Release Notes

FortiClient (Linux) 7.2.2

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

FORTINET TRAINING 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

October 04, 2023
FortiClient (Linux) 7.2.2 Release Notes
04-722-935804-20231004

TABLE OF CONTENTS

Change log

Date	Change Description
2023-10-04	Initial release.

Introduction

FortiClient (Linux) 7.2.2 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) 7.2.2 build 0753.

- Special notices on page 6
- What’s new in FortiClient (Linux) 7.2.2 on page 7
- Installation information on page 8
- Product integration and support on page 11
- Resolved issues on page 12
- Known issues on page 14

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 either 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`

What’s new in FortiClient (Linux) 7.2.2

For information about what's new in FortiClient 7.2.2, 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
- Debian
- CentOS
- Red Hat

For supported versions, see Product integration and support on page 11.

FortiClient (Linux) 7.2.2 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) 7.2.2.

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 and Debian:

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 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:
   1. In the terminal, run the `forticlient` command.
   2. 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 7.2.2 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	• 6.00287
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) 7.2.2: • 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) 7.2.2: • 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 7.2.2. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
921937	FortiClient (Linux) cannot register to EMS using *Register to EMS* button in invitation email.

Endpoint policy and profile

Bug ID	Description
915678	FortiClient (Linux) does not send acknowledged event to EMS if FortiClient (Linux) disconnects and reconnects to EMS right after acknowledging the one-way message.

Logs

Bug ID	Description
923245	Logs do not include timezone.

Remote Access

Bug ID	Description
777191	With exclusive routing enabled, Linux Ubuntu 18.02 using FortiClient still has access to local LAN devices.
909327	SSL VPN with SAML authentication fails to work after redirect to single sign on URL after authentication.

ZTNA connection rules

Bug ID	Description
871342	Zero trust network access error message showing on browser is not configurable.

Known issues

The following issues have been identified in FortiClient (Linux) 7.2.2. 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.

Configuration

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

GUI

Bug ID	Description
902592	GUI SAML prompt flashes on autoconnect.
923097	*Preferred DTLS Tunnel* does not work.

Malware Protection and Sandbox

Bug ID	Description
869664	Real-time protection does not monitor newly inserted USB drive.

Logs

Bug ID	Description
811746	FortiClient (Linux) sends duplicated and old logs to FortiAnalyzer.
872875	Disabling *Client-Based Logging When On-Fabric* in EMS does not work for Linux endpoints.

Endpoint control

Bug ID	Description
869658	FortiClient does not detect USB drive if the USB drive is not partitioned.
879108	EMS counts endpoint as on-Fabric when it does not meet all rules in an on-Fabric detection rule set.

License

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

Onboarding

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

Bug ID	Description
851600	FortiClient fails to connect to SSL VPN with FQDN resolving to multiple IP addresses while FortiClient (Linux) cannot reach resolved IP address.
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.
941256	Ubuntu 20.04 and 22.04 do not use SSL VPN with `prefer_ssl_vpn_dns=1`.
947381	When `prefer_sslvpn_dns=0` and SSL VPN is up, FortiClient (Linux) adds dns-suffix to all network interfaces.
949271	Dialup IPsec VPN split tunnel prefix limit is 200.
950306	SSL VPN creates two interfaces and routes and causes traffic loss.

Vulnerability Scan

Bug ID	Description
771833	FortiClient tags endpoint as vulnerable, even when EMS has enabled *Exclude Application Vulnerabilities Requiring Manual Update from Vulnerability*.
868184	FortiClient fails to fetch VCM engine from FDS.

Web Filter and plugin

Bug ID	Description
939743	Web Filter does not support IPv6.

Endpoint management

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

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.
950953	ZTNA TCP forwarding does not show certificate content for untrusted certificate.

FORTINET®

www.fortinet.com