows, macOS, and Linux—You can now define exclusions based on the referrer host (source) URL on FortiClient Windows, macOS, and Linux using the *Referrer Host* option in FortiEndpoint (see Web Filter) or the `<referrer>` XML option.

- Added support for uploading a custom FortiClient installer. To do so, go to *Deployment & Installers > FortiClient Installer*, click *Add*, and enable the *Create a manual installer* option under *Advanced Options* at the bottom of the *General* tab. See Adding a FortiClient installer in the FortiEndpoint Administration Guide for more information.
- FortiEndpoint EDR features and changes:
  - Secure browser—This feature is disabled by default.
  - The Forensics Viewer is back with the flow analyzer view, stacks view, and compare view.
  - Inconclusive events now appear in the Incidents view only if the FCS verdict is Malicious or Suspicious. The Action of such events will be Post Detection ( ) or Post Detection (Simulation) ( ), depending on whether the EDR console is in Prevention or Simulation mode. See Incidents pane for more information.
  - GUI enhancements:
    - "Raw data item" is renamed "variant"
    - Loading exceptions on supported Collectors only
    - Enhanced validation to exclusion fields

# What's new for 25.3

- FortiDeceptor integration—FortiDeceptor can connect to EMS, leveraging EMS capabilities to push deception tokens to FortiClient endpoints more efficiently without requiring mobile device management or group policy objects.
- FortiData integration—FortiClient can integrate with FortiData to retrieve file data labels and use them to control file access.
- Dual IPsec VPN tunnel support—You can create dual IPsec VPN IKEv2 connections for EMS-managed IPsec VPN tunnels, which allows you to route internet traffic through multiple VPN gateways for enhanced security.
- On-demand forensic artifact collection with forensic engine—Fortinet forensic analysts can request additional files from the endpoint for analysis on a case-by-case basis beyond the predefined set that the forensic engine collects. You can define the specific artifacts that the forensic agent collects and sends to EMS on-demand. You and forensic analysts can review these collected artifacts.
- RADIUS server authentication for administrators—You can configure a RADIUS server as an authentication server for EMS administrators so that they can log in to EMS with their RADIUS credentials. To enhance redundancy and scalability in the authentication process, you can configure multiple RADIUS servers for one EMS instance so that users can authenticate through various servers.
- Endpoint health check—In *Endpoints > All Endpoints*, the endpoint summary includes a new *Endpoint Health* section (which replaces the previous *Features* section) with a comprehensive view of feature statuses, such as whether a feature is installed, not installed, enabled, or disabled. It also reports any warnings or error messages associated with a feature.
- Support FortiClient ARM installer creation and deployment—FortiEndpoint supports creating and deploying an ARM installer to a Windows endpoint. You can also upload a repackaged ARM installer file to FortiEndpoint.
- FortiEndpoint EDR features and changes:
  - Host firewall—Use the new *Communications Control > Host Firewall* page to configure host firewall policies to control incoming and outgoing network traffic to protect endpoints against unwanted

connections based on remote addresses, protocols, or applications in use to reflect the organization's network policies.
- Disk encryption management for Windows and macOS endpoints—Use the new *Security Settings > Disk Encryption* page to configure disk encryption policies to enforce disk encryption on Windows 7 or later (using BitLocker, TPM is required) and macOS (using FileVault) endpoints to ensure consistent security configurations and compliance with regulatory requirements.
- New progress bar when exporting Communication Control applications
- The top-level row of the incidents view now represents an incident entity with its own state independent from the associated child events. As a result, filters are applied to both the top-level incidents and their child events. An incident may appear on its own if it matches the filter criteria even if none of its child events do.
- Localization - Chinese support

