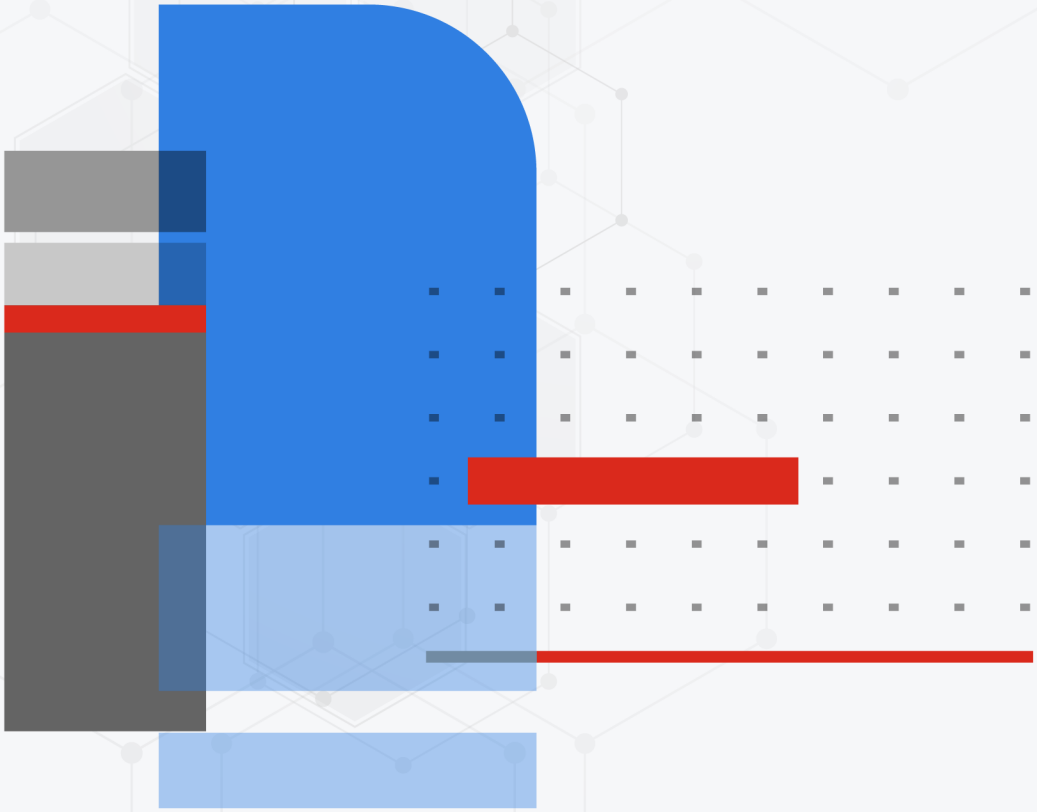
Release Notes

FortiClient (Linux) 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 27, 2025
FortiClient (Linux) 7.4.3 Release Notes
04-743-1109387-20251127

TABLE OF CONTENTS

Change log

Date	Change description
2025-03-20	Initial release.
2025-03-24	Updated: • Product integration and support on page 11 • Existing known issues on page 14
2025-03-25	Updated Installing FortiClient (Linux) from repo.fortinet.com on page 8.
2025-03-25	Updated Product integration and support on page 11.
2025-04-22	Added Common Vulnerabilities and Exposures on page 13.
2025-05-28	Updated Product integration and support on page 11.
2025-11-27	Updated Resolved issues on page 12 and Existing known issues on page 14.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Linux) 7.4.3 build 1736.

This document includes the following sections:

Review all sections prior to installing FortiClient.

Fortinet uses the following version number format:

<Major version number>.<minor version number>.<patch number>.<build number>

Example: 7.4.3.1736

Release Notes correspond to a certain version and build number of the product.

Licensing

See Windows, macOS, and Linux endpoint licenses.

