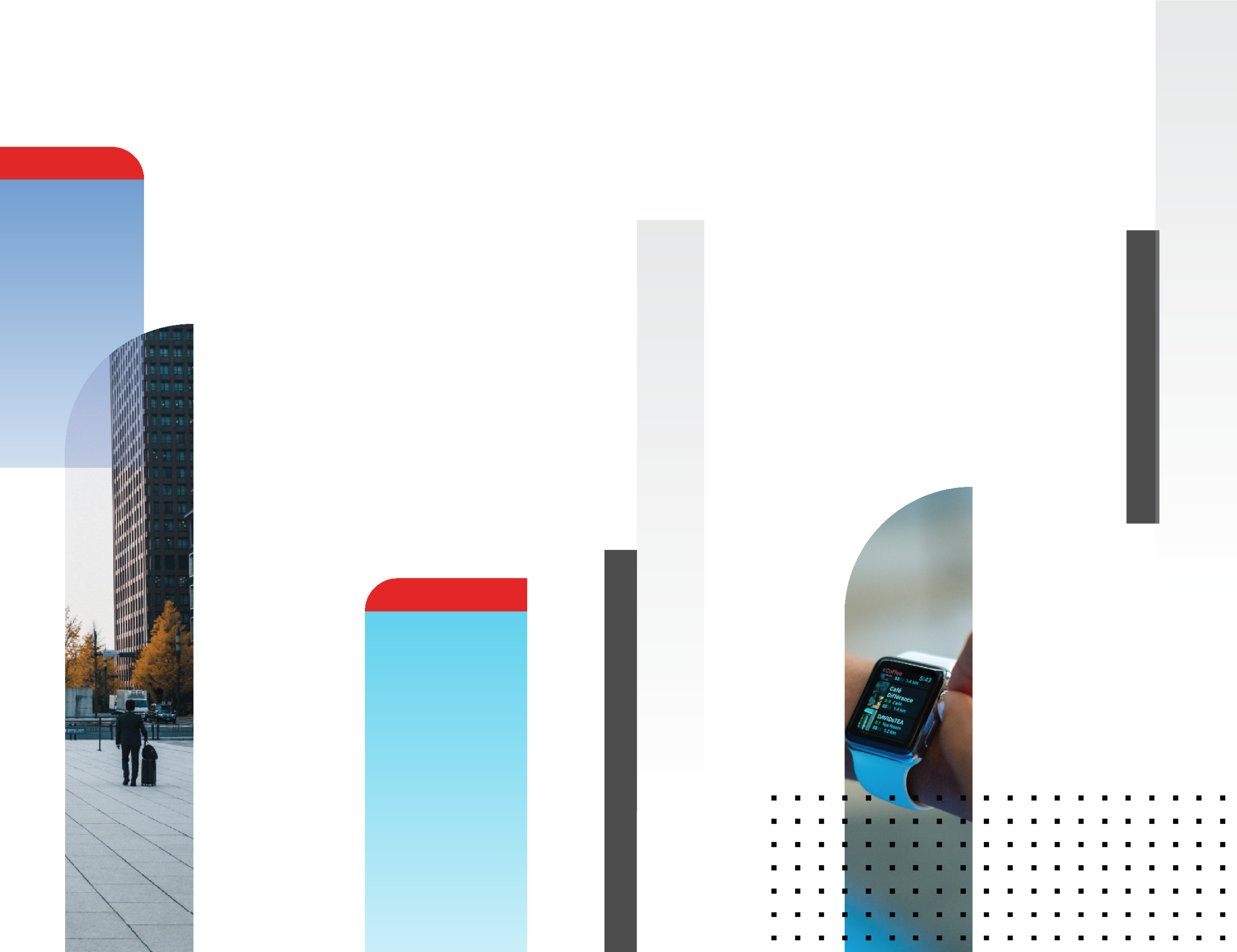
Release Notes

FortiClient (macOS) 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

FORTINET®

April 27, 2022
FortiClient (macOS) 7.0.4 Release Notes
04-704-789535-20220427

TABLE OF CONTENTS

Change log

Date	Change description
2022-04-27	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.0.4 build 0165.

This document includes the following sections:

- Special notices on page 6
- What's new in FortiClient (macOS) 7.0.4 on page 10
- Installation information on page 11
- Product integration and support on page 13
- Resolved issues on page 15
- Known issues on page 16

Review all sections prior to installing FortiClient. For more information, see the *FortiClient Administration Guide*.

