

FortiSwitch Release Notes

Version 6.2.2

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FORTINET PRIVACY POLICY

<https://www.fortinet.com/corporate/about-us/privacy.html>

FEEDBACK

Email: techdocs@fortinet.com



FortiSwitch Release Notes

August 19, 2020

11-622-566384-20200819

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models.....	5
What's new in FortiSwitchOS 6.2.2.....	5
Special notices	7
Supported features for FortiSwitchOS 6.2.2.....	7
Connecting multiple FSW-R-112D-POE switches.....	14
Upgrade information	15
Cooperative Security Fabric upgrade.....	15
Product integration and support	16
FortiSwitch 6.2.2 support.....	16
Resolved issues	17
Common vulnerabilities and exposures.....	17
Known issues	18

Change log

Date	Change Description
October 18, 2019	Initial release for FortiSwitchOS 6.2.2
October 30, 2019	Added bug 589129/591704.
December 3, 2019	Updated the feature matrix (added IPv6 and note 6).
February 4, 2020	Updated the “Common vulnerabilities and exposures” section.
April 27, 2020	Added bug 629721.
August 19, 2020	Added bug 566064.

Introduction

This document provides the following information for FortiSwitch 6.2.2 build: 0194.

- [Supported models on page 5](#)
- [Special notices on page 7](#)
- [Upgrade information on page 15](#)
- [Product integration and support on page 16](#)
- [Resolved issues on page 17](#)
- [Known issues on page 18](#)

See the [Fortinet Document Library](#) for FortiSwitch documentation.

Supported models

FortiSwitch 6.2.2 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE
FortiSwitch 5xx	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1048D, FS-1048E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 6.2.2

Release 6.2.2 provides the following new features:

- IPv6 router advertisement guard is now supported.
- Packet capture is now supported in the CLI and REST API.
- Interoperation with per-VLAN Rapid Spanning Tree Protocol (also known as Rapid PVSP or RPVST) is now supported.
- You can now enable priority tagging on outgoing frames with VLAN ID 0 for the native VLAN when you configure an 802.1p map.

- You can now trigger EAP authentication by sending multiple EAP packets to “silent supplicants” that send non-EAP packets when they wake up from sleep mode. The `set mab-eapol-request` command controls how many EAP packets are sent.
- RSPAN is now supported on the FSR-112D-POE model.
- The *System > FortiSwitchCloud* page now displays the status of the connection between the FortiSwitch unit and FortiSwitch Cloud.
- For increased security, you must create a password on your first login to the GUI or CLI of a FortiSwitch unit.
- There are more split-port modes for the 1048E model.
 - In the 4x100G configuration, ports 49, 50, 51, and 52 can now be split as 4x1G, 4x10G, 2x25G, and 2x50G, but only two of the four 100G uplink ports can be split.
 - In the 6 x 40G configuration, ports 49, 50, 51, and 52 can now also be split as 4 x 1G.
 - In the 4x4x25G configuration, all four 100G uplink ports (ports 49, 50, 51, and 52) can now be split as 4x1G, 4x10G, 2x25G, and 2x50G, but port 47 and 48 will be disabled.
- IGMP snooping, IGMP proxy, and IGMP querier are now supported on the FSR-112D-POE model.
- Reliable syslog using RFC 6587 is now supported.
- After a BIOS upgrade, passwords for all FortiSwitch local users must be reconfigured using the `config user local` command.
- Four new CLI commands allow you to clear and restore QoS or non-QoS hardware counters on all ports or specified ports.
- There are eight new API endpoints:
 - `execute/start/sniffer-profile-capture`
 - `execute/pause/sniffer-profile-capture`
 - `execute/stop/sniffer-profile-capture`
 - `execute/download/sniffer-profile`
 - `monitor/system/sniffer-capture-summary/<profile_name>`
 - `monitor/switch/modules-summary`
 - `monitor/switch/modules-limits`
 - `monitor/switch/modules-status`
- Unicast reverse-path forwarding (uRPF) is now supported.
- Additional object identifiers (OIDs) are supported by the LLDP management information base (MIB) file.
- You can now set the flow-tracking level so that the FortiSwitch unit collects the source MAC address and destination MAC address from the sample packet. You can also display the flow-export data or raw data for a specific MAC address.
- The specified VLAN configured in an LLDP-MED profile for a port will be automatically added in the allowed-vlans in a port.
- New `diagnose switch physical-ports hw-counter` commands provide access to some details of RX/TX packet counters for 124D, 2xx, and above.
- Three more FortiSwitch-compatible transceivers are now supported: FN-TRAN-QSFP+SR/QSFP-40GA4BDRNFN, FN-TRAN-SFP+LR/LCP-10G3B4QDRZFN, and FN-TRAN-SFP+SR/LCP-10G3A4EDRZFN.
- Diagnostics monitoring is now supported on QSFP+ transceivers.
- You can now enable logging when dynamic MAC addresses are learned, moved, and deleted.

