



FortiWLC - Release-Notes

Version 8.5.4

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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

May 06, 2021

FortiWLC 8.5.4 Release-Notes

TABLE OF CONTENTS

Change log	4
About FortiWLC 8.5.4	5
What's New	6
Supported Hardware and Software	7
Installing and Upgrading	8
Getting Started with Upgrade	9
Supported Upgrade Releases	9
Check Available Free Space	10
Set up Serial Connection	10
Upgrade Advisories	10
Upgrading Virtual Controllers	11
Upgrading FAP-U422EV	11
Mesh/VPN AP Deployments	11
Feature Groups in Mesh profile	11
Voice Scale Recommendations	11
Upgrading an NPlus1 Site	12
Restore Saved Configuration	12
Upgrading Virtual Controllers	12
Upgrading FortiWLC-1000D and FortiWLC-3000D	13
Upgrading via CLI	13
Upgrading via GUI	14
Switching Partitions	15
Fixed Issues	16
Known Issues	19
Common Vulnerabilities and Exposures	20

Change log

Date	Change description
2021-05-06	FortiWLC version 8.5.4 release document.

About FortiWLC 8.5.4

FortiWLC release 8.5.4 delivers WPA3-enterprise security support and resolved outstanding issues; see sections [What's New on page 6](#) and [Fixed Issues on page 16](#).

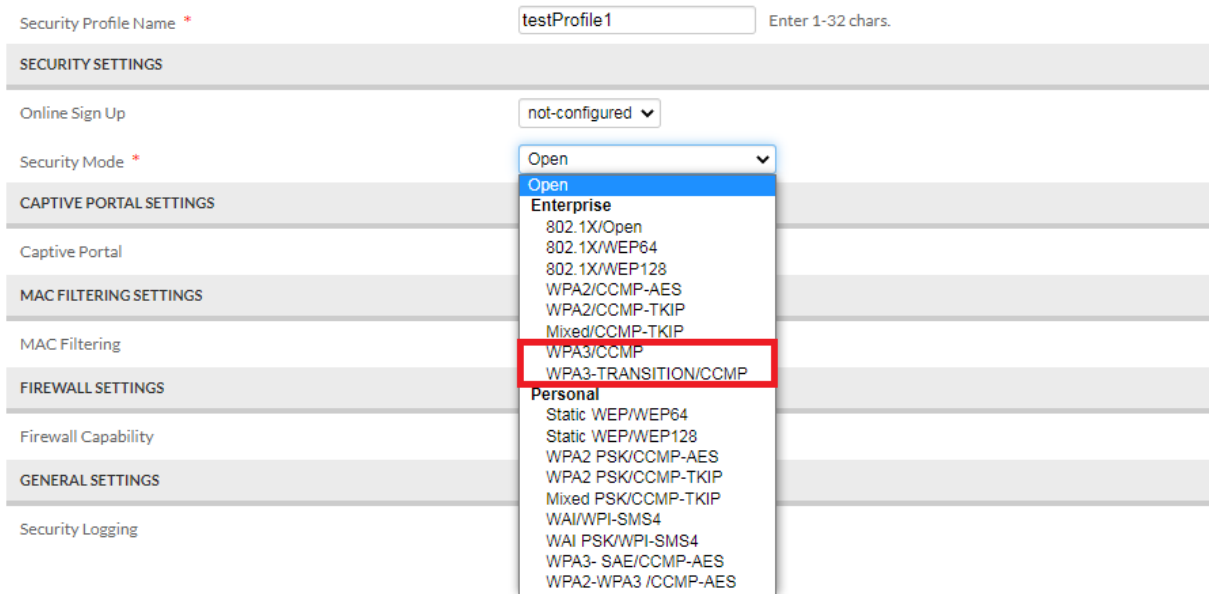
What's New

This release of FortiWLC supports the following L2 WPA3 enterprise security modes.

- WPA3/CCMP
- WPA3-Transition/CCMP

Navigate to *Configuration > Security > Profile*.

Security Profiles - Add



Security Profile Name * Enter 1-32 chars.