Licensing

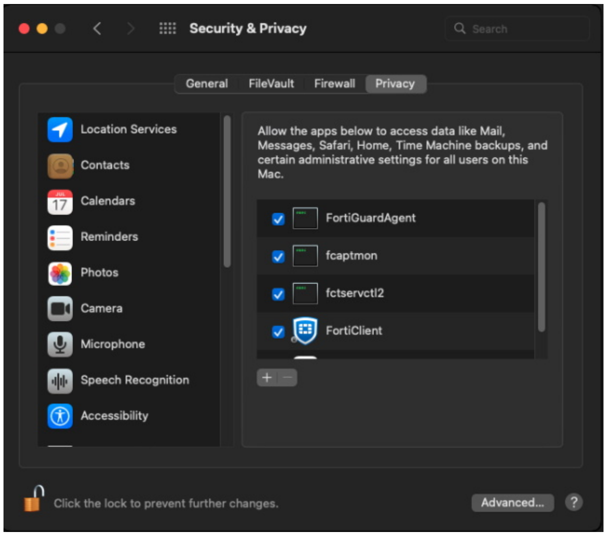
See Windows, macOS, and Linux endpoint licenses.

Special notices

Enabling full disk access

FortiClient (macOS) works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

- fcaptmon
- fctservctl
- fctservctl2
- fmon
- fmon2
- FortiClient
- FortiGuardAgent



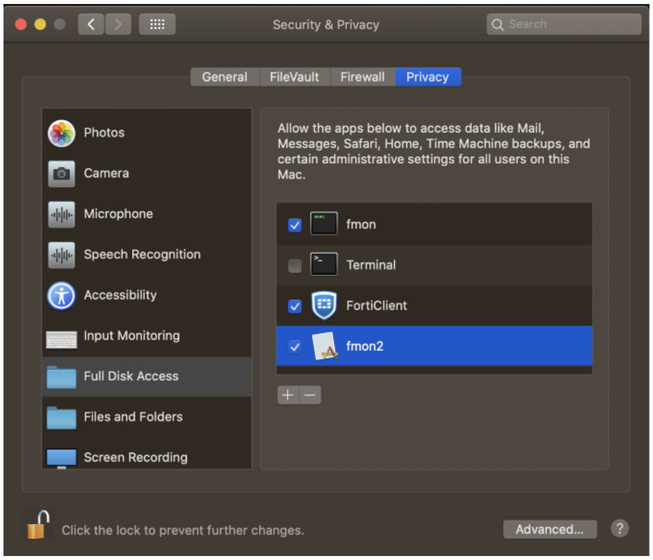
Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

☑ FortiGuardAgent
☑ fcaptmon
☑ fctservctl2
☑ FortiClient

Click the lock to prevent further changes.

The FortiClient (macOS) free VPN-only client does not include the fcaptmon, fmon, and fmon2 services. If you are using the VPN-only client, you only need to grant permissions for fctservctl and FortiClient.

You may have to manually add fmon2 to the list, as it may not be in the list of applications to allow full disk access to. Click the + icon to add an application. Browse to `/Library/Application Support/Fortinet/FortiClient/bin/` and select fmon2.



Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

- ☑ fmon
- ☐ Terminal
- ☑ FortiClient
- ☑ fmon2

Click the lock to prevent further changes.

The following lists the services and their folder locations:

- fmon, Fctservctl, Fcaptmon: `/Library/Application\ Support/Fortinet/FortiClient/bin/`
- FortiClient (macOS) application: `/Applications/FortiClient.app`
- FortiClient agent (FortiTray): `/Applications/FortiClient.app/Contents/Resources/runtime.helper/FortiGuardAgent.app`

Activating system extensions

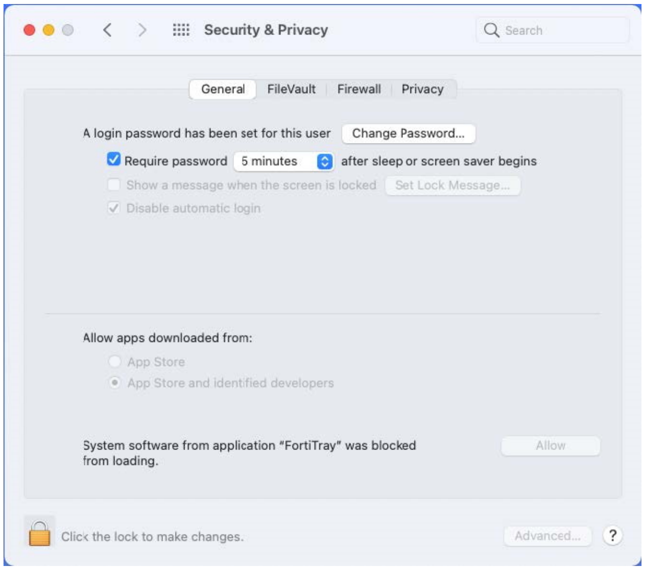
After you perform an initial install of FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

VPN

VPN works properly only when you allow system software from Fortinet to load in *Security & Privacy* settings.

To allow FortiTray to load:

1. Go to *System Preferences* > *Security & Privacy*.
2. Click the *Allow* button beside *System software from application "FortiTray" was blocked from loading*.



