FORTINET

Release Notes

FortiClient (Linux) 7.2.5

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

October 09, 2024
FortiClient (Linux) 7.2.5 Release Notes
04-725-1045779-20241009

TABLE OF CONTENTS

Change log

Date	Change description
2024-08-29	Initial release.
2024-10-01	Updated Product integration and support on page 10.
2024-10-02	Updated Product integration and support on page 10.
2024-10-09	Added Numbering conventions on page 17.

Introduction

FortiClient (Linux) 7.2.5 is an endpoint product for well-known Linux distributions that provides FortiTelemetry, remote access (IPsec IKEv2 and SSL VPN), zero trust network access, malware protection, web filter, and vulnerability scan features. FortiClient (Linux) can also download and use FortiSandbox signatures.

This document provides a summary of support information and installation instructions for FortiClient (Linux) 7.2.5 build 0854.

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 (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 of FortiClient fails on Ubuntu 23.10

FortiClient (Linux) installation fails on Ubuntu 23.10. The workaround is to manually install the following packages on the Linux endpoint before installing FortiClient on Ubuntu 23.10:

```
apt install gconf2-common_3.2.6-8_all.deb
apt install libgconf-2-4_3.2.6-8_amd64.deb
```

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

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) 7.2.5 features are only enabled when connected to EMS 7.2.

You must upgrade EMS to 7.2 before upgrading FortiClient.

See Recommended upgrade path for information on upgrading FortiClient (Linux) 7.2.5.

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 Fedora:

1. Add the repository:
   ```
   sudo dnf 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 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 8:

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 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 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 7.2.5 product integration and support information:

Operating systems	• Ubuntu 22.04. FortiClient (Linux) does not support Ubuntu 24.04. • CentOS Stream 9 • Red Hat 9 and later • Fedora 36 and later All supported with KDE or GNOME
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
FortiClient EMS	• 7.2.0 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) 7.2.5: • 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) 7.2.5: • 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 issues have been fixed in version 7.2.5. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
1007406	On-fabric public IP address rule does not accept subnets.

Endpoint security

Bug ID	Description
1032585	FortiClient fails to retrieve antivirus (AV) signatures - *Failed to download components: object data does not match the data checksum*.

FortiSASE

Bug ID	Description
1006830	EMS cannot push certificate to FortiClient which blocks deep packet inspection on FortiSASE.

GUI

Bug ID	Description
923097	*Preferred DTLS Tunnel* does not work.

Installation and upgrade

Bug ID	Description
977227	Installation fails on Ubuntu 23.10.
1032729	FortiClient does not install on Ubuntu 24.04 LTS.

Logs

Bug ID	Description
1046405	FortiClient generates system log for certificate.
966994	Endpoint floods upload logs to FortiAnalyzer if its FortiAnalyzer does not authorize EMS.

Malware Protection and Sandbox

Bug ID	Description
986775	AV scan quarantines the fctdns file as threat.

Remote Access

Bug ID	Description
964411	SAML autoconnect does not work.
1023362	SAML internal browser fails to complete process.

Remote Access - IPsec VPN

Bug ID	Description
1020835	IPsec VPN tunnel remains up on FortiClient (Linux) despite FortiGate sending down signal on rekeying when there is phase 2 DH group mismatch.
1012075	IPsec VPN IKEv2 connectivity fails if the client is registered to custom site.
1022517	IPsec VPN may fail to configure routes.

Remote Access - SSL VPN

Bug ID	Description
902595	FortiClient GUI SAML prompt flashes on autoconnect.
1006588	FortiClient experiences DNS issues.

Vulnerability Scan

Bug ID	Description
832731	FortiClient server version `forticlient vulscan scan` command returns no vulnerabilities.
871782	Updating system time causes Vulnerability Scan to display incorrect information.
913032	EMS does not update vulnerability events correctly after user performs vulnerability scan from FortiClient (Linux).

Web Filter and plugin

Bug ID	Description
1025272	Web Filter causes page loading delay when FortiGuard service is unavailable.

ZTNA

Bug ID	Description
991514	ztproxy destination hostname cannot properly handle capitalization.

Zero Trust tags

Bug ID	Description
943692	Zero Trust tag for Ubuntu OS version does not work if incremental update versions are not given.

Zero Trust Telemetry

Bug ID	Description
1055456	Endpoint reregisters with old FortiClient Cloud when using switch option.

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 7.2.5.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Linux) and remain in FortiClient (Linux) 7.2.5.

Remote Access

Bug ID	Description
969563	FortiClient (Linux) does not properly set and use SSL VPN DNS settings on Ubuntu 22.04.

Remote Access - SSL VPN

Bug ID	Description
1025855	FortiClient (Linux) does not respond to connect option for SSL SAML VPN if FQDN is not getting resolved.
1027822	FortiClient fails to connect VPN with the error *Config routing table failed*.

Vulnerability Scan

Bug ID	Description
1029191	FortiClient (Linux) does not detect vulnerabilities in kernel when an older Linux kernel is being used and newer kernel is installed.

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
950953	ZTNA TCP forwarding does not show certificate content for untrusted certificate.
975845	FortiClient does not notify end user that certificate is not trusted for ZTNA connection when `<disallow_invalid_server_certificate>` is enabled.

Numbering conventions

Fortinet uses the following version number format:

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

Example: 7.2.5.15

- 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