SECURITY SETTINGS

Online Sign Up

Security Mode *

CAPTIVE PORTAL SETTINGS

Captive Portal

MAC FILTERING SETTINGS

MAC Filtering

FIREWALL SETTINGS

Firewall Capability

GENERAL SETTINGS

Security Logging

Enterprise

- 802.1X/Open
- 802.1X/WEP64
- 802.1X/WEP128
- WPA2/CCMP-AES
- WPA2/CCMP-TKIP
- Mixed/CCMP-TKIP
- WPA3/CCMP**
- WPA3-TRANSITION/CCMP**

Personal

- Static WEP/WEP64
- Static WEP/WEP128
- WPA2 PSK/CCMP-AES
- WPA2 PSK/CCMP-TKIP
- Mixed PSK/CCMP-TKIP
- WAI/WPI-SMS4
- WAI PSK/WPI-SMS4
- WPA3- SAE/CCMP-AES
- WPA2-WPA3 /CCMP-AES

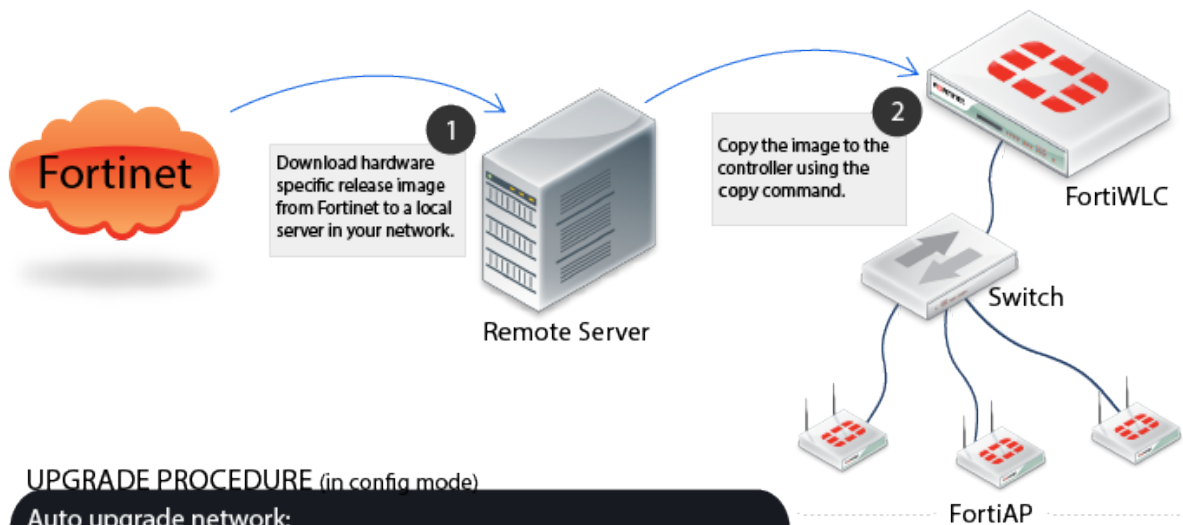
Supported Hardware and Software

This table lists the supported hardware and software versions in this release of FortiWLC.

Hardware and Software	Supported	
Access Points	AP122	FAP-U431F
	AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e	FAP-U433F
	FAP-U421EV	PSM3x
	FAP-U423EV	AP1010e*
	FAP-U321EV	AP1010i*
	FAP-U323EV	AP1020e*
	FAP-U422EV	AP1020i*
	FAP-U221EV	
	FAP-U223EV	
	FAP-U24JEV	
*Cannot be configured as a relay AP		
Controllers	FortiWLC-50D	MC3200
	FortiWLC-200D	MC1550
	FortiWLC-500D	MC4200 (with or without 10G Module)
	FortiWLC-1000D	
	FortiWLC-3000D	
	FWC-VM-50	
	FWC-VM-200	
	FWC-VM-500	
	FWC-VM-1000	
FWC-VM-3000		
FortiWLM	8.6.0, 8.6.1	
FortiConnect	16.9, 17.0	
Browsers		
FortiWLC (SD) WebUI	Internet Explorer 11	
	Mozilla Firefox 69	
	Google Chrome 77	
Note: A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs.		

Installing and Upgrading

Follow this procedure to upgrade FortiWLC-50D, FortiWLC-200D, FortiWLC-500D, MC1550, MC3200, and MC4200 controllers. See section to upgrade FortiWLC-1000D and FortiWLC-3000D. See [Upgrading Virtual Controllers](#) on page 12 to upgrade virtual controllers.



