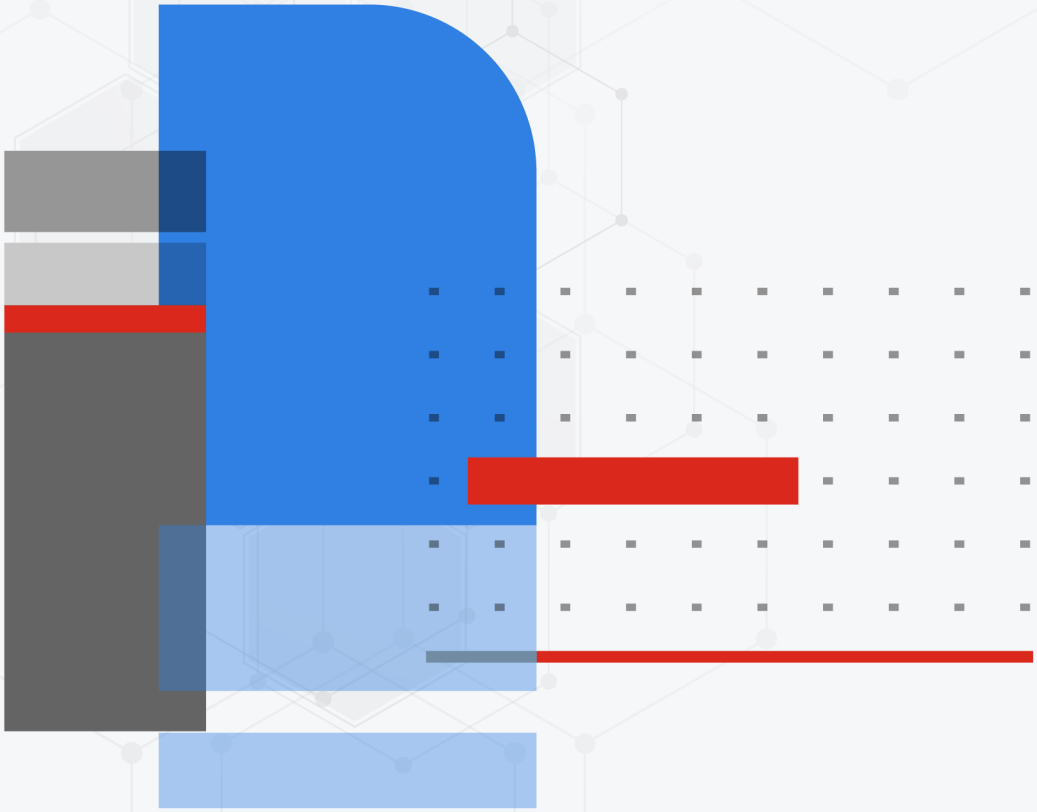
Release Notes

FortiClient (Linux) 7.4.7



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

April 27, 2026
FortiClient (Linux) 7.4.7 Release Notes
04-747-1284964-20260427

TABLE OF CONTENTS

Change log

Date	Change description
2026-04-27	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Linux) 7.4.7 build 1868.M.

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: 7.4.7.1868.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) 7.4.7 does not support IKEv1 for IPsec VPN. Please migrate to using IKEv2 instead.

No new version of VPN-only agent

FortiClient (Linux) 7.4.4 to 7.4.7 do 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 7.4.7. 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

Starting from 7.4.4, FortiClient (Linux) 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`

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) 7.4.7 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) 7.4.7.

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 7.4.7 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	• 7.4.7 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
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 • 7.2.0 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 • 7.2.0 and later
FortiSandbox	• 5.0.0 and later • 4.4.0 and later • 4.2.0 and later

Resolved issues

The following issue has been fixed in version 7.4.7. For inquiries about a particular bug, contact Customer Service & Support.

Other

Bug ID	Description
1189724	Security best practice: remove weak cipher support.

Known issues

Known issues are organized into the following categories:

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 7.4.7.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Linux) and remain in FortiClient (Linux) 7.4.7.

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

Bug ID	Description
1208501	Timeout and DNS resolution failure when using VPN over a USB Ethernet adapter with low MTU (e.g 1300). **Workaround:** Temporarily set MTU back to 1500 (`sudo ip link set dev eth0 mtu 1500`).

www.fortinet.com