



FortiNAC - Release Notes

Version 8.8.0

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/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



June 10, 2020

FortiNAC 8.8.0.1704 Release Notes

49-880-641429-20200610

TABLE OF CONTENTS

Overview of Version 8.8.0	4
Important	4
Supplemental Documentation	4
Version Information	4
Compatibility	6
Agents	6
Web Browsers for the Administration UI	6
Operating Systems Supported Without an Agent	7
New Features in 8.8.0	8
Enhancements and Addressed Issues	9
Version 8.8.0	9
Device Support	15
Version 8.8.0	15
System Update Settings	17
End of Support/End of Life	18
End of Support	18
Agent	18
Software	18
Hardware	18
Appliance Operating System	18
End of Life	19
Software	19
Numbering Conventions	20

Overview of Version 8.8.0

Version 8.8 is the latest release being made available to customers to provide functionality and address some known issues.

Important

- Requires access to downloads.bradfordnetworks.com from each appliance or virtual machine. The update automatically installs CentOS files for the new Local Radius Server feature on the Control Server(s). If access is blocked, the software upgrade will fail. The default transfer protocol can be changed from FTP to either HTTPS or HTTP. For instructions, refer to the Appendix of the CentOS Updates (<https://docs.fortinet.com/document/fortinac/8.3.0/updating-centos>) reference manual.
- Prior to upgrade, review the FortiNAC Known Anomalies posted in the [Fortinet Document Library](#).
- If using agents or configured for High Availability, additional steps may be required after upgrade for proper functionality. See [Upgrade Instructions and Considerations](#) posted in the Fortinet Document Library.
- Requires CentOS 7.4 or higher. The current CentOS version installed is listed as "Distribution" in the CLI login banner or typing "sysinfo".

Example:

```
> sysinfo
*****
Recognized platform: Linux
Distribution: CentOS Linux release 7.6.1810 (Core)
If the CentOS version is below 7.4, run OS updates and reboot before upgrading. For instructions on updating CentOS, refer to the Fortinet Document Library.
```

- For upgrade procedure, see [Upgrade Instructions and Considerations](#) posted in the Fortinet Document Library.

Supplemental Documentation

The following can be found in the [Fortinet Document Library](#).

- 8.x Fixes and Enhancements Summary
- FortiNAC Release Matrix

Version Information

These Release Notes contain additional Enhancements, Device Support, and features. Unique numbering is used for the various components of the product. The software version and Agent version supplied with this release are listed below.

Version: 8.8.0.1704

Agent Version: 5.2.3

A newer Persistent Agent may be required to support certain antivirus and anti-spyware products. Refer to the Agent Release Notes in the [Fortinet Document Library](#).

Firmware version represents a collection of system services and operating system features imaged on to the appliance before it leaves manufacturing. The firmware image cannot be updated by a Fortinet customer. Services within the image are updated by Fortinet or a certified Fortinet Partner in appliance maintenance packages released as new more robust and secure versions of services become available.

Note that upgrading software versions does not change firmware nor does it automatically require an upgrade to the Persistent Agent. Newer Persistent Agents are not compatible with older software versions unless that capability is specifically highlighted in the corresponding release notes.

Compatibility

FortiNAC Product releases are not backwards compatible. It is not possible to go from a newer release to any older release.

Example: 8.1.1.132 cannot be downgraded to any other release.

To backup the current system prior to upgrade on virtual machines, perform a snapshot. For physical appliances refer to the document Back Up and Restore an Image of a FortiNAC Appliance.

Agents

FortiNAC Agent Package releases 5.x are compatible with FortiNAC Product release 8.x. Compatibility of Agent Package versions 4.x and below with FortiNAC versions 8.x and greater are not guaranteed.