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

□ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

○ App Store

● App Store and identified developers

System software from application "FortiTray" was blocked from loading.

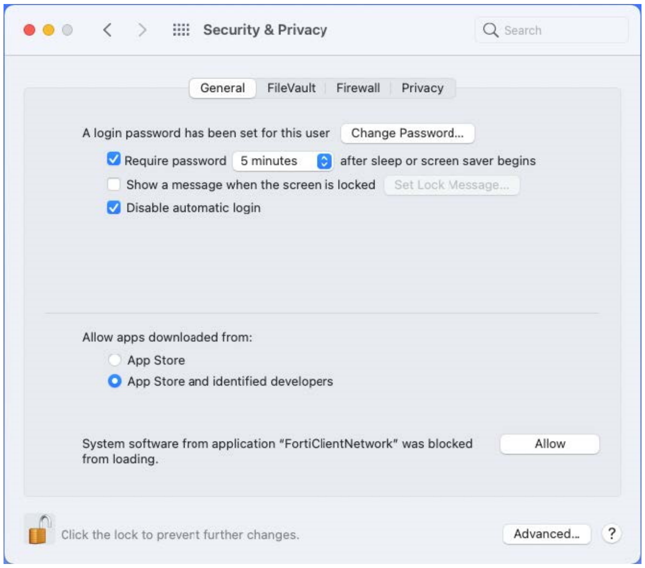
Click the lock to make changes.

Web Filter and Application Firewall

You must enable the FortiClientNetwork extension for Web Filter and Application Firewall to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

To enable the FortiClientNetwork extension:

1. Go to *System Preferences* > *Security & Privacy*.
2. Click the *Allow* button beside *System software from application "FortiClientNetwork" was blocked from loading*.



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

□ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

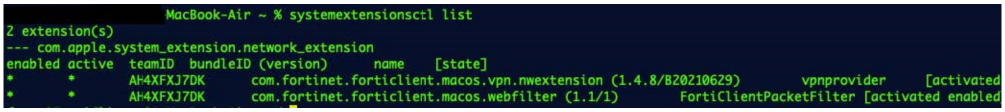
○ App Store

● App Store and identified developers

System software from application "FortiClientNetwork" was blocked from loading.

Click the lock to prevent further changes.

3. Verify the status of the extension by running the `systemextensionsctl list` command in the macOS terminal. The following provides example output when the extension is enabled:



```
[redacted] MacBook-Air ~ % systemextensionsctl list
2 extension(s)
--- com.apple.system_extension.network_extension
enabled active  teamID  bundleID (version)      name    [state]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.vpn.nwextension (1.4.8/B20210629)        vpnprovider     [activated
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.webfilter (1.1/1)        FortiClientPacketFilter [activated enabled
```

Enabling notifications

After initial installation, macOS prompts the user to enable FortiClient (macOS) notifications.

To enable notifications:

1. Go to *System Preferences* > *Notifications* > *FortiGuardAgent*.
2. Toggle *Allow Notifications* on.

DHCP over IPsec VPN not supported

FortiClient (macOS) does not support DHCP over IPsec VPN.

IKEv2 not supported

FortiClient (macOS) does not support IPsec VPN IKEv2.

MacBook Pro with M1X chip conflict

The FortiClient Application Firewall and Web Filter features conflict with the SSL VPN feature that is included on new MacBook Pro models that use the new M1X chip. This conflict does not occur on other macOS devices.

What’s new in FortiClient (macOS) 7.0.4

For information about what's new in FortiClient (macOS) 7.0.4, see the *FortiClient & FortiClient EMS 7.0 New Features Guide*.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.0.4.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.0.4.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from FortiClient.com:

File	Description
FortiClient_7.0.4.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.0.4.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.0.4 includes the FortiClient (macOS) 7.0.4 standard installer.

Review the following sections prior to installing FortiClient version 7.0.4: Introduction on page 5, Special notices on page 6, and Product integration and support on page 13.

Upgrading from previous FortiClient versions

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

FortiClient 7.0.4 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.0.4 features are only enabled when connected to EMS 7.0.

With the new endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.0.4.

Downgrading to previous versions

FortiClient 7.0.4 does not support downgrading to previous FortiClient versions.