# What's new for 25.1

- ZTNA automatic login using Microsoft Entra ID—When a user is logged in to an Entra ID domain on an endpoint then attempts to access zero trust network access (ZTNA) TCP-forwarding traffic, FortiClient automatically authenticates with the FortiGate using Entra ID credentials without the need for manual authentication. This feature requires FortiOS 7.6.1 or later.
- FortiPAM agent for macOS—You can now install FortiClient with the FortiPAM feature enabled on a macOS endpoint.
- FortiEndpoint now automatically retrieves FortiAnalyzer Cloud SNI information (account ID) and populates it in endpoint log settings if the administrator's FortiCloud account has a FortiAnalyzer Cloud entitlement. You only need to enable *Auto-config FAZ Cloud* in *Endpoint Profiles > System Settings > Log* to automatically populate the FortiAnalyzer Cloud connection information in the IP Address/Hostname field.
- EAP-TTLS support for IPsec VPN—When using IKEv2, user authentication is handled via Extensible Authentication Protocol (EAP). In FortiEndpoint, you can now configure FortiClient to use EAP-TTLS for authentication, which provides a more secure and flexible user authentication method. Only IKEv2 supports EAP-TTLS.
- Zero Trust tag renamed security posture tag
- Security posture tags enhancements for easier management, for example, you can now easily add descriptions for tags and manage tags and rules in a single page for simplicity.
- Upload custom certificate and private key for ZTNA—You can upload a custom intermediate root certificate and private keys to FortiEndpoint to use for signing zero trust network access (ZTNA) endpoint certificates instead of relying on the default certificate, `default_ZTNARootCA.pem`. This provides flexibility for organizations that need custom certificate chains for compliance or security reasons. It can also streamline the end user experience by helping to avoid certificate trust issues.
- Consolidated endpoint events—You can now view all events from all endpoints and take actions as necessary in the new *Endpoints > All Events* page.
- Syncing remote categories from imported FortiOS or FortiManager Web Filter profile—Web Filter profiles imported from FortiOS or FortiManager to FortiEndpoint now include *FortiGuard Category Based Filter > Remote Categories*. Endpoints that are assigned this profile can follow this URL filter list to block outbound connections to known malicious URLs and domains. Prior to this enhancement, you had to

manually update the FortiOS static URL filter list, which was time-consuming, error-prone, and inconvenient.

- Vulnerability detection popup—You can now configure FortiClient to display a *Vulnerabilities Scan Summary* popup to the user after a vulnerability scan on the endpoint.
- FortiEndpoint EDR features and changes:
  - The *Event Viewer* tab is renamed *Incidents* with usability improvements, such as tabbed view of different types of incidents. Clicking on an incident displays the *Handle Incident* button and an embedded preview of the investigation view within the console where you can perform operations without opening a separate tab.
  - eXtended detection with custom external systems—You can now add custom external systems as eXtended detection source when you create an extended detection connector in the *Administration > Integrations* page.
  - Device security posture indicator for Windows and macOS endpoints—The *Inventory > Collectors* page includes the new *DEVICE SECURITY* column which provides insights into the security posture of Windows and macOS endpoints based on OS-level configurations.
  - Visibility into external attack surface with FortiRecon integration—Analysts can prioritize security alerts and incidents based on risk factors such as severity of vulnerabilities, relevance of threat intelligence feeds, and severity of affected endpoints, ensuring that efforts are focused on addressing the most significant risks to the organization.
  - New look and feel of the EDR console

# What's new for 24.4

Initial release.

# Product integration and support

The following table lists FortiEndpoint 26.1.b product integration and support information:

| | |
|---|---|
| **Server operating systems** | As FortiEndpoint installs the FortiClient agent and EDR collector, you must ensure that the endpoints are running an operating system version that supports both the deployed FortiClient version and the deployed EDR collector version.<br>You can deploy FortiEndpoint on endpoints running the following operating systems:<br>• Windows 11/10<br>• Microsoft Server 2019 or later<br>• macOS 13 (Ventura)/14 (Sonoma)/15 (Sequoia)/26 (Tahoe)<br>• Ubuntu 22.04 and 24.04/Red Hat 9/CentOS Stream 9<br>• Android 5.0.1/5.1.1/6.0/7.0/7.1/8.0/8.1/9/10/11/12/13/14/15<br>• iOS 9/10/11/12/13/14/15/16/17/18/26<br>  Legacy OS versions (see full list) are supported via separate standalone EDR deployment. Contact Fortinet Support for more details. |
| **Supported browsers** | • Google Chrome<br>• Microsoft Edge<br>• Mozilla Firefox |
| **FortiOS** | • 7.6.0 and later—For FortiOS 7.6.3 and later versions, see SSL VPN tunnel mode replaced with IPsec VPN.<br>• 7.4.0 and later |
| **FortiClient (Windows/macOS/Linux)** | • 7.4.0 and later<br>• 7.2.0 and later |
| **FortiClient iOS and Android** | • 7.4.0 and later |
| **FortiAnalyzer** | • 7.6.0 and later<br>• 7.4.0 and later |
| **FortiManager** | • 7.6.5 and later<br>• 7.4.9 and later<br>  FortiEndpoint 26.1.b does not support FortiManager 7.4.0-7.4.8 and 7.6.0-7.6.4 due to the communication protocol upgrade from HTTP/1.0 to HTTP/2. See Changes to compatibility with FortiManager 7.4 and 7.6 on page 6 for more details. |
| **FortiAuthenticator** | • 8.0.0 and later<br>• 6.6.0 and later |

| | |
|---|---|
| | • 6.5.0 and later |
| **FortiSandbox** | • 5.0.0 and later<br>• 4.4.0 and later |
| **FortiData** | • 7.6.1 and later |

# Supported regions

FortiEndpoint is hosted in the following regions:

- North America:
  - United States:
    - San Jose
    - Plano
  - Toronto
  - Vancouver
- EMEA:
  - Frankfurt
  - Madrid
  - U.K.:
    - London
- APAC:
  - Tokyo
  - Sydney
  - Singapore
- Middle East:
  - Dubai

EDR data is stored in selected locations only. Contact Fortinet Support for EDR data location options.