Web Browsers for the Administration UI

Safari web browser version 6 or greater

Google Chrome version 26 or greater

Mozilla Firefox version 20 or greater

Internet Explorer version 9.0 or greater

Opera version 12.15 or greater

Many of the views in FortiNAC are highly dependent on JavaScript. The browser used directly impacts the performance of these views. For example, the new Host view in one browser may take 2 seconds to load, but the same view in a different browser may take 20 seconds. To improve performance, it is recommended that you choose a browser which is fast at processing JavaScript, such as, Google Chrome. Articles on comparing the performance of various web browsers are freely available on the internet. Some performance sites include:

- <http://legitreviews.com/article/1347/1/>
- <http://w-shadow.com/blog/2010/04/20/web-browser-performance-comparison/>
- <http://sixrevisions.com/infographs/browser-performance/>
- <http://w-shadow.com/blog/2010/11/03/browser-performance-comparison/>

If your browser is not optimized for processing JavaScript, you may see an error message display when accessing a view that uses JavaScript. The message will vary depending on your browser.

Example:

Warning: Unresponsive script

A script on this page may be busy, or it may have stopped responding. You can stop the script now or you can continue to see if the script will complete.

Script: http://<IP>/js/yui/yahoo-dom-event/yahoo-dom-event.js:8"

Operating Systems Supported Without an Agent

Android	Apple iOS	Blackberry OS	BlackBerry 10 OS
Chrome OS	Free BSD	Kindle	Kindle Fire
iOS for iPad	iOS for iPhone	iOS for iPod	Linux
Mac OS X	Open BSD	Net BSD	RIM Tablet OS
Solaris	Symian	Web OS	Windows
Windows CE	Windows Phone	Windows RT	

New Features in 8.8.0

- FortiGuard IoT Service for Device Profiling
- Script based Device Profiling method. See section [Adding a Rule in the Administration Guide](#) for details.
- Support for Jamf MDM for Apple devices including application information polling
For details on Jamf integration, refer to the Fortinet Document Library.
- Built-in local RADIUS server which can process RADIUS MAC and 802.1x EAP authentication. This is separate and in addition to the existing RADIUS server functionality which provides RADIUS MAC authentication and proxies 802.1x EAP authentication to an external RADIUS server.
- Support for Mist Wireless. For details, refer to the Mist Wireless Integration reference manual in the Fortinet Document Library.

Enhancements and Addressed Issues

These changes have been made in FortiNAC Version 8.8.0. These enhancements are in addition to the enhancements that are outlined in 8.7 and previous releases.

Version 8.8.0

Ticket #	Description (8.8.0)
631164	Fortiguard IoT service
581244	Support for Jamf MDM for Apple devices including application information polling.
585369	Added RADIUS authentication support for HP J9729A and HP J8697A
599182	Added column for matching device profiling rule to the Adapter View
636385	Fixed Supplicant EasyConnect for Windows, macOS. It could not successfully create profiles or connect to the desired SSID.
625690	Fixed "Login" box being grey'd out on the Guest Self Registration page. This prevented user from being able to register after sponsor approval.
629260	Fixed communication issues between the NCM and pods
635285	Fixed issued where JAVA used 100% CPU and high memory
628958	Device Profile rule for Fortigate returned false positive matches
633909	Updated "bscftp" alias to connect to the correct location.
611585	Fixed issue with USB external adapter/dongle sharing between hosts. Agent technology can now be configured to remove adapters from the host record when the agent no longer detects the adapter connected. Note: This function is disabled by default and cannot be enabled through the Administration UI. Contact Support for assistance.
633541	Fixed Adapter Panel > Show Fortigate Sessions not filtering to the selected adapter
631627	Fixed adding or modifying the Firewall Tag using the direct configuration. Previously, this would result in "HTTP 404 Not Found" error.
631249	Fixed incorrect modification of property file by .masterPropertyFile.
612340	Added new Device Profiling method called "FortiGuard" which pulls IoT device information from FortiGuard based on the MAC address. Also added new Device Profiler settings to configure FortiGuard IoT service if desired.
633364	Fixed Device Profiler DHCP method where attempting to match hostnames with 'D*' was matching with letter contained in any position.

