

Release Notes

FortiOS 7.2.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



April 1, 2024

FortiOS 7.2.1 Release Notes

01-721-802670-20240401

TABLE OF CONTENTS

Change Log	5
Introduction and supported models	7
Supported models	7
Special notices	8
IPsec phase 1 interface type cannot be changed after it is configured	8
IP pools and VIPs are not considered local addresses for certain FortiOS versions	8
Support for FortiGates with NP7 processors and hyperscale firewall features	8
Changes in CLI	9
Changes in GUI behavior	11
Changes in default behavior	13
New features or enhancements	15
Upgrade information	27
Fortinet Security Fabric upgrade	27
Downgrading to previous firmware versions	28
Firmware image checksums	29
Strong cryptographic cipher requirements for FortiAP	29
FortiGate VM VDOM licenses	29
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name	29
GUI firmware upgrade does not respect upgrade path	30
Product integration and support	31
Virtualization environments	31
Language support	32
SSL VPN support	33
SSL VPN web mode	33
Resolved issues	34
Anti Virus	34
Application Control	34
Data Leak Prevention	34
DNS Filter	35
Endpoint Control	35
Explicit Proxy	35
Firewall	36
FortiView	37
GUI	37
HA	38
Hyperscale	39
Intrusion Prevention	40
IPsec VPN	40
Log & Report	41

Proxy	41
Routing	43
Security Fabric	44
SSL VPN	45
Switch Controller	47
System	47
Upgrade	50
User & Authentication	50
VM	51
VoIP	51
WAN Optimization	51
Web Application Firewall	51
Web Filter	52
WiFi Controller	52
ZTNA	52
Common Vulnerabilities and Exposures	53
Known issues	54
Anti Virus	54
Explicit Proxy	54
GUI	54
HA	55
Hyperscale	55
IPsec VPN	55
Proxy	55
Routing	55
Security Fabric	56
SSL VPN	56
System	56
User & Authentication	56
Web Filter	57
ZTNA	57
Built-in AV Engine	58
Built-in IPS Engine	59
Limitations	60
Citrix XenServer limitations	60
Open source XenServer limitations	60

Change Log

Date	Change Description
2022-08-04	Initial release.
2022-08-08	Updated Resolved issues on page 34 , Known issues on page 54 , Built-in AV Engine on page 58 , and Built-in IPS Engine on page 59 .
2022-08-09	Updated New features or enhancements on page 15 and Known issues on page 54 .
2022-08-15	Updated Changes in default behavior on page 13 , Resolved issues on page 34 , and Known issues on page 54 .
2022-08-17	Updated Fortinet Security Fabric upgrade on page 27 and Product integration and support on page 31 .
2022-08-22	Updated New features or enhancements on page 15 and Known issues on page 54 .
2022-08-29	Updated Resolved issues on page 34 and Known issues on page 54 .
2022-08-31	Updated New features or enhancements on page 15 .
2022-09-19	Updated New features or enhancements on page 15 and Known issues on page 54 .
2022-09-26	Updated Resolved issues on page 34 and Known issues on page 54 .
2022-10-03	Updated Resolved issues on page 34 , Known issues on page 54 and Built-in IPS Engine on page 59 .
2022-10-06	Updated Resolved issues on page 34 .
2022-10-17	Updated Resolved issues on page 34 , Known issues on page 54 and Built-in IPS Engine on page 59 .
2022-11-01	Updated Resolved issues on page 34 , Known issues on page 54 and Built-in IPS Engine on page 59 .
2022-11-02	Updated Resolved issues on page 34 and Known issues on page 54 .
2022-11-15	Updated Known issues on page 54 .
2022-11-28	Updated Resolved issues on page 34 .
2022-12-12	Updated Resolved issues on page 34 and Known issues on page 54 .
2022-12-19	Updated Built-in IPS Engine on page 59 .
2022-12-27	Updated Known issues on page 54 .
2023-01-09	Updated Resolved issues on page 34 .
2023-01-23	Updated New features or enhancements on page 15 and Resolved issues on page 34 .
2023-02-02	Updated Product integration and support on page 31 .

