Release Notes

FortiClient (Linux) 7.4.5

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

December 11, 2025
FortiClient (Linux) 7.4.5 Release Notes
04-745-1208454-20251211

TABLE OF CONTENTS

Change log

Date	Change description
2025-12-11	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Linux) 7.4.5 build 1835.M.

This document includes the following sections:

- Special notices on page 6
- What’s new in FortiClient (Linux) 7.4.5 on page 8
- Installation information on page 9
- Product integration and support on page 12
- Resolved issues on page 13
- Known issues on page 14

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: 7.4.5.1835.M

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

Special notices

No IKEv1 support for IPsec VPN

FortiClient (Linux)7.4.5 no longer supports IKEv1 for IPsec VPN. Please migrate to using IKEv2 instead.

No new version of VPN-only agent

FortiClient (Linux)7.4.5 does not include a new version of the free VPN-only agent as no feature updates were made to the free VPN-only agent between 7.4.3 and 7.4.4. Users can continue to use the FortiClient (Linux) 7.4.3 free VPN-only agent.

Using the same default MTU size for VPN interfaces across all platforms

FortiClient (Linux)7.4.5 now uses the same default MTU size for SSL and IPsec VPN interfaces as Windows and macOS, which improves connection efficiency. You can modify the MTU size using the `<mtu_size>` XML option. See the XML Reference Guide.

No support for concurrent third-party tunneling or proxy clients

Using third-party tunneling or proxy clients (including VPN, DNS, HTTP(s), SOCKS, ZTNA or PAC files) in parallel or nested combination with FortiClient's VPN, ZTNA or Web Filter is not recommended nor supported.

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) 7.4.5

For information about what's new in FortiClient 7.4.5, 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 12.

FortiClient (Linux) 7.4.5 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) 7.4.5.

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 7.4.5 product integration and support information:

Operating systems	• Ubuntu 22.04 and 24.04 • CentOS Stream 9 • Red Hat 9 All supported with 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	• 7.4.5 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
AV engine	7.0.41
VCM engine	2.0034
FortiEDR for Linux hF10	5.1.15.1034
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later
FortiAuthenticator	• 8.0.0 and later • 6.6.0 and later • 6.5.0 and later
FortiManager	• 7.6.0 and later • 7.4.0 and later
FortiSandbox	• 5.0.0 and later • 4.4.0 and later

Resolved issues

The following issues have been fixed in version 7.4.5. For inquiries about a particular bug, contact Customer Service & Support.

Remote Access - SSL VPN

Bug ID	Description
1197576	SSL VPN and Realm connection with SAML MFA authentication fails on FortiClient Linux.

Zero Trust telemetry (On Boarding)

Bug ID	Description
1183973	After de-registeration from cloud EMS, FortiClient auto-registers back to cloud EMS on reboot.

ZTNA TCP/UDP Forwarding

Bug ID	Description
1202014	When multiple TCP forwarding authentication requests happen at the same time, they will all wait for a SAML auth response instead of reusing the response from the first authentication instance.

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 7.4.5.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Linux) and remain in FortiClient (Linux) 7.4.5.

Endpoint control

Bug ID	Description
949324	Re-authentication error for verified registered FortiClient endpoints with the SAML or Entra ID user verification type when *User Verification Period* is enabled in EMS.

Remote Access - IPsec VPN

Bug ID	Description
1199352	Missing DH-Group 28 for IPsec phase 1 and phase 2 settings.

Remote Access - SSL VPN

Bug ID	Description
1035496	FortiClient has connection problems with SAML, multifactor authentication, and Linux CLI options.

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.