Ticket #	Description (8.8.0)
629949	Fixed potential database corruption when using Device Profiling Rules after upgrade from 8.6 to 8.7
632387	Fixed NMAP Scan Results Shows Wrong IP Address
632457	Fixed Run Nmap scan dialog title does not update with the current IP
631629	Fixed Hosts > Scan Results view not displaying any information regardless of the filter used.
631135	Maximum Concurrent License Count incorrectly displayed a number greater than the licensed count (typically 4 more). This has been fixed.
554910	Added the ability to read VLAN-Pool from Meru WLC
625316	Added Access Point Management service to REST API. The service covers the System > Settings > Control > AccessPointManagement view.
620438	Added Quarantine service to REST API. The service covers the System > Settings > Control > Quarantine view.
630825	Fixed Adapter View not showing IP address of the host. This was affecting the ability to Device Profile rogue hosts.
601846	Disappearing SSID Tab
629263	Fixed potential NullPointerException error when "FortiGate" Method was used in Device Profiling Rule. This issue could cause the rule match to fail.
624144	FSSO Tag is added/removed constantly which toggles the applied firewall policy
624227	Added ability to make certain POST API calls to the NCM
627666	Included FortiNAC Agent 5.2.3 in FortiNAC installer
617431	Enhancements made to Nozomi integration
611216	Changed how vlans are read/write on Juniper Ex 3400 switches
611593	FortiGate modeling error with eight linked FortiSwitches
612336	Fixed issue where Host IP address information was not updated correctly after completing registration. This affects wireless hosts connecting to the FortiWiFi and FortiAP.
619347	Added the ability for FortiNAC to be configured to respond to traffic using the same interface it was received (policy based routing). Required for VPN integrations and static IP environments. This function is disabled by default and requires configuration via CLI. Refer to the applicable VPN integration guide or contact Support for assistance.
621277	"User does not have permission for this operation" error when attempting to Set Expiration on multiple users.
627343	Added Criticality column in SharedFilterReport
614344	Syslog parse error and null pointer exception with FGT Syslog connection updates
608823	Added the ability to profile devices with a custom command line script.

Ticket #	Description (8.8.0)
612467	Added "Criticality" Column to the host, user and network device view. Used to set criticality level information to send to FortiAnalyzer for reporting purposes.
618248	Added RADIUS Authentication support for Aruba JL256A and HP J9727A
614069	Unable to read VLANs on Cisco 9000 IOS-XE
614172	Support for Arista "switchport access" and "switchport trunk" modes
614171	Arista.mib login sequence
598661	SNMP bsnMobileStationDeleteAction Client Disconnect Not Supported on WLC C9800
612433	FortiGate Add/Move/Delete Syslog messages are not processed
608224	grab-log-snapshot sometimes doesn't gather the correct master_loader logs
609372	High cpu/load averages on control server
603302	Added SNMP option for reading VLANs for Extreme devices. Enabling this option can improve VLAN read times on switches that support dot1qPvid.
626009	Set Model Configuration view non-functional
592597	FortiNAC cannot L3 poll Fortigate FortiGate-201E v6.0.5, build0268, 190507 (GA)
609641	Added "Rogue Evaluation Queue Size: NNN", "Details" button and "Flush" button to the Device Profiling Rules view to provide better visibility and control over the rogue evaluation queue.
614351	Fixed potential database corruption issue when using Device Profiling Rules with custom DHCP fingerprints.
611982	Meraki SSIDs are removed when they are set to disabled on the AP
615921	Security Fabric > REST API request to /api/v2/host/disable-by-mac returns HTTP status 403 (Forbidden)
609346	Bulk Device support via email mappings
617120	FortiNAC periodically does not gzip backup files on the Secondary HA Server.
618977	OutOfMemoryError caused by unpacking a fragmented NSTD_MSG_SYNC_GLOBAL_VIEW_REP packet
624908	Config Wizard not displaying UUID and eth0 MAC address
620852	DHCP Fingerprint additions and updates
614497	PODs are not synchronizing in NCM GUI
520795	Location Based Policy Not Matching Due to SSID Name Containing ":"
607069	Fixed NCM Endpoint Compliance Policy Syncing issues
608451	Fixed alarms failing to trigger over time when any alarm was configured with an event frequency of "0" events occurring within X hours.
623776	Under System Updates, if the SFTP protocol is selected, an error dialog will display when