UPGRADE PROCEDURE (in config mode)

Auto upgrade network:

To upgrade controllers and APs

```
#upgrade system <target-version>
```

Phase upgrade:

To upgrade controllers first and then all APs

```
#auto-ap-upgrade disable
```

```
#upgrade controller <target-version>
```

```
#upgrade ap same all OR upgrade ap same <ap-ID>
```

Step upgrade:

To upgrade controllers and then auto upgrade all APs

```
#auto-ap-upgrade enable
```

```
#upgrade controller <target-version>
```

Patch upgrade:

To upgrade controllers to a patch release

```
#patch install <target-patch/version>
```

1. Download image files from the remote server to the controller using one of the following commands:
copy ftp://ftpuser:<password@ext-ip-addr>/<image-name-rpm.tar.fwlc><space>.
 [OR]
copy tftp://<ext-ip-addr>/<image-name-rpm.tar.fwlc><space>
 Where, **image-name** for FortiWLC: forti-{release-version}-{hardware-model}-rpm.tar.fwlc For example, forti-8.5-2-FWC2HD-rpm.tar.fwlc
2. Disable AP auto upgrade and then upgrade the controller (in config mode)
auto-ap-upgrade disable
copy running-config startup-config
upgrade controller <target version> (Example, upgrade controller 8.3)

The **show flash** command displays the version details.

3. Upgrade the APs
 - # **upgrade ap same all**

After the APs are up, use the **show controller** and **show ap** command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is available in the controller using the **show running -config** command (if not, recover from the remote location). See the Backup Running Configuration step.

Getting Started with Upgrade

The following table describes the approved upgrade path applicable for all controllers except the new virtual controllers.

NOTE:

In pre-8.4.3 releases, if the MAC-delimiter is set to hyphen in the RADIUS profile for 802.1x authentication, the controller sends the **called station id** with MAC-delimiter as colon.

When you upgrade to the current release from pre-8.4.3 release, if there is a RADIUS reject for the MAC-delimiter, then reconfigure the RADIUS server.

Supported Upgrade Releases

This section describes the upgrade path for this release.

From FortiWLC release...	To FortiWLC Release...
8.4.7, 8.4.8, 8.5.2, and 8.5.3	8.5.4

NOTES:

- Fortinet recommends that while upgrading 32-bit controllers, use the **upgrade controller** command instead of the **upgrade system** command.
- Controller upgrade performed via CLI interface will require a serial or SSH2 connection to connect to the controller and use its CLI.
- FortiWLC-1000D and FortiWLC-3000D and 64-bit virtual controller upgrades can be performed via GUI as well.
- Upgrade the FortiWLC-1000D and 3000D controllers with manufacturing version prior to 8.3-0GAbuild-93 to version 8.3-0GAbuild-93 and then to the later builds.

Check Available Free Space

Total free space required is the size of the image + 50MB (approximately 230 MB). You can use the **show file systems** command to verify the current disk usage.

```
controller# show file systems

Filesystem 1K-blocks Used Available Use% Mounted on
/dev/hdc2 428972 227844 178242 57% /none 4880 56 4824 2% /dev/shm
```

The first partition in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **delete flash:<flash>** command to free up space by deleting older flash files until there is enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the current running version).

Set up Serial Connection

Set the serial connection for the following options:

NOTE:

Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits
- Parity--None
- Stop Bit—1
- Flow Control—None

Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

NOTES:

- [32-bit controllers] Prior to upgrading to FortiWLC, delete any old image files to avoid issues related to space constraints.
- Upgrade Controller using wired client/laptop and **NOT** using wireless client/laptop.
- [Patch installation] When both AP and controller patches are to be applied; the controller patch must be installed prior to the AP patch.

Upgrading Virtual Controllers

In the upgrade-image command, select the options **Apps** or **Both** based on these requirements:

- **Apps**: This option will only upgrade the Fortinet binaries (rpm).
- **Both**: This option will upgrade Fortinet binaries as well as kernel (iso).

Upgrading FAP-U422EV

If the controller is running on pre-8.4.0 version and FAP-U422EV is deployed, follow these points:

- Disable **auto -ap -upgrade**
OR
- It is advised not to plug in FAP-U422EV till the controller gets upgraded.

Mesh/VPN AP Deployments

[32-bit controllers] When attempting to upgrade a VPN/mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller. Run the **upgrade system** command.

Feature Groups in Mesh profile

If APs that are part of a mesh profile are to be added to feature group, all APs of that mesh profile should be added to the same feature group. The Override Group Settings option in the **Wireless Interface** section in the **Configuration > Wireless > Radio** page must be enabled on the gateway AP.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, navigate to **Configuration > Devices > System Settings > Scale Settings** tab.
2. Enter a channel number in the **Voice Scale Channel** List field and click **OK**.

NOTE:

Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and this result in a noticeable reduction of throughput in data traffic.

Upgrading an NPlus1 Site

To upgrade a site running NPlus1, all controllers must be on the same FortiWLC-SD version and the backup controller must be in the same subnet as the primary controllers.

You can choose any of the following options to upgrade:

Option 1 - Just like you would upgrade any controller, you can upgrade an NPlus1 controller.

1. Upgrade master and then upgrade slave.
2. After the upgrade, run the **nplus1 enable** command to enable master on slave controller.