Date	Change Description
2023-02-06	Updated Resolved issues on page 34 and Known issues on page 54 .
2023-02-21	Updated Resolved issues on page 34 .
2023-02-24	Updated New features or enhancements on page 15 and Resolved issues on page 34 .
2023-03-13	Updated Resolved issues on page 34 .
2023-03-20	Updated Changes in CLI on page 9 and Resolved issues on page 34 .
2023-03-24	Added VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name on page 29 .
2023-03-27	Updated Changes in default behavior on page 13 and Resolved issues on page 34 .
2023-04-17	Updated Changes in default behavior on page 13 .
2023-05-02	Updated New features or enhancements on page 15 and Known issues on page 54 .
2023-05-15	Updated Known issues on page 54 .
2023-05-29	Updated New features or enhancements on page 15 , Resolved issues on page 34 , and Known issues on page 54 .
2023-06-12	Added IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 8 .
2023-06-13	Updated Resolved issues on page 34 and Known issues on page 54 .
2023-06-26	Updated Resolved issues on page 34 and Known issues on page 54 .
2023-08-24	Updated Product integration and support on page 31 .
2023-09-06	Updated Built-in AV Engine on page 58 and Built-in IPS Engine on page 59 .
2023-09-18	Updated Resolved issues on page 34 .
2023-10-04	Updated Resolved issues on page 34 and Known issues on page 54 .
2023-10-16	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 8 , Resolved issues on page 34 , and Known issues on page 54 .
2023-10-31	Updated Resolved issues on page 34 .
2023-11-14	Updated Resolved issues on page 34 .
2023-12-12	Updated Resolved issues on page 34 .
2024-02-13	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 8 .
2024-03-06	Updated Known issues on page 54 .
2024-04-01	Added GUI firmware upgrade does not respect upgrade path on page 30 . Updated New features or enhancements on page 15 .

Introduction and supported models

This guide provides release information for FortiOS 7.2.1 build 1254.

For FortiOS documentation, see the [Fortinet Document Library](#).

Supported models

FortiOS 7.2.1 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

- IPsec phase 1 interface type cannot be changed after it is configured on page 8
- IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 8
- Support for FortiGates with NP7 processors and hyperscale firewall features on page 8

IPsec phase 1 interface type cannot be changed after it is configured

In FortiOS 7.2.0 and later, the IPsec phase 1 interface type cannot be changed after it is configured. This is due to the tunnel ID parameter (`tun_id`), which is used to match routes to IPsec tunnels to forward traffic. If the IPsec phase 1 interface type needs to be changed, a new interface must be configured.

IP pools and VIPs are not considered local addresses for certain FortiOS versions

For FortiOS 6.4.9 and later, 7.0.1 to 7.0.12, 7.2.0 to 7.2.5, and 7.4.0, all IP addresses used as IP pools and VIPs are not considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is not considered a destination for those IP addresses and cannot receive reply traffic at the application layer without special handling.

- This behavior affects FortiOS features in the application layer that use an IP pool as its source IP pool, including SSL VPN web mode, explicit web proxy, and the phase 1 local gateway in an interface mode IPsec VPN.
- The FortiGate will not receive reply traffic at the application layer, and the corresponding FortiOS feature will not work as desired.
- Configuring an IP pool as the source NAT IP address in a regular firewall policy works as before.

For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see [Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4](#).

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.2.1 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For information about hyperscale firewall support for FortiOS 7.2.1, refer to the [Hyperscale Firewall Release Notes](#).