Ticket #	Description (8.8.0)
	attempting to save or test with any names where SFTP access is no longer supported to download code. Other names or IP addresses can still be configured to use SFTP.
605485	Additional clean ups and expansions to the REST API
612106	DHCP fingerprinting on ETH1 interface is not working
606514 608202	Fixed connection issue between Control Manager and managed FortiNAC servers. Previously, this condition could cause the following behavior: - Management processes on the Control Manager to report "down" - Managed FortiNAC servers to stop processing RADIUS authentication packets
625759	Device Profiler errors on Active scan
586523	Fixed DNS behavior when system fails over in L3 High Availability configurations. Previously, the Secondary Server (in control) was replying to DNS inquiries with the Primary Server ETH1 IP address. This caused DNS resolution to fail for isolated hosts.
609013	FortiNAC is sending an incorrect serial number to FortiGate via CSF
618003	FortiNAC is replying with the wrong path to FortiGate via CSF
611540	Fixed Apply to Group drop down menu under SSO Agent options in the FortiGate model Elements tab. Previously, this menu was grayed out when the "Apply to Group" check box was selected.
617063	Uncompressed database backup replication to secondary causing 100% Disk usage
607953	Fixed DeviceImport tool throwing "Unable to parse line" exception when a blank line is encountered in the CSV.
608211	Admin Profile Manage Hosts and Ports setting not being saved
615996	Attempting to disable a host by IP Address using the REST API fails if the host is offline.
619028	API calls that result in a 4XX error returning a status message of "Success"
622104	Added Mac Address Exclusion Service to REST API
622034	Fixed files in /var/named/chroot/etc not replicating to the secondary properly
606802	PA Communication State flag reliability improvements
612701	Unable to access REST API URL /api/server with an Administrator user (ie root).
606532	Cannot export XML for Device Profiling rules
573085	Update REST API to run globally from the NCM vs. each pod
608203	Added Lockout Threshold and Duration for Admin user login for failed login attempts to the Administration UI.
608199	Device Profile Rules of type ONVIF throw status of 500 (Internal Server Error) on export to XML
612743	Changed default inactivity time in the Administration UI to 5 minutes
608520	Renamed "FortiGate Telemetry" to "Security Fabric Connection" in Settings view

Ticket #	Description (8.8.0)
609297	FortiNAC takes a long time to recognize when a FortiGate connection has closed
608551	Fixed Log Receiver Syslog Facility not displaying in the Settings view.
607526	AutoCompleteManager exceptions in catalina.out
608824	Added new methods to retrieve a HostRecord from an IP or MAC Address.
608458	Add Logical Network dialog - enter key closes view but does not create entry
604996	Fixed a bug which prevented setting the port in the WinRM method configuration of Device Profiling Rules.
603333	Fixed HPE OfficeConnect 1950-48G VLAN change method.
5933780	FortiNAC now deletes the groups when the conference is either deleted automatically or when an admin deletes it.
601597	Fixed NullPointerException in tomcat-admin catalina.out when accessing Logs > Connections
605778	Fixed issue where Settings > Credential Configuration > Persistent Agent > RADIUS/LDAP used Local instead of LDAP. Previously, the Persistent Agent did not register hosts when this option was selected.
605036	Added Security Actions to System > Groups > In Use
601560	Changed the field Serial Number if FortiAnalyzer is selected as a type in Log Receivers.
605952	Fixed remove group methods in Role, RoleMapping and Profile
589236	Fixed sync issues with pods due to duplicate groups
606993	Fixed distribute of updates from NCM to pods. Previously, attempting to use the Distribute button in the NCM Administration UI would fail with a 500 error code.
607248	Fixed issue with VLAN reads and VLAN switching for Aruba SSeries DLink and HP WX Wireless
582519	Cisco C2600 routers with 16 port Ethernet card not reading VLANs or Updating MAC address information
579289	Cisco 2901 routers with 8 ethernet port cards do not update connection information after L2 poll
638344	Fixed firewall session polling. Previously, it was generating a null pointer exception in the master logs.
637327	Removed check for FortiAnalyzer serial number
637280	Added code to fix Device Profiling Rule rankings if corrupted
631121	Add Wired RADIUS integration with Aruba/HP 2900 series
612477	Changed the default value for "Collect Application Inventory" to false for new Endpoint Compliance Configurations.
635431	NCM Host view doesn't load properly for a pod in High Availability that has failed over.
606177	JAVA use 100% CPU and high memory
635285	