Special notices

Supported features for FortiSwitchOS 6.2.2

The following table lists the FortiSwitch features in Release 6.2.2 that are supported on each series of FortiSwitch models. All features are available in Release 6.2.2, unless otherwise stated.

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Management and Configuration									
CPLD software upgrade support for OS	—	—	—	—	—	—	—	1024D 1048D	—
Firmware image rotation (dual-firmware image support)	—	✓	✓	148E 148E-POE	✓	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓	✓	✓	✓
Support for switch SNMP OID	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP conflict detection and notification	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiSwitch Cloud configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security and Visibility									
802.1x port mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
802.1x enhancements, including MAB	✓	✓	✓	✓	✓	✓	✓	✓	✓
MAB reauthentication disabled	—	✓	✓	✓	✓	✓	✓	✓	✓
open-auth mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
Support of the RADIUS accounting server	Partial	✓	✓	✓	✓	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages	—	✓	✓	✓	✓	✓	✓	✓	✓
EAP Pass-Through	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network device detection	—	—	✓	—	✓	✓	✓	✓	✓
IP-MAC binding	✓	—	—	—	—	—	✓	✓	✓
sFlow	✓	✓	✓	—	✓	✓	✓	✓	✓
Flow export	—	—	✓	—	✓	✓	✓	✓	✓
ACL	—	—	✓	—	✓	✓	✓	✓	✓
Multistage ACL	—	—	—	—	—	—	✓	✓	✓
Multiple ingress ACLs	—	—	✓	—	✓	✓	✓	✓	✓
Schedule for ACLs	—	—	✓	—	✓	✓	✓	✓	✓
DHCP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
Allowed DHCP server list	—	✓	✓	✓	✓	✓	✓	✓	✓
DHCP blocking	—	—	✓	—	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
IP source guard	—	—	✓	—	✓	✓	—	—	—
Dynamic ARP inspection	✓	—	✓	✓	✓	✓	✓	✓	✓
ARP timeout value	—	✓	✓	✓	✓	✓	✓	✓	✓
Access VLANs	—	✓	✓	✓	✓	✓	✓	✓	✓
VLAN tag by ACL	—	—	✓	—	✓	✓	✓	✓	✓
RMON group 1	—	✓	✓	✓	✓	✓	✓	✓	✓
Reliable syslog (RFC 6587)	—	✓	✓	✓	✓	✓	✓	✓	✓
Packet capture	—	—	✓	—	✓	✓	✓	✓	✓
Layer 2									
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	8	8	8	24/48	24/48	24/64
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓	✓	✓
IPv6 RA guard	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP proxy	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP querier	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP transmit	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED: ELIN support	—	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
LLPD-MED: PoE negotiation	—	✓	✓	✓	✓	✓	✓	—	—
Per-port max for learned MACs	—	—	✓	✓	✓	✓	✓	—	—
MAC learning limit (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—
Learning limit violation log (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—
set mac-violation-timer	—	✓	✓	✓	✓	✓	✓	✓	✓
Sticky MAC	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total MAC entries	—	✓	✓	✓	✓	✓	✓	✓	✓
MSTP instances	—	0-15	0-15	0-15	0-15	0-15	0-32	0-32	0-32
STP root guard	—	✓	✓	✓	✓	✓	✓	✓	✓
STP BPDU guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rapid PVST interoperation	—	✓	✓	✓	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces	—	✓	✓	✓	✓	✓	✓	✓	✓
Private VLANs	✓	—	✓	—	✓	✓	✓	✓	✓