Changes in CLI

Bug ID	Description
750230	<p>Add support for up to 30 virtual clusters (previously, only two were supported). The <code>vcluster2</code> and <code>config secondary-vcluster</code> settings have been replaced.</p> <pre>config system ha set vcluster-status enable config vcluster edit <id> ... next end end</pre>
773524	<p>Add option to configure whether the banned IP list persists through a power cycle.</p> <pre>config firewall global set banned-ip-persistency {disabled permanent-only all} end</pre> <p>The <code>diagnose user quarantine <parameter></code> command has changed to <code>diagnose user banned-ip <parameter></code>.</p>
789554	<p>Consolidate the FGSP settings by moving the previous <code>config system cluster-sync</code> settings into a subtable under <code>config system standalone-cluster</code>.</p> <p>Old syntax:</p> <pre>config system cluster-sync edit <id> set peervd <VDM> set peerip <address> set syncvd <VDM> config session-sync-filter ... end next end</pre> <p>New syntax:</p> <pre>config system standalone-cluster config cluster-peer edit <id> set peervd <VDM> set peerip <address> set syncvd <VDM> config session-sync-filter</pre>

Bug ID	Description
	<pre> ... end next end end </pre>
795943	<p>NetFlow collector and source IPs can be configured as an IPv4 or IPv6 address. This is supported in VDOM mode within global and VDOM configurations.</p> <pre> config system netflow set collector-ip <IPv4/IPv6_address> set source-ip <IPv4/IPv6_address> end </pre>
798305	<p>For non-hyperscale VDOMs, extend the maximum PBA timeout to 86400 seconds (3 - 86400, default = 30):</p> <pre> config firewall ippool edit <name> set pba-timeout <integer> next end </pre> <p>For CGNAT cases, extending the PBA timeout allows PBA logs to be generated less frequently on the FortiGate.</p>
799832	<p>For webhook, aws-lambda, azure-function, google-cloud-function, and alicloud-function automation actions, change the headers attribute to a http-headers configurable subtable (instead of a PARSE_F_MEMBER attribute) so the subtable entries are a key-value pair that can be variable sized strings.</p> <pre> config system automation-action edit <name> set action-type {webhook aws-lambda azure-function google- cloud-function alicloud-function} config http-headers edit 1 set key <string> set value <string> next edit 2 set key <string> set value <string> next end next end </pre>
801707	<p>Remove the ike-monitor, ike-monitor-interval, ike-heartbeat-interval, and ike-use-rfc6311 settings from config system cluster-sync.</p>
816604	<p>Remove the purge command under endpoint-control fctems.</p>