Uninstalling FortiClient

The EMS administrator may deploy uninstall to managed FortiClient (macOS) endpoints.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal. After logging in, click on *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product integration and support

The following table lists FortiClient (macOS) 7.0.4 product integration and support information:

Desktop operating systems	• macOS Monterey (version 12) • macOS Big Sur (version 11) • macOS Catalina (version 10.15)
Minimum system requirements	• Intel processor or M1 chip • 256 MB of RAM • 20 MB of hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation
AV engine	• 6.00266
FortiClient EMS	• 7.0.0 and later
FortiOS	The following versions support ZTNA: • 7.0.0 and later The following versions support IPsec and SSL VPN: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiAnalyzer	• 7.0.0 and later
FortiManager	• 7.0.0 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
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

Language support

The following table lists FortiClient language support information:

Language	GUI	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)	Yes		
Chinese (traditional)	Yes		
French (France)	Yes		
German	Yes		
Japanese	Yes		
Korean	Yes		
Portuguese (Brazil)	Yes		
Russian	Yes		
Spanish (Spain)	Yes		

The FortiClient language setting defaults to the regional language setting configured on the client workstation unless configured in the XML configuration file.

If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Resolved issues

The following issues have been fixed in FortiClient (macOS) 7.0.4. For inquiries about a particular bug, contact Customer Service & Support.

Zero Trust Network Access connection rules

Bug ID	Description
786340	FortiClient (macOS) does not route Zero Trust Network Access (ZTNA) traffic to ZTNA proxy.

Remote Access

Bug ID	Description
780519	Always up option does not remain enabled after user manually disconnects SSL VPN tunnel when using SAML.

Vulnerability Scan

Bug ID	Description
770605	FortiClient (macOS) does not display the correct scheduled scan time information with weekly and monthly vulnerability scheduled scans.

Endpoint control

Bug ID	Description
766663	FortiClient (macOS) must process error first for a keepalive reply.
792659	FortiClient (macOS) loses connection to EMS after upgrade.
792662	`Route_type` for connecting to SSL VPN is `2` instead of `1`.

Known issues

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

Configuration

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

Zero Trust Network Access connection rules

Bug ID	Description
761497	macOS displays security confirmation popup twice on Monterey 12.0.1 when user starts, registers, unregisters, or shuts down FortiClient.

GUI

Bug ID	Description
753663	When using off-net profile with antivirus protection enabled, FortiClient (macOS) does not show Malware Protection in navigation bar.
763681	EMS cannot update current VPN connection on FortiClient (macOS).

Endpoint control

Bug ID	Description
706496	Deep inspection does not work and the endpoint does not download the certificate.
735589	Non-default site shows incorrect deployment state.

Remote Access

Bug ID	Description
723599	FortiClient uses FortiSASE egress IP address as the public IP address.
736245	IPsec VPN does not work when multiple remote gateways are configured in a priority-based list.
738425	SSL VPN GUI and tray mismatch in unity features.
750703	FortiClient (macOS) does not appropriately log IPsec and SSL VPN events on FortiAnalyzer.
765621	Network connection issue after waking from sleep mode.
768818	After connecting to SSL VPN main or full tunnel, user cannot access corporate internal network, while Internet works fine.
776888	FortiClient does not dynamically display button to disconnect VPN unless you reopen the FortiClient (macOS) window.
783439	SAML SSL VPN is stuck at authentication step with some identity providers.
783502	SSL VPN connection fails when fully qualified domain name is set for remote gateway.
785147	FortiSASE VPN does not automatically reconnect after upgrading FortiClient.
790392	FortiClient blocks the network when Wi-Fi is changed.
794215	GUI displays server name indication through EMS Telemetry information when connected to FortiClient Cloud.
794730	Auto connect and always up options appear as enabled after disconnecting from VPN when they are disabled on the XML profile.
800923	Customized host check failure message for SSL VPN does not work.
801134	FortiClient (macOS) does not generate or replicate SSL VPN logs for uploading to FortiAnalyzer when tunnel is established.

Zero Trust tags

Bug ID	Description
697655	ZTNA tag for file vault detection disappears.
793033	ZTNA LDAP group rule does not work.

Vulnerability Scan

Bug ID	Description
786011	Vulnerability feature does not autopatch macOS Monterey 12.2.1 after it detects operating system (OS) vulnerability on macOS Monterey 12.1.
790288	Vulnerability scan does not detect OS vulnerabilities.

Web Filter and plugin

Bug ID	Description
755055	When action set for site categories is warn, browser does not show the customized webpage, which allows user to bypass blocking.
757920	Web Filter does not get enabled when FortiClient (macOS) is off-Fabric.
758472	Web Filter does not work when SSL VPN is connected.
772332	External Ethernet adapter dongle gets disconnected when speed test is run.
795631	Web Filter does not block the selected categories.

Application Firewall

Bug ID	Description
718957	Application Firewall does not work after reboot.
800344	You can remotely access quarantined endpoints using VNC protocol.

Endpoint management

Bug ID	Description
770364	Disable third party features for macOS endpoints.

Performance

Bug ID	Description
778651	Large downloads and speed tests result in high latency, packet loss, and poor performance.

Install and deployment

Bug ID	Description
754722	Uninstall deployment from EMS does not work.
782213	FortiClient upgrade fails due to being unable to extract install file.

FORTINET®

www.fortinet.com