All customer FortiEndpoint data, including backup instances for redundancy or data recovery, are kept in the region selected when provisioning the cloud instance.

You can use the FortiEndpoint Service monitoring site to check the status of the FortiEndpoint service and any scheduled maintenance times.

FortiEndpoint is ISO/IEC 27001 certified. See ISO 27001 compliance standard.


ISO
27001

# Resolved issues

The following topics list issues fixed in each FortiEndpoint release:


- 26.1.b on page 16
- 26.1.a on page 17
- 25.3 on page 22
- 25.1 on page 28


## 26.1.b

The following issues have been fixed in FortiEndpoint 26.1.b:

### EDR

| Bug ID | Description |
|---|---|
| 1174797, 1177824 | Threat Hunting query that contains "NOT" does not filter correctly. |
| 1230971, 1231450 | Parsing failure of Taxii feed. |
| 1257703, 1249534, 1258256 | Adding a process to Exclusion Policy via Incident View results in blank screen. |
| 1229966, 1230923 | Exception creation fails due to an empty value. |
| 1234632, 1234818 | Failure in retrieving reports from a disconnected Collector. |
| 1224830, 1224852 | Users with a Read-Only role cannot export data from the Inventory page. |
| 1217600, 1224858 | Hardening related to key injection as a variable. |
| 1229820, 1233765 | Issue with dashboard queries of "Top Affected Devices". |
| 1234348, 1239292 | Incident Report fails to display the full event process path. |
| 1231073, 1235251 | Incident report generation gets stuck at 5%. |
| 1231674, 1232143 | Classification response actions are displayed in the wrong chronological order in Incident View. |
| 1234440, 1240548, 1237245 | Syslog becomes unresponsive due to a status update failure, causing log transmission to stop unexpectedly. |
| 1230144, 1235745 | Exception is created on the wrong security event. |

| Bug ID | Description |
|---|---|
| 1233707, 1234310 | Adding an incident comment is logged with a default user information. |
| 1232273, 1233766 | Sorting by total number does not correctly order the values in Incident View. |
| 1217982, 1222702 | Wrong file or process name is displayed while the correct file has been remediated. |
| 1227989, 1250027, 1228723 | Applying the “Malicious” classification filter prevents associated raw events from being displayed. |
| 1252095, 1252561 | Applying a filter prevents exporting the Collectors report in the Inventory. |
| 1252094, 1226670, 1252560 | Incidents sometimes appear as unclickable duplicates when you scroll or hover in the UI. |
| 1251352 | Certain events are partially saved during consolidation. |
| 1254115, 1252688, 1250220 | Editing an exception incorrectly displays an event as "deleted". |
| 1244654, 1246159, 1244724, 1244129, 1246479 | Potential error in consolidation flow. |
| 1243125, 1251355 | Multiple entities are marked as erased but are not actually cleaned from the database. |
| 1230520, 1240181 | When creating an exception via handling an event, selecting an IP from the destination list incorrectly selects all IPs. |
| 1240953, 1245595, 1242029 | Deleting an event while using a filter results in deletion of multiple events within the same aggregation. |
| 1227194, 1243039, 1227652 | Changing an exception’s destination from "Specific" to "All Destinations" incorrectly triggers a “cannot select both” error. |
| 1234354, 1235517, 1245708, 1237735 | Performance issue with event processing. |
| 1250351, 1251431 | Security Policy Search fails due to an internal error. |
| 1248720, 1249641 | Error when creating an exception on a specific event. |
| 1243641, 1244635 | Issue with exporting unmanaged devices list. |
| 1252134, 1254404 | Click "Add Connector" and the dropdown shows most connector options grayed out. |
| 1111981, 1218423 | When syslog field values are too long, the first max characters will be displayed. |

# 26.1.a

The following issues have been fixed in FortiEndpoint 26.1.a:

# Deployment and Installers

| Bug ID | Description |
|---|---|
| 1203744 | Installer assigned to a group of endpoints does not trigger the upgrade as the deployment schedule is not created. |

# Endpoint Management

| Bug ID | Description |
|---|---|
| 1216934 | Entra ID sync and deregistration issue. |
| 1179268 | Large Entra ID domain import fails. |