Ticket #	Description (8.8.0)
633491	Fix Error when saving a TLS Service Configuration with "Automatically Update Ciphers And Protocols on Upgrade" set. The modify dialog would not open until after FortiNAC was restarted.
622827	Cisco devices with no defined VLANs fail to read L2 data with SNMP

Device Support

These changes have been made in FortiNAC Version 8.8.0. These are in addition to the device support added in 8.7 and previous releases.

Version 8.8.0

Ticket #	Vendor (8.8.0)
614170	Arista Networks CCS-720XP-48Y6
624552	ArubaOS (MODEL: 515) - 14823.1.2.107
605015	Aruba IAP device
590256	Aruba 8400 Switch
623860	ArubaOS (MODEL: 304), Version 6.5.4.3-6.5.4.3
627031	Catalyst C9407R 9.1.2500 firmware IOS-XE16.9 missing
631140	Modeling Cisco 3750 stack; the model is locked and remains locked - java.lang.NullPointerException
631478	Cisco switches(9.1.2364 and 9.6.1.82.48.2)
630780	Cisco Catalyst L3 Switch (CAT3K_CAA-UNIVERSALK9-M)
627260	Cisco ASA Firepower models 2130,
613010	Cisco Catalyst 9300 (IOS-XE.16.6) unsupported - mapped to wrong MIB
613732	Cisco IE3x00-UNIVERSALK9-M IOS 16.12
613094	Cisco IOS Software, IOS-XE Version 03.11.00.E
616212	Cisco IOS Software [Fuji], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M)
618251	Cisco IOS Software, IE2000 Software (IE2000-UNIVERSALK9-M) - 9.1.1729
618986	Cisco IOS Software (C3560CX-UNIVERSALK9-M) - 9.1.2133
616197	Cisco router C1111-4P
610565	Cisco IOS Version Mapping
634583	Cisco IOS-XE 16.8 support
610682	CiscoIOS-XE.03.11

Ticket #	Vendor (8.8.0)
624554	Cisco SG300-52 52-Port Gigabit Managed Switch
622817	Cisco Adaptive Security Appliance Version 9.12(3)9
618987	Dell S4048T-ON switch
630837	Extreme switch vm386EXOS (1916.2.291)
615527	ExtremeXOS (X440-8t) version 16.2.2.4 - 1916.2.172
631274	Fortigate 61F series
606537	FortiGate 6000F in FortiNAC
634251	FortiGate FWF60EV
615097	Added FortiSwitch missing models to the supported list
623433	Hirschmann (Now Belden) Switches
615555	HPE A5120-24G-POE+ SI Switch Software Version 5.20 - 25506.11.1.15
624558	HPE 5120 24G POE+ (370W) SI Switch - 25506.11.1.253
607718	HPE 5130-48G-PoE+-2SFP+-2XGT
608214	HP 1920G Switch
604560	HP 5900AF-48G-4XG-2QSFP+ Switch
623122	ISW 4-10/100P, 2-10/100T, 2-SFP, PoE Switch - 1916.2.240
616223	Meraki MS125-48LP Cloud Managed PoE Switch - 29671.2.374
615559	Meraki MS125-24P Cloud Managed PoE Switch - 29671.2.372
623858	Meraki Cloud Managed AP
554929	Mist wireless integration
608540	Support for Motorola Wing 5 NX5500Wireless Controller
627368	Checkpoint support for OID 1.3.6.1.4.1.2620.1.6.123.1.69
627369	Checkpoint support for OID 1.3.6.1.4.1.2620.1.6.123.1.37
554907	Ubiquity Unifi Wireless

System Update Settings

Use the following System Update Settings when upgrading through the Administrative UI:

Field	Definition
Host	Set to update.bradfordnetworks.com
Directory or Product Distribution Directory	Systems running version 8.3.x and higher: Set to Version_8_8 Systems running version 8.2.x and lower: Set to Version_8_8_NS
User	Set to updates (in lowercase)
Password	Keep the current value.
Confirm Password	Keep the current value
Protocol	Set to desired protocol (FTP, PFTP, HTTP, HTTPS) Note: SFTP has been deprecated and connections will fail using this option. SFTP will be removed from the drop down menu in a later release.

