FORTINET

Release Notes

FortiClient (Linux) 7.2.0

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 30, 2023
FortiClient (Linux) 7.2.0 Release Notes
04-720-848987-20230330

TABLE OF CONTENTS

Change log

Date	Change Description
2023-01-31	Initial release.
20223-03-30	Added Install FortiClient (Linux) from repo.fortinet.com on page 8. Updated Installing FortiClient (Linux) on page 8.

Introduction

FortiClient (Linux) 7.2.0 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) 7.2.0 build 0644.

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) 7.2.0

For information about what's new in FortiClient 7.2.0, 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) 7.2.0 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) 7.2.0.

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:
   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 7.2.0 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	• 6.00282
FortiAnalyzer	• 7.2.0 and later • 7.0.0 and later
FortiAuthenticator	• 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
FortiManager	• 7.2.0 and later • 7.0.0 and later
FortiOS	The following FortiOS versions support zero trust network access with FortiClient (Linux) 7.2.0: • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support SSL VPN with FortiClient (Linux) 7.2.0: • 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

Resolved issues

The following issues have been fixed in version 7.2.0. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
777473	FortiClient Cloud is unaware of UID change when it sends a new UID to FortiClient.
841149	Endpoint tries to use zero trust network access (ZTNA) certificate when ZTNA option is disabled.

Avatar and social login information

Bug ID	Description
778017	Social media login feature does not work.
825913	FortiClient (Linux) reports system user changes to EMS inconsistently.

Logs

Bug ID	Description
713287	FortiClient does not generate local logs for ZTNA.
838555	fctsched fills up the syslog with logs.

ZTNA connection rules

Bug ID	Description
821868	Certificate required for ZTNA do not appear in browser on Ubuntu 18.04.

Malware Protection and Sandbox

Bug ID	Description
857482	Built-in AV engine is not updated to 6.00282.

Remote Access

Bug ID	Description
824435	FortiClient does not update DNS domains on the correct interface.
777191	With exclusive routing enabled, FortiClient (Linux) on Ubuntu 18.02 still has access to local LAN devices.
810365	FortiClient (Linux) fails to autoconnect VPN on reboot.
822654	VPN does not skip pushed routes from FortiOS that cause routing issues.
833680	Linux internal DNS is not restored if Linux crashes or does not properly restart while connected to SSL VPN.

Zero Trust tags

Bug ID	Description
832623	AV signature is up-to-date rule does not count days.

Application Firewall

Bug ID	Description
834596	FortiClient (Linux) must bypass DHCP traffic when EMS quarantines it.

Known issues

The following issues have been identified in FortiClient (Linux) 7.2.0. 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. **Note**: Snap-based Firefox browsers do not work for ZTNA proxy in Ubuntu 22.04. You must download an apt-based Firefox browser to use this feature in Ubuntu 22.04.
871342	Allow ZTNA error message showing on browser to be configurable.

Avatar and social login information

Bug ID	Description
878050	Avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.

Malware Protection and Sandbox

Bug ID	Description
869664	Real-time protection does not monitor newly inserted USB drive.
870602	Fmon initiated from CLI terminates with runtime error when it redirects output outside of terminal.

Vulnerability Scan

Bug ID	Description
868184	FortiClient does not fetch VCM engine from FDS.

Performance

Bug ID	Description
871645	FortiAnalyzer log upload on Linux has high memory usage.
873422	FortiAnalyzer log upload reaches 100% memory usage when invalid FortiAnalyzer IP address is set.

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 Vulnerability and AV after EMS license is updated from Endpoint Protection Platform to Remote Access.

Endpoint control

Bug ID	Description
867394	FortiClient migration using *Switch EMS by IP* supports invitation code for migration.
869658	FortiClient does not detect USB drive if the USB drive is not partitioned.
870938	Quarantined Linux client can connect to VPN via CLI.
878514	FortiClient cannot get tenant ID after EMS administrator deploys FortiClient 7.2.0 over 7.0.7 from the EMS server.
879108	EMS counts endpoint as on-Fabric when it does not meet all rules in an on-Fabric detection rule set.

Remote Access

Bug ID	Description
825387	SSL VPN with SAML when FQDN with DNS round robin is used for load balancing does not work.
870048	FortiClient cannot retrieve correct public IP address after SSL VPN connection terminates.
871028	When VPN profile options for SSL and IPsec VPN are disabled, FortiClient can connect to VPN.
874395	FortiClient cannot connect to FortiGate via SSL VPN due to PPP getting read remote timeout error.
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.

Configuration

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

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.

www.fortinet.com