Multi-stage load balancing	—	—	—	—	—	—	—	✓	✓
Priority-based flow control	—	—	—	—	—	—	✓	✓	✓
Storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per-port storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	✓	—	✓	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Percentage rate control	✓	—	✓	—	✓	✓	✓	✓	✓
VLAN stacking (QinQ)	—	—	✓	—	✓	✓	✓	✓	✓
VLAN mapping	—	—	✓	—	✓	✓	✓	✓	✓
SPAN	✓	✓	✓	✓	✓	✓	✓	✓	✓
RSPAN and ERSPAN	—	RSPAN	✓	—	✓	✓	✓	✓	✓
Layer 3									
Static routing (v4 v6)	✓	—	✓	—	✓	✓	✓	✓	✓
Hardware routing offload (v4 v6)	✓	—	✓	—	✓	✓	✓	✓	✓
Software routing only	✓	✓	—	✓	—	—	—	—	—
OSPF (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
RIP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
VRRP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
BGP (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
IS-IS (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
PIM (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
Hardware-based ECMP	—	—	—	—	—	—	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Static BFD	—	—	✓	✓	✓	✓	✓	✓	✓
uRPF	—	—	—	—	—	—	✓	✓	✓
DHCP relay feature	✓	—	✓	✓	✓	✓	✓	✓	✓
DHCP server	—	—	—	—	✓	4xx only	✓	✓	✓
High Availability									
MCLAG (multichassis link aggregation)	Partial	—	—	—	✓	✓	✓	✓	✓
STP supported in MCLAGs	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping support in MCLAG	✓	—	—	—	✓	✓	✓	✓	✓
Quality of Service									
802.1p support, including priority queuing trunk and WRED	✓	—	✓	—	✓	✓	✓	✓	✓
QoS queue counters	—	—	✓	—	✓	✓	✓	✓	✓
QoS marking	—	—	✓	—	✓	✓	✓	✓	✓
Summary of configured queue mappings	✓	—	✓	✓	✓	✓	✓	✓	✓
Egress priority tagging	—	—	✓	—	✓	✓	✓	✓	✓
Miscellaneous									
PoE-pre-standard detection (See Note 1.)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
PoE modes support: first come, first served or priority based (PoE models)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—
Control of temperature alerts	—	✓	✓	—	✓	✓	✓	✓	✓
Split port (See Note 6.)	Partial	—	—	—	—	—	✓	1048E	✓
TDR (time-domain reflectometer)/cable diagnostics support	✓	—	✓	—	✓	✓	✓	—	—
Auto module max speed detection and notification	✓	—	—	—	—	—	✓	✓	—
Monitor system temperature (threshold configuration and SNMP trap support)	—	✓	✓	—	✓	✓	✓	✓	✓
Cut-through switching	—	—	—	—	—	—	—	✓	✓
Add CLI to show the details of port statistics	—	✓	✓	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode	—	—	—	—	—	—	✓	1048D 1048E	✓
Energy-efficient Ethernet	—	✓	✓	✓	✓	✓	✓	—	—
PHY Forward Error Correction (see Note 5)	—	—	—	—	—	—	—	1048E	3032E

Notes

1. PoE features are applicable only to the model numbers with a POE or FPOE suffix.
2. 24-port LAG is applicable to 524D, 524-FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
3. To use the dynamic layer-3 protocols, you must have an advanced features license.
4. The per-VLAN MAC learning limit and per-trunk MAC learning limit are not supported on the 448D/448D-POE/448D-FPOE/248E-POE/248E-FPOE/248D series.
5. Supported only in 100G mode (clause 91).
6. On the 3032E, you can split one port at the full base speed, split one port into four sub-ports of 25 Gbps each (100G QSFP only), or split one port into four sub-ports of 10 Gbps each (40G or 100G QSFP).

