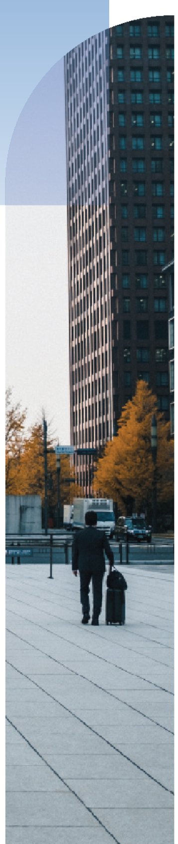
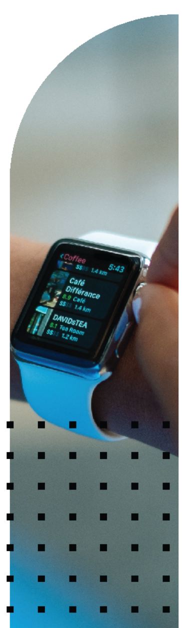
Release Notes

FortiClient (Linux) 7.0.4





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

April 27, 2022
FortiClient (Linux) 7.0.4 Release Notes
04-704-789533-20220427

TABLE OF CONTENTS

Change log

Date	Change Description
2022-04-27	Initial release.

Introduction

FortiClient (Linux) 7.0.4 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) 7.0.4 build 0169.

- Special notices on page 6
- What’s new in FortiClient (Linux) 7.0.4 on page 7
- Installation information on page 8
- Product integration and support on page 10
- Resolved issues on page 11
- Known issues on page 12

Review all sections prior to installing FortiClient.

Licensing

See Windows, macOS, and Linux endpoint licenses.

Special notices

Zero Trust Network Access 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	`/etc/ssl/certs/ca-certificates.crt`
• CentOS • Red Hat	`/etc/pki/tls/certs/ca-bundle.crt`

What’s new in FortiClient (Linux) 7.0.4

For information about what's new in FortiClient 7.0.4, see the *FortiClient & FortiClient EMS 7.0 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 10.

FortiClient (Linux) 7.0.3 features are only enabled when connected to EMS 7.0.

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

See Recommended upgrade path for information on upgrading FortiClient (Linux) 7.0.4.

FortiClient (Linux) 7.0.4 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:

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 7.0.4 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 All supported with KDE or GNOME
AV engine	• 6.00258
FortiAnalyzer	• 7.0.0 and later
FortiClient EMS	• 7.0.0 and later
FortiManager	• 7.0.0 and later
FortiOS	The following FortiOS versions support Zero Trust Network Access (ZTNA) with FortiClient (Linux) 7.0.4: • 7.0.0 and later The following FortiOS versions support SSL VPN with FortiClient (Linux) 7.0.4: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 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 7.0.4. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
766663	FortiClient (Linux) must process error first for a keepalive reply.
792659	FortiClient (Linux) loses connection to EMS after upgrade.

Malware Protection and Sandbox

Bug ID	Description
725402	FortiClient halts the operating system.

Remote Access

Bug ID	Description
780519	Always up option does not remain enabled after user manually disconnects SSL VPN tunnel when using SAML.
795407	FortiClient (Linux) deletes resolv.conf.

Known issues

The following issues have been identified in FortiClient (Linux) 7.0.4. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Avatar and social network login

Bug ID	Description
785876	JavaScript error while using external browser for SSL VPN SAML authentication.

Malware Protection and Sandbox

Bug ID	Description
713459	FortiClient crash accompanied by scanunit.

Remote Access

Bug ID	Description
715444	SSL VPN traffic drops randomly in FortiClient installed on Ubuntu.
776888	FortiClient does not dynamically display button to disconnect VPN unless you reopen the FortiClient (Linux) window.
777191	With exclusive routing enabled, Ubuntu 18.02 with FortiClient installed can access local LAN devices.
781762	FortiSASE SSL VPN SAML autoconnect feature does not work.
782013	FortiSASE SSL VPN SAML always up feature does not work.
796455	FortiClient fails to connect to SSL VPN with SAML even with external browser.

Configuration

Bug ID	Description
730415	FortiClient (Linux) backs up configuration that is missing locally configured Zero Trust Network Access connection rules.

www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.