Option 2 - Upgrade slave and then upgrade master controller.

After the upgrade, run the **nplus1 enable** command to enable master service on the slave controller.

Option 3 - If there are multiple master controllers

1. Upgrade all master controllers followed by slave controllers. After the upgrade, run the **nplus1 enable** command to enable all master controllers on slave controllers .

2. Run the the **nplus1 enable** command to enable master controller on slave controller.

3. Connect to all controllers using SSH or a serial cable.

4. Run the **show nplus1** command to verify if the slave and master controllers are in the cluster.

The output should display the following information:

```
Admin: Enable
```

```
Switch: Yes
```

```
Reason: -
```

```
SW Version: 8.3-1
```

5. If the configuration does not display the above settings, run the **nplus1 enable <master-controller-ip>** command to complete the configuration.

6. Run the **nplus1 add master** command to add any missing master controller to the cluster.

Restore Saved Configuration

After upgrading, restore the saved configuration.

1. Copy the backup configuration back to the controller:

```
# copy ftp://<user>:<passwd>@<offbox-ip-address>/runningconfig.txt orig-config.txt
```

2. Copy the saved configuration file to the running configuration file:

```
# copy orig-config.txt running-config
```

3. Save the running configuration to the start-up configuration:

```
# copy running-config startup-config
```

Upgrading Virtual Controllers

Virtual controllers can be upgraded the same way as the hardware controllers. See sections [Upgrading via CLI](#) on page 13, [Upgrading via GUI](#) on page 14, and [Upgrading an NPlus1 Site](#) on page 12.

Download the appropriate virtual controller image from Fortinet Customer Support website.

For more information on managing the virtual controllers, see the *Virtual Wireless Controller Deployment Guide*.

Upgrading the controller can be done in the following ways:

- Using the FTP, TFTP, SCP, and SFTP protocols.
- Navigate to **Maintenance < File Management** in the FortiWLC GUI to import the downloaded package.

The following are sample commands for upgrading the virtual controllers using any of these protocols.

- **upgrade-image tftp://10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar.fwlc both reboot**
- **upgrade-image sftp://build@10.xx.xxx.xxx:/home/forti-x.x-xGAbuild-88-FWC1KD-rpm.tar.fwlc both reboot**
- **upgrade-image scp://build@10.xx.xxx.xxx:/home /forti-x.x-xGAbuild-88-FWC1KD-rpm.tar.fwlc both reboot**
- **upgrade-image ftp://anonymous@10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar.fwlc both reboot**

The **both** option upgrades the Fortinet binaries (rpm) as well as the Kernel (iso), the **apps** option upgrades only the Fortinet binaries (rpm).

After upgrade, the virtual controller should maintain the System-id of the system, unless there were some changes in the fields that are used to generate the system-id.

The international virtual controller can be installed, configured, licensed and upgraded the same way.

Upgrading FortiWLC-1000D and FortiWLC-3000D

To upgrade to FortiWLC-1000D and FortiWLC-3000D, use the following instructions.

In version 8.4.0, the image naming systems have been changed for 64 bit controller models from Primary/Secondary to image0/image1. This change applies to the upgrade procedure in the related FortiWLC GUI screens and CLI commands.

Upgrading via CLI

1. Use the **show images** command to view the available images in the controller. By default, a new controller will boot from the primary partition which contains the running image.

```
Master-3000D(15)# show images
Running image : image0
On reboot : image0
```

```
-----
-----
Running image details.
System version: 0.3.14
System memory: 231M/463M
Apps version: 8.5-2build-4
Apps size: 251M/850M
-----
```

```
-----  
Other image details.  
System version: 0.3.14  
System memory: 240M/473M  
Apps version: 8.5-1build-7  
Apps size: 177M/849M
```

2. To install the latest release, download the release image using the **upgrade-image** command.
upgrade-image scp://<username>@<remote-server-ip>:<path-to-image>/<image-name>-rpm.tar.fwlc both

reboot

The above command will upgrade the secondary partition and the controller will reboot to secondary partition.

NOTE:

After an upgrade the current partition will shift to the second partition. For example, if you started upgrade in primary partition, post upgrade the default partition becomes secondary partition and vice-versa.

Upgrading via GUI

This section describes the upgrade procedure through the FortiWLC GUI.

NOTES:

- Fortinet recommends upgrading via CLI to avoid this issue which occurs due to file size limitation.
 - This issue does not exist on controllers with manufacturing build as 8.3.3 GA and above.
1. To upgrade controllers using GUI, navigate to **Maintenance > File Management > SD Version**.
 2. Click **Import** to choose the image file.

