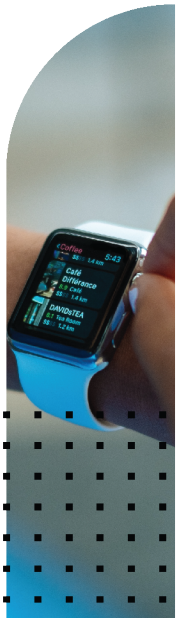
Release Notes

FortiClient (Linux) 7.0.8



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 16, 2023
FortiClient (Linux) 7.0.8 Release Notes
04-708-886316-20230316

TABLE OF CONTENTS

Change log

Date	Change Description
2023-03-16	Initial release.

Introduction

FortiClient (Linux) 7.0.8 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) 7.0.8 build 0292.

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 • Debian	`/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
- Debian
- CentOS
- Red Hat

For supported versions, see Product integration and support on page 9.

FortiClient (Linux) 7.0.8 features are only enabled when connected to EMS 7.0 or 7.2.

You must upgrade EMS to 7.0.2 or newer before upgrading FortiClient.

See Recommended upgrade path for information on upgrading FortiClient (Linux) 7.0.8.

FortiClient (Linux) 7.0.8 is not available to install from repo.fortinet.com.

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 or Debian:

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 or Debian:

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

Product integration and support

The following table lists version 7.0.8 product integration and support information:

Operating systems	• Ubuntu 18.04 and later • Debian 11 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	• 6.00258
FortiAnalyzer	• 7.2.0 and later • 7.0.0 and later
FortiClient EMS	• 7.2.0 and later • 7.0.0 and later
FortiManager	• 7.2.0 and later • 7.0.0 and later
FortiOS	The following FortiOS versions support zero trust network access with FortiClient (Linux) 7.0.8: • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support SSL VPN with FortiClient (Linux) 7.0.8: • 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	• 4.2.0 and later • 4.0.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later • 2.5.0 and later

Resolved issues

The following issues have been fixed in version 7.0.8. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
841149	FortiClient tries to use zero trust network access (ZTNA) certificate when ZTNA is disabled.

Avatar and social login information

Bug ID	Description
778017	Social media login does not work.

ZTNA connection rules

Bug ID	Description
821868	FortiClient certificate required for ZTNA does not appear in browser on Ubuntu 18.04.

Logs

Bug ID	Description
838555	fctsched fills up the syslog with logs.

Performance

Bug ID	Description
871645	FortiAnalyzer log upload on Linux has high memory usage.

Malware Protection and Sandbox

Bug ID	Description
857482	Built-in antivirus (AV) engine must be updated to 6.00282.
870602	fmon initiated from CLI terminates with runtime error when it redirects output outside of terminal.

Remote Access

Bug ID	Description
777191	With exclusive routing enabled, FortiClient (Linux) on Ubuntu can access local LAN devices.
810365	FortiClient fails to autoconnect to VPN on reboot.
815823	SSL VPN connection fails due to *vpn_connection:1276 Backup routing table failed* error.
822654	VPN does not skip routes pushed from FortiOS that cause routing issues.
833680	FortiClient (Linux) does not restore internal DNS if it crashed or did not properly restart while connected to SSL VPN.
874395	FortiClient (Linux) cannot connect to FortiGate via SSL VPN due to PPP getting read remote timeout error.
889370	FortiClient fails to connect to SSL VPN on CentOS 9 with *Config routing table failed* error.

Zero Trust tags

Bug ID	Description
832623	Zero Trust tagging rule for AV signature being up-to-date rule does not count the days that the signature was last updated.

Application Firewall

Bug ID	Description
834596	FortiClient cannot bypass DHCP traffic when EMS has quarantined it.

Known issues

The following issues have been identified in FortiClient (Linux) 7.0.8. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

ZTNA connection rules

Bug ID	Description
803402	Firefox fails to store zero trust network access (ZTNA) certificate on Ubuntu 22.04.

Avatar and social login information

Bug ID	Description
878050	FortiClient (Linux) avatar does not update on FortiGate dashboards and FortiGate cannot show updated information.

Malware Protection and Sandbox

Bug ID	Description
606634	FortiClient fails to remove quarantined files after number of days configured with cullage option.
713459	FortiClient crashes accompanied by scanunit.

Vulnerability Scan

Bug ID	Description
832731	Server version `forticlient vulscan scan` command returns no vulnerabilities.

Logs

Bug ID	Description
872875	Disabling *Client-Based Logging When On-Fabric* in EMS does not work for Linux endpoints.

License

Bug ID	Description
874676	Endpoint is tagged with existing ZTNA host tags for vulnerabilities and antivirus after EMS license is updated from Endpoint Protection Platform to Remote Access.

Remote Access

Bug ID	Description
781762	FortiSASE SSL VPN SAML autoconnect feature does not work.
782013	FortiSASE SSL VPN SAML always up feature does not work.
825387	SSL VPN with SAML when fully qualified domain name with DNS round robin is used for load balancing does not work.
871028	FortiClient (Linux) can connect to VPN when VPN profile options for SSL and IPsec VPN are disabled.
876539	FortiClient (Linux) cannot resolve domain name properly using DNS server pushed by SSL VPN in Red Hat 9.
892847	FortiClient always save SAML credentials. Credentials window is unavailable on subsequent login.
892973	"Core Dumped" failure occurs when configuring VPN tunnel with certificate on.
893237	User has no chance to reenter password during autoconnect after identity provider password change.

Configuration

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

Endpoint Control

Bug ID	Description
867394	Migration using *Switch EMS by IP* is not unified with *Switch EMS by Invitation*.
869658	FortiClient (Linux) does not detect USB drive if USB drive is unpartitioned.
870938	Quarantined FortiClient (Linux) can connect to VPN via CLI.

Onboarding

Bug ID	Description
811976	FortiClient may prioritize using user information from authentication user registered to EMS.

www.fortinet.com