# Endpoint Policy and Profile

| Bug ID | Description |
|---|---|
| 1162867 | FortiEndpoint displays duplicate entries for web filter profiles imported from FortiGate. Deleting one of the duplicated entries results in both being removed. |
| 1176906 | After switching from "Manual Set" to "Mode Config" for an IKEv2 tunnel, FortiEndpoint still pushes the old manually set configuration to FortiClient. |
| 1204095 | Entra ID users are not matched against policies and end up matching the default policy. |

# Fabric and Connectors

| Bug ID | Description |
|---|---|
| 1150817 | No "Delete associated auto-detected ZTNA application data" option when removing a FortiGate from an HA cluster. |
| 1231061 | All destinations configured and synced from the FortiGate are duplicated on the ZTNA Applications Catalog. |

# Software Inventory

| Bug ID | Description |
|---|---|
| 1209075 | All software inventory is deleted within 10 minutes of software being reported by FortiClient. |

# Zero Trust Telemetry (On Boarding)

| Bug ID | Description |
|---|---|
| 1195127 | FortiEndpoint login using email fails if the UPN and SAM account name have different naming conventions. |

# ZTNA TCP/UDP Forwarding

| Bug ID | Description |
|---|---|
| 1104178 | ZTNA application is missing after being edited on the FortiGate. |
| 1158448 | The alias for a ZTNA server disappears from the FortiEndpoint GUI after you create a new ZTNA server on the FortiGate. |
| 1184219 | Auto-detected ZTNA destinations cannot be deleted, even after removal on the FortiGate. |

# FortiGuard Outbreak

| Bug ID | Description |
|---|---|
| 1103367 | Outbreak detection rules are tagged/untagged by FortiEndpoint. |

# EDR

| Bug ID | Description |
|---|---|
| 1234317 | Navigation bar display issue for low screen resolutions. |
| 1171377, 1170260 | Non-aggregated event ID in custom connector. |
| 1186639 | Issue with "Scan executable files only" in file scan. |
| 1158939 | Error message is confusing when the host firewall rule description exceeds 255 characters. |
| 1218426 | Added "Process Owner" to the Incidents list. |
| 1170992 | Confusing error message in Connectors page. |
| 1138142 | Missing icon for *Add rule* button in host firewall page. |
| 1171957 | Disk encryption should not list the partial encrypt option for macOS. |
| 1178979 | Sorting by *Last Seen Descending* leads to unreadable data on the *Communication* |

| Bug ID | Description |
|---|---|
| | *Control* page. |
| 1185174 | Deleting incident does not work after filtering. |
| 1186141 | No validation that aggregator mapping is unique for Collector move. |
| 1188836 | Misleading error message when a read-only user tries to enable a disk encryption policy. |
| 1184678 | UI refresh issue after a read-only user attempts to add groups to disk encryption or host firewall policies. |
| 1163104 | The *Add connector* drop-down menu should be sorted alphabetically. |
| 1211611 | Incident View sort issue. |
| 1224803 | Issue with username length limit. |
| 1230456, 1220014 | Isolating a device and removing isolation does not work in *Investigation View*. |
| 1238237, 1215753 | Incident ID is missing in syslog. |
| 1174766, 1179507 | An XDR event is displayed as unpopulated in *Incidents View*. |
| 1188797, 1191908 | Misalignment of classification. |
| 1159575, 1166684 | Issue with device count display. |
| 1182053, 1182450 | Unmanaged devices display issue. |
| 1186676, 1187253 | An exception output in a syslog message. |
| 1183540, 1187348, 1191060, 1188833 | Exclusion path validation causes Collector degradation. |
| 1182762, 1191427 | User access connector fails to connect after credentials update. |
| 1187519, 1188322 | Improved performance of *Get Logs* action. |
| 1187126, 1196273 | Issue with fetching threat hunting data when the organization is deleted. |
| 1200914, 1201714 | Issue with Linux Collector content upload. |
| 1179001, 1202248, 1184113 | Failure in exporting exception settings. |
| 1177744, 1203931 | Process name display issue in *Investigation View*. |
| 1191006, 1205581, 1199216 | A rare memory allocation issue. |
| 1193913, 1205080 | Error in configuration update. |
| 1159891, 1219304, 1196888, 1201154 | Covering query slows down with large number of destinations. |
| 1202613, 1209301 | Display issue in *Most Targeted* items view. |

