FORTINET

Release Notes

FortiClient (Linux) 7.2.4

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

March 04, 2024
FortiClient (Linux) 7.2.4 Release Notes
04-724-998653-20240304

TABLE OF CONTENTS

Change log

Date	Change description
2024-03-04	Initial release.

Introduction

FortiClient (Linux) 7.2.4 is an endpoint product for well-known Linux distributions that provides FortiTelemetry, antivirus, SSL VPN, 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) 7.2.4 build 0809.

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 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 7.2.7 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) 7.2.4

For information about what's new in FortiClient 7.2.4, see the *FortiClient & FortiClient EMS 7.2 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) 7.2.4 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) 7.2.4.

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 7.2.4 product integration and support information:

Operating systems	• Ubuntu 18.04 and later • CentOS Stream 8, CentOS 7.4 and later • Red Hat 7.4 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) 7.2.4: • 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) 7.2.4: • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 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 7.2.4. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint management

Bug ID	Description
891264	EMS creates duplicate records for domain-joined Ubuntu endpoints.

GUI

Bug ID	Description
952680	GUI fails to launch and shows up blank or white.

Remote Access

Bug ID	Description
964411	SAML autoconnect does not work.

Known issues

The following issues have been identified in FortiClient (Linux) 7.2.4. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Avatar and social login information

Bug ID	Description
878050	Avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.
969058	FortiClient (Linux) pops up periodically after enabling *Notify Users to Submit User Identity Information*.

Configuration

Bug ID	Description
730415	FortiClient (Linux) backs up configuration that is missing locally configured ZTNA connection rules.

GUI

Bug ID	Description
902595	GUI SAML prompt flashes on autoconnect.
923097	*Preferred DTLS Tunnel* does not work.
972930	FortiClient has delay in opening the embedded or external browser after clicking *SAML* button for VPN connection.
975581	GUI does not open after fresh installation for root user and FortiClient (Linux) works only via CLI.

Malware Protection and Sandbox

Bug ID	Description
869664	Real-time protection does not monitor newly inserted USB drive.
888356	User can stop antivirus (AV) quick or full scan that EMS triggered.
986775	AV scan quarantines the fctdns file as a threat.

Installation and upgrade

Bug ID	Description
977227	Install fails on Ubuntu 23.10.

Logs

Bug ID	Description
872875	Disabling *Client-Based Logging When On-Fabric* in EMS does not work for Linux endpoints.
979669	User avatar fails to upload to FortiAnalyzer.

Endpoint control

Bug ID	Description
869658	FortiClient does not detect USB drive if the USB drive is not partitioned.
999081	When pushing endpoint certificates, EMS also pushes ZCONF even though that config is already up-to-date for the endpoint.

Onboarding

Bug ID	Description
872136	User verification period option under user verification does not work as configured.

Remote Access

Bug ID	Description
825387	SSL VPN with SAML when FQDN with DNS round robin is used for load balancing does not work.
851600	FortiClient fails to connect to SSL VPN with FQDN resolving to multiple IP addresses while FortiClient (Linux) cannot reach resolved IP address.
857154	FortiClient (Linux) does not include option to enable load balancing SSL VPN gateways with single FQDN.
874669	FortiClient does not attempt to connect with redundant SAML VPN gateway if it cannot reach first gateway.
876539	FortiClient on Red Hat 9 cannot resolve domain name properly using DNS server that SSL VPN pushed.
893237	User cannot reenter password during autoconnect after identity provider password change.
914271	SSL VPN resilience is misconfigured when pushed from EMS.
917898	`host-check-policy` works as AND operation instead of OR operation.
929544	SSL VPN tunnel created using the CLI fails to save the username and authentication is always disabled.
930919	VPN immediately disconnects.
941256	Ubuntu 20.04 and 22.04 do not use SSL VPN with `prefer_ssl_vpn_dns=1`.
950306	SSL VPN creates two interfaces and routes and causes traffic loss.
954067	FortiClient (Linux) autoconnect does not work with save-password option and SAML authentication.
969563	FortiClient (Linux) does not properly set and use SSL VPN DNS settings on Ubuntu 22.04.
972004	*Enable Invalid Server Certificate Warning* does not work for IPsec VPN with SAML authentication.
972089	FortiClient VPN is stuck at 98% when connected to iPhone hotspot.

System Settings

Bug ID	Description
829631	User cannot disable *Delete Timeout* in EMS.

Vulnerability Scan

Bug ID	Description
771833	FortiClient tags endpoint as vulnerable, even when EMS has enabled *Exclude Application Vulnerabilities Requiring Manual Update from Vulnerability*.
832731	Server version `forticlient vulscan scan` command returns no vulnerabilities.
868184	FortiClient fails to fetch VCM engine from FortiGuard distribution server.

Web Filter and plugin

Bug ID	Description
939743	Web Filter does not support IPv6.
962343	FortiClient does not block unrated sites when it cannot access FortiGuard servers.
977317	FortiClient does not use Web Filter rating URL provided using XML tag on EMS.

Zero trust tags

Bug ID	Description
943692	Ubuntu OS version ZTNA tag does not work for incremental update versions if major version is configured in rule settings.

ZTNA connection rules

Bug ID	Description
857909	FortiClient (Linux) does not support enabling encryption for ZTNA TCP forwarding rules acquired from ZTNA service portal.
857999	FortiClient (Linux) does not support using external browser for SAML authentication for ZTNA rules acquired through service portal.
941037	ZTNA destination does not work after host reboot.
950257	ZTNA destination works when using IP address but fails when using FQDN to the same destination.

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.

Other

Bug ID	Description
934636	FortiClient (Linux) displays an orange icon with exclamation mark on Linux deployments.

www.fortinet.com