Software Image Library and Logs ?

AP Init Script	Diagnostics	SD versions	Patches	Syslog
<div style="display: flex; gap: 10px;"> ↻ REFRESH 📁 IMPORT </div>				
Running image	image0			
On reboot	image0			
Running Image Details :				
System version	0.6.5			
System memory	143M/463M			
Apps version	8.5-4reldev-10			
Apps size	188M/850M			
Other Image Details :				
System version	0.6.5			
System memory	199M/473M			
Apps version	8.5-4reldev-8			
Apps size	183M/849M			

- After the import is complete, a pop message for upgrade confirmation is displayed.

Click **OK** to upgrade; the controller reboots. Click **Cancel** to abort the upgrade and continue in the existing version.

Switching Partitions

To switch partitions in FortiWLC-1000D, FortiWLC-3000D and the new virtual controllers, select the partition during the boot up process.

Fixed Issues

These are the fixed issues in this release of FortiWLC. Controller issues listed in this section are applicable on all models unless specified; AP issues are applicable to specific models.

AP Reboot/Stability

Tracking ID	Description
590627	[FAP-U22xEV/FAP-U24JEV] Random AP reboot.
652724	[FAP-U32xEV/FAP-U42xEV] Random AP reboot.
670488	[FAP-U43xF] AP reboot when DTLS was enabled.
674607	[AP122] AP stops forwarding data on the second LAN Interface.
680968	[AP822] Random AP reboot after upgrade.
691857	VPN APs unable to discover the controller after controller replacement.
705366	[FAP-U43xF] Low download speed with bridged SSID.

Captive Portal

Tracking ID	Description
674931	Captive portal redirect issue on IE due to an additional slash in the URL.
696206	Unable to obtain the captive portal login page with Forti Authenticator.

Configuration – Controller/AP

Tracking ID	Description
681595	Unable to save configuration to startup on the GUI using Privilege level 10 user account.
687742	Configuration changes not reflected on random APs until rebooted.
688642	Pre-upgrade configuration not saved that lead to lost LACP configuration FAP-Us.
712863	Disabling PMK caching in security profile did not take effect.

Controller Processes/Sluggishness

Tracking ID	Description
544542	Ping OUI restarts when client locator was enabled/disabled with the client already connected.
670394/678123/679033	Random securityMM crash observed.
671710	Service control unavailable on Radius-VLAN-Only configured SSIDs.
688283	[FortiWLC-500D] Low file partition size.
702014	IGMP snooping daemon crashed after upgrading.
707004	Ping OUI process failed to start.

GUI/CLI

Tracking ID	Description
633492	The station-log show command did not work after upgrade.
658488	Unable to configure WPA3-enterprise in both GUI and CLI modes.
670270	Sometimes, the GUI prompts for login credentials in Chrome when navigating to other pages.
671932	The show interface Dot11Radio statistics command output displays unformatted lists.
687421	The diagnostics-controller command does not provide complete output.
697998	FortiWLC Dashboard Monitor statistics values are not refreshed.
698700	Running/Startup configuration export failed in the GUI using Google Chrome.

Intermittent Connectivity

Tracking ID	Description
665284	[Spectralink] The controller crashed as the phones register to two different SIP servers.
668907	iOS devices unable to connect with the 802.11r enabled ESSID.
673963	[AP110] Wired clients not assigned an IP address.
693613	Random controller reboot.
699890	Random controller reboot.

Logs

Tracking ID	Description
675136	Station activity logs are inserted at wrong timestamp.

NPlus1

Tracking ID	Description
710237	Unable to add master controller to the slave.

Others

Tracking ID	Description
685454	Cisco switch learned the client MAC address in tunneled SSID.
691534	[FAP-U22xEV] Poor performance during downstream traffic in both tunnel and bridge modes.
695737	Configuration synchronization after AP bootup removed init script radio settings.
700985	MC4200-VE controller locked up with no SSH/GUI access.
702509	SNMP trap not sent to all of the configured trap receiver addresses.

Known Issues

These are the known issues in this release of FortiWLC. Controller issues listed in this section are applicable on all models unless specified; AP issues are applicable to specific models.

Tracking ID	Description	Impact	Workaround
671626	SNMP walk returns No Such Object available on this agent at this OID error.		

Common Vulnerabilities and Exposures

This release of FortiWLC is no longer vulnerable to the following:

Vulnerability	Description
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-121	Stack-based Buffer Overflow
CWE-284	Improper Access Control
CWE-657	Violation of Secure Design Principles
CWE-824	Access of Uninitialized Pointer

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



Copyright© 2021 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.