| Bug ID | Description |
|---|---|
| 1204005, 1217350, 1235353, 1209298 | Core dergadation issue. |
| 1220710, 1209328, 1211303 | Advanced search display issue related to policies list and device groups. |
| 1204636, 1209664 | Moving a collector results in a license error. |
| 1210844, 1216877 | Sorting inventory by *Last Seen* switches back to the default sort. |
| 1218726, 1213231 | Layout issue of a long path in event analysis view. |
| 1212148, 1216876 | Consolidation status update sync issue. |
| 1126928, 1216841 | Event exception shows "with any script" instead of command line in the description. |
| 1210689, 1217325 | Cannot update existing threat hunting profile when associated to deleted categories. |
| 1217394, 1191006, 1219474, 1220588, 1221207, 1221209, 1225416, 1225928, 1227186, 1227190, 1228871, 1228776, 1230422, 1230989, 1232300, 1235808, 1236359, 1236360, 1238680, 1240019, 1240021, 1218992 | Memory handling issue causing display update delays and errors. |
| 1151334, 1220012 | Internal IP is shown as N/A in *Investigation View*. |
| 1055629, 1216874 | GUI issue with creating an exception on command line. |
| 1213961, 1218997 | Error in saving new applications in *Application Control Manager* after organization migration. |
| 1220688, 1225345 | Error message popup in *File Scan*. |
| 1225514, 1227791, 1225348 | Cannot load events when a filter is selected in the *Incidents View*. |
| 1226198, 1226608 | Incident export file contains irrelevant data. |
| 1211626, 1227651 | No Collector report under *Application Usage* when you select an application in the *Communication Control* page. |
| 1227059, 1230365 | Inconsistent results when searching event ID. |

| Bug ID | Description |
|---|---|
| 1229819 | Not all variants are displayed when using advanced filters in *Investigation View*. |
| 1182542, 1198243 | Deep scan failure when a duplicate IoT device is detected. |
| 1159891, 1163601 | Saving a specific exception is slow. |
| 1182540, 1183001 | CVE links in *Communication Control* goes to the old site instead of the new one. |
| 1207734, 1207962 1198710 | Failure in saving a new LDAP connector. |
| 1145570, 1156914 | Error when converting query. |
| 1231251, 1232168, 1232649 | Incidents with identical process names appear as separate incident entries. |

## Vulnerabilities and Exposures

FortiEndpoint 26.1.a is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

| Bug ID | Description |
|---|---|
| 1199423 | CVE-2025-59922 |
| 1229399 | CVE-2026-21643 |

# 25.3

The following issues have been fixed in FortiEndpoint 25.3:

## Administration

| Bug ID | Description |
|---|---|
| 1138296 | Admins with *Manage Invitations* permission cannot create invitations due to an unexpected error. |

# Endpoint Management

| Bug ID | Description |
|---|---|
| 1095972 | Local ad connector stuck at 1%. |
| 1111936 | Higher maximum limit for license timeout setting. |
| 1116089 | User cannot delete custom group with no associated endpoints. |
| 1117228 | LDAP sync fails due to long UPN char with the following error: *error: mssql: The data for table*valued parameter "@updated" doesn't conform*. |
| 1119648 | FortiEndpoint EMS is showing SAM user name instead of UPN name for endpoints logged in with Azure account. |
| 1135123 | Unable to add LDAP admin and unable to import user/device from domain with the following error: *Invalid idp guid*. |
| 1139290 | FortiEndpoint EMS AD sync intermittently fails with bind parameter and Kerberos errors. |
| 1139723 | LDAP sync improvement: reduce number of binds. |
| 1142865 | FortiEndpoint AD connector randomly goes offline and then comes online again. |
| 1148779 | (Windows) LDAP sync error "*uq_users_uid_name_sid_saml_id_auth_type_upn_domain_id*". |
| 1150306 | Endpoints cannot be returned to original group after being moved to a custom group. |
| 1150641 | Ad connector gets stuck after LDAP connection timeout. |
| 1152075 | GUI inconsistency in reporting the sync progress for LOCAL AD domain. |
| 1166665 | LDAP sync fails due to special characters in user data. |

# Endpoint Policy and Profile

| Bug ID | Description |
|---|---|
| 1112386 | FortiEndpoint EMS does not apply Azure user-group policies intermittently. |
| 1136465 | Error syncing web filter profile from FortiManager. |
| 1142846 | ZTNA application import enables UDP while the enable_udp option is set to FALSE. |
| 1159904 | Azure AD group-based policy assignments are not being applied: endpoints are receiving the default policy. |

# Endpoint control

| Bug ID | Description |
|---|---|
| 1140281 | Existing HTML files of "send one-way message" using Japanese cannot be previewed due to an error. |

# Fabric Devices

| Bug ID | Description |
|---|---|
| 1142252 | FortiGate fails to sync security posture tags from FortiEndpoint EMS, blocking compliant VPN users. |
| 1169328 | The firewall dynamic address table still keeps the IP/MAC even when VPN client is down. |

# GUI

| Bug ID | Description |
|---|---|
| 1153047 | FortiEndpoint EMS vulnerability scan dashboard shows wrong number of affected endpoints. |

