FORTINET

Release Notes

FortiClient (Linux) 7.2.12

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

September 29, 2025
FortiClient (Linux) 7.2.12 Release Notes
04-7212-1200011-20250929

TABLE OF CONTENTS

Change log

Date	Change description
2025-09-29	Initial release.

Introduction

FortiClient (Linux) 7.2.12 is an endpoint product for well-known Linux distributions that provides Telemetry, remote access (IPsec VPN IKEv2 and SSL VPN), zero trust network access, malware protection, web filter, and vulnerability scan. FortiClient (Linux) can download and use FortiSandbox signatures.

This document provides a summary of support information and installation instructions for FortiClient (Linux) 7.2.12 build 1018.

Review all sections prior to installing FortiClient.

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 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 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

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

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 10.

FortiClient (Linux) 7.2.12 features are only enabled when connected to EMS 7.2 or later.

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

See Recommended upgrade path for information on upgrading FortiClient (Linux) 7.2.12.

Install 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/7.2/centos/8/os/x86_64/fortinet.repo
```
2. Install FortiClient:
```
sudo yum install forticlient
```

To install on Ubuntu 18.04 LTS and 20.04 LTS:

1. Install the gpg key:
```
wget -O - https://repo.fortinet.com/repo/forticlient/7.2/ubuntu/DEB-GPG-KEY | sudo apt-key add -
```
2. Add the following line in `/etc/apt/sources.list`:
```
deb [arch=amd64] https://repo.fortinet.com/repo/forticlient/7.2/ubuntu/ /stable multiverse
```
3. Update package lists:
```
sudo apt-get update
```
4. Install FortiClient:
```
sudo apt install forticlient
```

To install on Ubuntu 22.04 or 24.04 LTS:

1. Install the gpg key:
   ```
   wget -O - https://repo.fortinet.com/repo/forticlient/7.2/debian/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/7.2/debian/ 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 (Linux) installation rpm file> -y
   ```
   `<FortiClient (Linux) installation rpm file>` is the full path to the downloaded rpm file.

If running Red Hat 7 or CentOS 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 (Linux) using the following command:
   ```
   $ sudo apt-get install <FortiClient (Linux) installation deb file>
   ```
   `<FortiClient (Linux) 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:
   - In the terminal, run the `forticlient` command.
   - 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
```

To uninstall FortiClient from Ubuntu:

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

Product integration and support

The following table lists version 7.2.12 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
FortiClient EMS	• 7.2.0 and later
AV engine	6.00287
FortiAnalyzer	• 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 • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later
FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiOS	The following FortiOS versions support zero trust network access with FortiClient (Linux) 7.2.12: • 7.4.0 and later • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support SSL VPN with FortiClient (Linux) 7.2.12: • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later • 3.2.0 and later

Resolved issues

The following issue has been fixed in version 7.2.12. For inquiries about a particular bug, contact Customer Service & Support.

Remote Access - SSL VPN

Bug ID	Description
1117733	Unable to add default route for SSL VPN full tunnel or split tunnel with "all" as destination in policy.

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 7.2.12.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Linux) and remain in FortiClient (Linux) 7.2.12.

Remote Access

Bug ID	Description
1114626	User can disable autoconnect on FortiClient when it is pushed from EMS.

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.
1087901	On Ubuntu 22.04, FortiClient (Linux) shows 0 bytes while connected to SAML SSL VPN.
1094273	SSL VPN resiliency fails when FortiClient (Linux) cannot reach a gateway after reboot.
1102801	FortiClient (Linux) using SAML authentication retains credentials.

Web Filter and plugin

Bug ID	Description
977317	FortiClient does not use Web Filter rating URL provided using XML tag on EMS.

ZTNA connection rules

Bug ID	Description
1094278	Zero trust network access (ZTNA) fails to process when destination rule configured with port range.
1097804	FortiClient (Linux) does not save port range when ZTNA rules are manually created.
1155036	Zero trust network access (ZTNA) TCP forwarding SAML session starts redirect with TCP forwarding path.

Numbering conventions

Fortinet uses the following version number format:

<First number>.<Second number>.<Third number>.<Fourth number>

Example: 7.2.12.15

- First number = major version
- Second number = minor version
- Third number = maintenance version
- Fourth number = build version

Release Notes pertain to a certain version of the product. Release Notes are revised as needed.

www.fortinet.com