Special notices

ZTNA certificates

Zero trust network access (ZTNA) certificate provisioning requires Trusted Platform Module (TPM) 2.0 on the endpoint with one of the following:

- Maximum of TLS 1.2 in FortiOS
- Maximum of TLS 1.3 in FortiOS if the TPM 2.0 implementation in the endpoint supports RSA PSS signatures

For ZTNA tags for checking certificates, FortiClient (Linux) does not check user certificates and only checks root certificate authority certificates installed on the system. These routes are:

Operating system	Route
Ubuntu	`/etc/ssl/certs/ca-certificates.crt`
• CentOS • Red Hat	`/etc/pki/tls/certs/ca-bundle.crt`

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 versions below:

- 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 in FortiClient (Linux) 7.4.3

For information about what's new in FortiClient 7.4.3, see FortiClient & FortiClient EMS 7.4 New Features.

Installation information

Installing FortiClient (Linux)

You can install FortiClient (Linux) on the following operating systems:

- Ubuntu
- CentOS
- Red Hat

For supported versions, see Product integration and support on page 11.

FortiClient (Linux) 7.4.3 features are only enabled when connected to EMS.

You must upgrade EMS to 7.2 or a later version before upgrading FortiClient.

See Recommended upgrade path for information on upgrading FortiClient (Linux) 7.4.3.

Installing FortiClient (Linux) from repo.fortinet.com

To install on Red Hat or CentOS:

1. Add the repository:
```
sudo yum-config-manager --add-repo
https://repo.fortinet.com/repo/forticlient/7.4/centos/8/os/x86_64/fortinet.repo
```
2. Install FortiClient:
```
sudo yum install forticlient
```

To install on Ubuntu:

1. Install the gpg key:
```
wget -O - https://repo.fortinet.com/repo/forticlient/7.4/ubuntu22/DEB-GPG-KEY | gpg --dearmor |
sudo tee /usr/share/keyrings/repo.fortinet.com.gpg
```
2. Create `/etc/apt/sources.list.d/repo.fortinet.com.list` with the following content:
```
deb [arch=amd64 signed-by=/usr/share/keyrings/repo.fortinet.com.gpg]
https://repo.fortinet.com/repo/forticlient/7.4/ubuntu22/ stable non-free
```
3. Update package lists:
```
sudo apt-get update
```
4. Install FortiClient:
```
sudo apt install forticlient
```

Installing FortiClient (Linux) using a downloaded installation file

To install on Red Hat or CentOS:

1. Obtain a FortiClient (Linux) installation rpm file.
2. In a terminal window, run the following command:
   `$ sudo dnf install <FortiClient installation rpm file> -y`
   `<FortiClient installation rpm file>` is the full path to the downloaded rpm file.

If running Red Hat 7, replace `dnf` with `yum` in the command in step 2.

To install on Ubuntu:

1. Obtain a FortiClient Linux installation deb file.
2. Install FortiClient using the following command:
   `$ sudo apt-get install <FortiClient installation deb file>`
   `<FortiClient installation deb file>` is the full path to the downloaded deb file.

Installation folder and running processes

The FortiClient installation folder is `/opt/forticlient`.

In case there are issues, or to report a bug, FortiClient logs are available in `/var/log/forticlient`.

Starting FortiClient (Linux)

FortiClient (Linux) runs automatically in the backend after installation.

To open the FortiClient (Linux) GUI:

1. Do one of the following:
   a. In the terminal, run the `forticlient` command.
   b. Open Applications and search for `forticlient`.

After running the FortiClient (Linux) GUI for the first time, you can add it to the favorites menu. By default, the favorites menu is usually on the left-hand side of the screen.

Uninstalling FortiClient (Linux)

You cannot uninstall FortiClient while it is connected to EMS. Disconnect FortiClient from EMS before uninstalling it.

To uninstall FortiClient from Red Hat or CentOS:

```
$ sudo dnf remove forticlient
```

If running Red Hat 7 or CentOS 7, replace `dnf` with `yum` in the command.