# Onboarding

| Bug ID | Description |
|---|---|
| 1126324 | Cannot delete SAML configuration. |
| 1139975 | AD UPN matching case sensitivity for user verification with SAML authentication and domain authorization. |
| 1147712 | FortiClient cannot connect to FortiEndpoint EMS using AD accounts where SAMAccountName differs from UPN. |
| 1163833 | Invitation emails lose installer link after a while. |

# Remote Access

| Bug ID | Description |
|---|---|
| 1138981 | Dh group 31 is not available in FortiEndpoint EMS dhgroup: invalid value 31. |

| Bug ID | Description |
|---|---|
| 1160262 | FortiClient continiously attempts to connect to machine prelogon tunnel after user is already logged in. |

## System Settings

| Bug ID | Description |
|---|---|
| 1159054 | Tag removal issue for offline endpoints despite auto tag removal being enabled. |

## Upgrade

| Bug ID | Description |
|---|---|
| 995790 | During the device upgrade check, duplicate Android devices are end up getting mistaken as duplicates and deleted in upgrade. |

## License

| Bug ID | Description |
|---|---|
| 1143273 | FortiEndpoint license seats are out of sync with FortiCare during license renewal, causing license expiration and endpoints de-registration. |

## Web Filter and Plugin

| Bug ID | Description |
|---|---|
| 1026115 | Some web filter categories are not visible on FortiEndpoint EMS GUI for configuration. |
| 1156273 | FortiEndpoint EMS adds new XML tags to control FortiClient to force user to enabled "Allow in private" when the web filter plugin is enabled. |

## Zero Trust Network Access (ZTNA) Connection Rules

| Bug ID | Description |
|---|---|
| 1057009 | FortiEndpoint EMS GUI page shows "mask must be null or an IPv4 formatted string" error message when creating a ZTNA Destinations profile. |
| 1133163 | Failed to create ZTNA application due to long FQDN. |
| 1142055 | FortiClient randomly looses registry-based security posture tag, even if the condition is true to match the tag. |

## Security Posture Tags

| Bug ID | Description |
|---|---|
| 1148269 | In HA mode, FortiEndpoint EMS does not assign tags to the endpoint when connect to FortiEndpoint EMS after few days. |
| 1152696 | FortiEndpoint EMS does not assign *User in AD group* tag to macOS endpoints. |
| 1165567 | Failure in saving security posture tags for certificate with special character in Issuer CN. |
| 1176991 | Entra ID group is not shown when you hover over an affected endpoint's end user name in the FortiEndpoint EMS endpoint pane. |
| 1195069 | FortiClient cannot properly sync with FortiEndpoint EMS in retrieving the Security Posture tags. |

## Other

| Bug ID | Description |
|---|---|
| 1152169 | Restoring backup throws errors even when the restore is successful. |

## EDR

| Bug ID | Description |
|---|---|
| 1184211, 1184732, 1186391, 1187299, 1188820, 1191006, 1189146, 1191934, 1184679 | Memory issues on a massive response number from FCS due to an event that requires mail sending. |

| Bug ID | Description |
|---|---|
| 1182542, 1184109 | Scan fails when duplicate IoT devices are detected. |
| 1188797, 1191908 | Classification is not updated according to the classification received from FCS. |
| 1188319 | Connected Collectors do not appear in the group. |
| 1030485, 1035404 | Integration with FortiManager does not support Workspace mode. |
| 1139228, 1147014 | Integration with FortiSOAR fails. |
| 1095132, 1161767 | Error when creating an exception using an asterisk in the detected script (.sh file) on Linux. |
| 1131478, 1139171 | Failure in filtering events by SimulationBlock action. |
| 992289, 990535, 1001334, 964808, 815837 | Exception covering query issue with uncovered RDI's. |
| 1147352, 1156913 | Missing audit log of handling or unhandling an event. |
| 1158490, 1163603 | Unable to investigate or handle Threat Hunting incidents. |
| 1151959, 1158401 | Windows Collectors are shown as degraded after upgrade to 25.1. |
| 1119659, 1158402 | Moving a Collector to a group results in all Collectors from the selected Collector group being moved. |
| 1174120 | Failure in saving exception for a deleted event. |
| 1174766 | XDR events are not populated in Incidents view |
| 1177825 | Error with saved query event. |
| 1177053, 1177829 | Multiple drivers are blocked incorrectly under C:\System32\drivers folder. |
| 1179232, 1180072, 1180211, 1179504 | Faiure in loading the IoT Devices page. |
| 1181437, 1181391 | Memory issues. |
| 1161894, 1162753, 1173493, 1180517 | Issue with syslog and emails. |
| 1134239 | Archived events are not displayed as expected. |
| 1111573 | Update number of shards task causes many registration requests. |
| 1111339 | Threat hunting displays error "Query parsing failed". |
| 1126848 | Linux Collector registration failure. |
| 1053068, 1113772 | Incident page display issues. |
| 1115524 | Calculation of diff application control OOTB. |
| 1111822 | UI shows the device as isolated when it is not. |

| Bug ID | Description |
|---|---|
| 1111786 | App Control configuration sometimes does not reach the Collector. |
| 1111225 | Issue with updating application properties. |
| 1139614 | Failure in running ad hoc scan. |