Connecting multiple FSW-R-112D-POE switches

The FSW-R-112D-POE switch does not support interconnectivity to other FSW-R-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitch 6.2.2 supports upgrading from FortiSwitch 3.5.0 and later.

Cooperative Security Fabric upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

Product integration and support

FortiSwitch 6.2.2 support

The following table lists 6.2.2 product integration and support information.

Web browser	<ul style="list-style-type: none">• Mozilla Firefox version 52• Google Chrome version 56 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in 6.2.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
542650	After a resetting the PoE on the port or rebooting the phone, the connected PC does not allow traffic to pass until the authentication is cleared.
561745	The FS-248E-FPOE model does not display ports 39-48 on the switch faceplate on the <i>System > Dashboard</i> page.
564912	If DHCP snooping is enabled, the PXE client does not start.
566064	After the flood-unknown-multicast option is enabled and then disabled, unknown multicast traffic is not dropped.
568918	The user cannot authenticate using 802.1x when running 548Ds in FortiLink mode.
571142	It should not be possible to configure both the trust-dot1p-map and qnq options or both the vlan-mapping and dot1p-map options.
571242	Switches go offline randomly.
574563	A loop is created when two WAN ports of a FortiAP are connected to an FS-448-FPOE unit.
576264	The <code>diagnose switch-controller dump trunk-state</code> command is not displaying output on the FortiGate unit.
576578	After upgrading, only two out of four ports provide power over Ethernet (PoE).

Common vulnerabilities and exposures

FortiSwitchOS 6.2.2 is no longer vulnerable to the following CVEs:

- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479
- CVE-2019-17657
- CVE-2007-6750

Visit <https://fortiguard.com/psirt> for more information.

Known issues

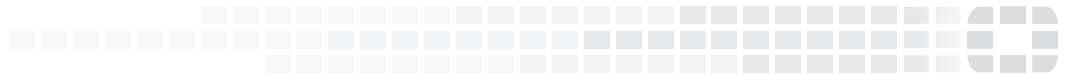
The following known issues have been identified with 6.2.2. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).
480605	<p>When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.</p> <p>Workarounds:</p> <ul style="list-style-type: none">—Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN.—Temporarily disable dhcp-snooping on vlan, issue the <code>execute interface dhcpclient-renew <interface></code> command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	<p>The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values.</p> <p>Workaround: When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag <physical port name></code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>
520954	When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.
542031	For the 5xx switches, the <code>diagnose switch physical-ports led-flash</code> command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.

Bug ID	Description
572052	<p>Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters.</p> <p>Workaround: Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.</p>
580967	<p>Protocol Independent Multicast (PIM) routing does not work on the FSW-3032E switch.</p> <p>Workaround: Enable IGMP snooping on the egress VLANs.</p>
585550	<p>When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.</p>
587071	<p>On the 1048D, 1024D, and 3032D models, using the GUI or REST API to make any change to the OSPF interface (such as changing the BFD mode) might cause the loss of the MD5 keys.</p> <p>Workaround: Use the CLI to configure the MD5 key.</p>
589129, 591704	<p>Using MAB authentication might cause high CPU usage.</p>
629721	<p>HTTP and HTTPS connections from the same client or from the same browser do not work.</p> <p>Workaround: Use HTTP and HTTPS connections from different clients (with a different IP address) or different browsers (for example, Firefox for HTTP and Chrome for HTTPS) or clear the cookies between using HTTP and HTTPS.</p>



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.