To uninstall FortiClient from Ubuntu:

```
$ sudo apt-get remove forticlient
```

Product integration and support

The following table lists version 7.4.3 product integration and support information:

Operating systems	• Ubuntu 22.04 and 24.04 • CentOS Stream 9 • Red Hat 9 and later All supported with KDE or GNOME
Minimum system requirements	• Linux-compatible computer with Intel processor or equivalent. • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections
FortiClient EMS	• 7.4.0 and later • 7.2.0 and later
FortiOS	• 7.6.0 and later. FortiOS 7.6.3 and later versions do not support SSL VPN tunnel mode. See Migrating from SSL VPN tunnel mode to IPsec VPN. • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
AV engine	7.0.38
IPS engine	7.6.1040
FortiEDR for Linux hF10	5.1.11.1041
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiAuthenticator	• 6.5.0 and later • 6.4.0 and later • 6.3.0 and later
FortiManager	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later

Resolved issues

The following issues have been fixed in version 7.4.3. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
1100661	FortiClient (Linux) does not send sever name indication when connecting to on-premise EMS.
1105523	FortiClient (Linux) does not have option to use the invitation code from new upgrade installer.

Remote Access

Bug ID	Description
1075772	VPN Unity features are inconsistent with FortiClient (Windows).
1114626	User can disable autoconnect on FortiClient when pushed from EMS.

Remote Access - SSL VPN

Bug ID	Description
1082262	When FortiClient (Linux) connects to SSL VPN, disconnects, then reconnects in quick succession, sometimes the reconnection fails.
1091033	SSL VPN with exclusive routing enabled and FortiGate and FortiClient (Linux) in same subnet does not disconnect gracefully.
1094273	SSL VPN resiliency fails when one of the gateways is not reachable after a reboot.
1099641	Connecting to SSL VPN tunnel fails when connecting over Wi-Fi.
1101442	SSL VPN drops during file downloads through the tunnel.

ZTNA connection rules

Bug ID	Description
1087113	Zero trust network access (ZTNA) does not work when subnet mask configured in EMS ZTNA rule.

Common Vulnerabilities and Exposures

Bug ID	Description
878156	FortiClient (Linux) 7.4.3 is no longer vulnerable to the following CVE Reference: • CVE-2024-50570

Known issues

Known issues are organized into the following categories:

- New known issues on page 14
- Existing known issues on page 14

To inquire about a particular bug or to report a bug, contact Customer Service & Support.

New known issues

No new issues have been identified in version 7.4.3.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Linux) and remain in FortiClient (Linux) 7.4.3.

Endpoint control

Bug ID	Description
1092354	Autoconnect only when offnet does not work.

Remote Access - IPsec VPN

Bug ID	Description
968442	IKEv2 with `<ipv4_split_exclude_networks>` does not work.
968473	IPsec VPN IKEv2 rekey fails with NO-PFS.
1007101	FortiClient (Linux) does not support IPsec IKEv2 with IPv6.
1076413	FortiClient (Linux) does not support split DNS with full tunnel IPsec VPN IKEv2.

Remote Access - SSL VPN

Bug ID	Description
950306	SSL VPN creates two interfaces and routes, causing traffic loss.
1027822	FortiClient fails to connect to VPN with *Config routing table failed* error.
1035496	FortiClient has connection problems with SAML, multifactor authentication, and Linux CLI options.
1087119	VPN CLI commands fail after shutdown and restart of FortiClient.
1087901	On Ubuntu 22.04, FortiClient shows 0 bytes received or sent while connected to SAML SSL VPN.
1102801	Linux clients using FortiClient for SAML authentication retain credentials.

Web Filter and plugin

Bug ID	Description
939743	Web Filter does not support IPv6.

ZTNA connection rules

Bug ID	Description
1101924	Zero trust network access (ZTNA) TCP forwarding does not work if using SAML authentication on Ubuntu.

www.fortinet.com