# 25.1

The following issues have been fixed in FortiEndpoint 25.1:

## Dashboard

| Bug ID | Description |
|---|---|
| 1076303 | Vulnerability dashboard shows wrong numbers for low, medium, high, and critical vulnerabilities. |

## Endpoint management

| Bug ID | Description |
|---|---|
| 993480 | FortiClient unexpectedly disconnects from FortiEndpoint EMS. |
| 1076058 | Under *Administration > Authentication Servers*, you must edit the username and remove domain\ (or @domain) to authenticate via NTLM instead of Kerberos. |
| 1085449 | Azure domain sync is stuck at 1% because AdDaemon does not send all configured domains to Active Directory connector for syncing. |
| 1110507 | FortiEndpoint EMS does not use Kerberos authentication for LDAP and always uses NTLM. |
| 1112618 | FortiEndpoint EMS fails to recognize endpoints as Microsoft Entra ID-joined devices and puts them in workgroup instead of Entra ID group. |
| 1116613 | Invalid characters in filter by distinguished name causes LDAP result code 201 filter compile error. |
| 1116767 | FortiClient 7.2.7 cannot register with FortiEndpoint EMS because of the following error: *Error: mssql: Cannot insert duplicate key row in object 'dbo.Devices' with unique index 'uq_devices_guid'*. |
| 1116781 | Error occurs when syncing LDAP after updating EMS. |

## Endpoint policy and profile

| Bug ID | Description |
|---|---|
| 1082916 | EMS considers *.example.private wildcard FQDN an invalid zero trust network access (ZTNA) destination. |

## Fortinet Security Fabric devices

| Bug ID | Description |
|---|---|
| 1078114 | EMS OAuth 2.0 Fabric Connector has the following error: *Serial Number format does not match Connector Type*. |

## Onboarding

| Bug ID | Description |
|---|---|
| 1088431 | Connecting to EMS fails when using special characters like = in LDAP password. |

## Performance

| Bug ID | Description |
|---|---|
| 1021702 | AD connector has memory loss issue. |

## Vulnerability Scan

| Bug ID | Description |
|---|---|
| 798409 | EMS GUI does not display paths for detected vulnerabilities. |

## ZTNA connection rules

| Bug ID | Description |
|---|---|
| 1103786 | EMS does not support using underscore for ZTNA destinations. |
| 1118615 | Adding ZTNA rules in ZTNA destination profile automatically creates a manually |

| Bug ID | Description |
|---|---|
| | created ZTNA application in application catalog. |
| 1133163 | EMS fails to create ZTNA application due to long FQDN. |

# EDR

| Bug ID | Description |
|---|---|
| 984125, 992151 | Latency caused by an internal handling of muting security events. |
| 1000559 | In Fortinet pre-defined applications, selecting a group checkbox selects only the first page. |
| 987989 | Application Control and Exclusion validation error messages regarding the usage of wildcards in the application name/path are not accurate. |
| 996156 | In Fortinet pre-defined applications, application name is missing from audit logs. |
| 988393 | Spaces should not be allowed at the beginning or end of exclusion list names. |
| 988394 | Exclusion List name validation - Error message text display issue. |
| 985337 | Incorrect path length display in error message when importing or exporting exclusions. |
| 988385 | Cannot close the Import/Export Exclusion window using the *Close* (*X*) button. |

# Vulnerabilities and Exposures

FortiEndpoint 25.1 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

| Bug ID | Description |
|---|---|
| 958896 | CVE-2023-48786 |
| 958963 | CVE-2025-22855 |
| 1112619 | CVE-2025-22859 |

# Known issues

The following issues have been identified in FortiEndpoint 26.1.b. For inquiries about a particular bug, contact Customer Service & Support.