End of Support/End of Life

Fortinet is committed to providing periodic maintenance releases for the current generally available version of FortiNAC. From time to time, Fortinet may find it necessary to discontinue products and services for a number of reasons, including product line enhancements and upgrades. When a product approaches its end of support (EOS) or end of life (EOL), we are committed to communicating that information to our customers as soon as possible

End of Support

Agent

Versions 2.x and below of the Fortinet Agent will no longer be supported. FortiNAC may allow the agent to communicate but functionality will be disabled in future versions. Please upgrade to either the Safe Harbor or latest release of the Fortinet Agent at your earliest convenience.

Fortinet Mobile Agent for iOS will no longer be supported. It will be completely removed in a future version. EasyConnect features are not affected as they do not require an agent on iOS.

Software

When a code series has been announced End of Support, no further maintenance releases are planned. Customer specific fixes will still be done.

Hardware

Physical appliance hardware reaches end-of-support when the maintenance contract is non-renewed, or at the end of year 4 (48 months beyond purchase date), whichever is first.

Appliance Operating System

Fortinet relies on the CentOS organization to publish periodic bug fixes and security updates for the CentOS Distribution.

CentOS 5

Effective March 31, 2017, CentOS will no longer provide updates for CentOS 5. Any vulnerabilities found with CentOS 5 after March 31st will not be addressed. FortiNAC software releases will continue to be supported on CentOS 5 through December 31, 2018.

As of 2016 Fortinet's appliances are based on the CentOS 7 Linux distribution. New appliance migration options are available for customers with CentOS 5 appliances who require operating system vulnerability patches, maintenance updates and new features available on CentOS 7.

CentOS 7

Effective June 30 2024, CentOS will no longer provide updates for CentOS 7. Any vulnerabilities found with CentOS 7 after June 30th will not be addressed.

FortiNAC and Analytics software releases will continue to be supported on CentOS 7 through December 31 2026 or end of product life (whichever comes first). See Product Life Cycle chart for details. (<https://support.fortinet.com/Information/ProductLifeCycle.aspx>)

End of Life

Software

When a code series has been announced End of Life, no further maintenance releases are planned. In addition, customer specific fixes will not be done. If experiencing problems with a version of FortiNAC in the code series, you would be required to update before any issues can be addressed.

With the release of FortiNAC Version 8.5.0, Fortinet announced the End-Of-Life for FortiNAC 8.1. Existing customers under maintenance are strongly encouraged to upgrade to the current Safe Harbor release.

Considerations are as follows:

- FortiNAC Versions 7.0 and higher are not supported on appliances running firm -ware Version 2.X (SUSE) because of the limitations of this operating system and the hard ware on which it is installed. Please contact your sales representative for hardware upgrade options.
- If you attempt to install FortiNAC Versions 7.0 and higher on an unsupported Operating System and hardware combination, the install process displays the following message: "This release is not supported on 1U SUSE Linux appliances (firmware 2.x). The install process will exit now. Please contact Fortinet at: +1 866.990.3799 or +1 603.228.5300"
- On July 13, 2010 Microsoft ended support for Windows 2000 and Windows 2000 Server. These Operating Systems will be removed from the list of options in the Scan Policy Configuration screens in a future release.

Numbering Conventions

Fortinet is using the following version number format:

<First Number>.<Second Number>.<Third Number>.<Fourth Number>

Example: 8.0.6.15

- First Number = major version
 - Second Number = minor version
 - Third Number = maintenance version
 - Fourth Number = build version
-
- Release Notes pertain to a certain version of the product. Release Notes are revised as needed. The Rev letter increments accordingly. For example, updating the Release Notes from Rev C to Rev D indicates changes in the Release notes only -- no changes were made to the product.
 - The next number represents the version in which a Known Anomaly was added to the release notes (for example, V8.0).



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.