## Endpoint control

| Bug ID | Description |
|---|---|
| 1252180 | Endpoints on subnet 172.17.0.0/16 cannot register telemetry with FortiEndpoint. |

## Deployment and installers

| Bug ID | Description |
|---|---|
| 1247941 | FortiEndpoint deployment to update FortiClient feature sets for the same FortiClient version fails unless the initial deployment was done using the FortiEndpoint-generated FortiClient EXE installer or the MSI file (rather than the MST file). |

## Endpoint control

| Bug ID | Description |
|---|---|
| 1213829 | FortiClient auth-period registry is not reset to 0 after *User Verification Period* is disabled in FortiEndpoint. |

# Endpoint management

| Bug ID | Description |
|---|---|
| 1127493 | FortiEndpoint displays inaccurate user information for endpoints running on the Windows Server operating system. |
| 1211682 | Unable to delete ADDS authentication server when it is not reachable. |

# Endpoint policy and profile

| Bug ID | Description |
|---|---|
| 1089889 | Chromebooks intermittently receive error *Failed to retrieve user profile from FortiEndpoint*. |
| 1219573 | FortiEndpoint fails to apply Entra ID policies to Entra ID-joined devices that use an alias domains instead of the primary UPN domain. |

# GUI

| Bug ID | Description |
|---|---|
| 1186739 | Back button in endpoint vulnerability details page returns to Dashboard instead of previous page. |

# EDR

| Bug ID | Description |
|---|---|
| 1050795 | No message to explain why the user cannot set the UI to prevention mode when all policies are in simulation mode. |
| 733592 | Number of destinations under communication control is limited to 100 IP addresses. |
| 733598 | Safari 11.1 on macOS malfunctions when viewing events. |
| 757253 | EDR Connect cannot be used to run commands that are user-interactive. |

| Bug ID | Description |
|---|---|
| 765648 | On Linux, threat hunting exclusions only work in kernel space mode, not in user space mode. |
| 771630 | Device internal and external IP is missing from Threat Hunting events of Linux devices. |
| 777707 | Linux Collector content file is large and uploads slowly to the Central Manager. |
| 807930 | Application Control search only works by exact match |
| 809060 | EDR Connect session may be disconnected due to inactivity of the EDR Console, even though the Connect session is active. |
| 833152 | Raw data IDs appearing in the Collector tray and Incidents view may differ. |
| 837038 | Application Control cannot remove multiple tags in one action. |
| 842110 | In some network configurations, a rare issue might cause Collectors to be detected as IoT devices. |
| 885691 | Threat Hunting: The tooltip displayed when hovering might prevent access to adding a filter. |
| 889410 | When switching to Threat Hunting from *Incidents > Automated Analysis*, queries malfunction when more than one device is involved<br>**Workaround**: Filter by the same Collectors directly from Threat Hunting, which brings results. |
| 890339 | "Query Parsing Failed" in Threat hunting pops up multiple times after invalid query. |
| 891668 | Free text query in threat hunting, when using invalid text, no error message is displayed. The query returns empty results. |
| 892109 | Unable to filter by empty registry names in facets in Threat Hunting. |
| 894384 | In Threat Hunting, clicking *Retrieve Target File* for "File Rename" events retrieves the old file name instead of the renamed one. |
| 899736 | In a threat hunting search, if you search for "Target.Registry.Path:" AND "Registry.Path" the results will be empty<br>**Workaround**: Use either "Target.Registry.Path" or "Registry.Path" in a specific search. |
| 909654 | IoT filter by ″First connection=Today″ brings empty results. |
| 914348 | Investigation View: Incident response data is inaccurate. |
| 914792 | Unarchiving all events in large environments might cause the EDR console to malfunction.<br>**Workaround**: Filter events before unarchiving to reduce unarchive size. |
| 915698 | In the Investigation View, the message is wrong in the *Block address on firewall* window when you click *Firewall Block*. |

| Bug ID | Description |
|---|---|
| 935001, 938847, 1048422, 1064821, 1066657 | System event page default filtering is required. |
| 939481 | In some cases, the communication control feature does not work due to unforeseen technical issues. |
| 954553, 969494 | Some event log entries in threat hunting display logged event values in incorrect logged event fields. |
| 988884 | Incorrect threat hunting profile order of Fortinet pre-defined application profiles. |
| 994324 | Improve "file permission change" text in Threat Hunting Exclusions display. |
| 994334 | Added Threat Hunting columns are inaccessible unless the columns are narrowed. |
| 994348 | Log does not contain concrete helpful errors for API. |
| 994359 | Threat Hunting Collection Profiles - rule name and icon not aligned. |
| 1001334 | Security events fully covered by an exception retains the full coverage indication icon even after new uncovered raw data items come in. |
| 1003257, 1025493 | Missing field in Checkpoint firewall integration. |
| 1014489, 1035403 | Failure to delete aggregations in big bulks over 20K. |
| 1039714, 1041152 | Confusing error message when uploading a wrong formatted file in *Application Control Manager > Upload Applications*. |
| 1040055, 1041151 | Ad hoc network discovery tooltip has a mistake in Japanese. |
| 1040805, 1048215 | Incident view count changes with sort. |
| 1052668, 1060356 | Syslog is created with no audit. |
| 1062894, 1063406 | No validation for SecurityExclusionRepoEntity.path in exclusions configuration. |
| 1079894, 1081873 | Exceptions report can be slow. |

www.fortinet.com