Changes in GUI behavior

Bug ID	Description
739194	<p>Add a time frame selector to the log viewer pages, so the logs can be loaded more efficiently.</p> <ul style="list-style-type: none">• Logs sourced from FortiAnalyzer and FortiCloud have the same time frame selection options as FortiView.• Logs sourced from disk have options to select <i>5 minutes</i>, <i>1 hour</i>, <i>24 hours</i>, <i>7 days</i>, or <i>None</i>.
753095	<p>Add visibility for configuring advanced options for wireless features in the FortiGate wireless controller GUI:</p> <ul style="list-style-type: none">• Add navigation entries under the <i>WiFi & Switch Controller</i> menu:<ul style="list-style-type: none">• <i>Operation Profiles</i>: includes tabs to configure FortiAP, QoS, and FortiAP configuration profiles• <i>Connectivity Profiles</i>: includes tabs to configure MPSK and bonjour profiles• <i>Protection Profiles</i>: includes tabs to configure WIDS and L3 firewall (also known as L3 access control list configurations for FortiAPs) profiles• Additional advanced options for wireless features under the <i>SSIDs</i> and <i>WiFi Settings</i> entries.
753107	<p>Add IoT device information to the <i>Security Fabric > Asset Identity Center</i> page, including the device name, software OS, hardware vendor, status, IP address, hostname, time last seen, port, VLAN, and so on.</p>
758549	<p>Enhance the <i>Managed FortiExtenders</i> tab on the <i>Network > FortiExtenders</i> page with additional monitoring features:</p> <ul style="list-style-type: none">• Add two charts for displaying <i>Status</i> and <i>Mode</i>.• Update <i>Status</i> column with <i>Online</i>, <i>Offline</i>, and <i>Waiting For Authorization</i> states.• Add default <i>Details</i> column populated with the data used by the modem/SIM card when FortiExtender is in WAN extension mode, or the connected IPsec tunnel used with the FortiGate when FortiExtender is in LAN extension mode.• When FortiExtender is in WAN extension mode, display modem information by left-clicking or hovering the mouse over the FortiExtender name to show a tooltip then clicking <i>Diagnostics and Tools</i>.• Make the <i>Serial #</i> column optional (previously this was a default column). <p>Enhance the <i>Profile</i> tab on the <i>Network > FortiExtenders</i> page with two charts for displaying <i>Status</i> and <i>Mode</i>.</p>
761169	<p>Update the <i>Log & Report > System Events</i> and <i>Security Events</i> pages:</p> <ul style="list-style-type: none">• Rename the <i>Details</i> tab to <i>Logs</i> tab.• Update the filters used in the log viewer to adjust the log filters and the <i>Log Details</i> pane.• Update the time frame settings for each <i>Log & Report</i> page so they are independent of each other.
775203	<p>Add <i>Network > IPAM</i> GUI page to centralize all IP address management (IPAM) details within three new tabs: <i>IPAM Interfaces</i>, <i>IPAM Rules</i>, and <i>IPAM Settings</i>.</p>

Bug ID	Description
	<p>This page is only viewable on a FortiGate that is not in a Security Fabric, or on the root FortiGate in a Security Fabric. In a Security Fabric, downstream FortiGates will receive a notification to view the root FortiGate.</p> <p>This new page replaces the IPAM dashboard widget and IPAM connector card within <i>Security Fabric > Fabric Connectors</i>, which have been removed.</p> <p>When viewing the IPAM interfaces tab, IP conflict markers are displayed to notify an administrator of IPAM pool IP conflicts with manually configured IPs and prompts administrators to use the <i>Edit Interface</i> dialog to manually resolve the conflict by changing the interfaces' IP/netmask settings.</p>
779209	<p>Advanced BGP options can be configured in the GUI on the <i>Network > BGP</i> page, including: the BGP neighbor local AS, hold time timer, keepalive timer, and enforcing eBGP multihop. The <i>View in Routing Monitor</i> buttons in the right-side of the screen can display the BGP neighbors list, the BGP IPv4 routing table, or the BGP IPv6 routing table in a slide-out window instead of redirecting to the monitor page. The <i>Routing</i> monitor includes an option to soft reset a neighbor from the BGP neighbors list.</p>
797544	<p>Enhance the <i>Summary</i> tabs on the <i>System Events</i> and <i>Security Events</i> pages under <i>Log & Report</i>:</p> <ul style="list-style-type: none">• Each event list footer shows the number of events related to that type.• In the top-left corner of the page, the number of total events is displayed. Hovering over the number displays number of events with a time stamp.• Clicking on any event entry or table title redirects to the log page with start and end time stamp as a filter.• On the <i>System Events > Summary</i> tab, hovering on the <i>Total Events By Level</i> label in the chart legend shows a tooltip of the total number of events with a time stamp.

Changes in default behavior

Bug ID	Description
689737	<p>Prior to this enhancement, individual applications can be selected in SD-WAN rules by default. Upon upgrade, the GUI functionality is available if applications are already configured in SD-WAN rules prior to upgrading. Otherwise, by default, individual applications and application groups cannot be selected in SD-WAN rules.</p> <p>To enable in the GUI:</p> <ol style="list-style-type: none">1. Go to <i>System > Feature Visibility</i>.2. In the <i>Additional Features</i> section, enable <i>Application Detection Based SD-WAN</i>.3. Click <i>Apply</i>. <p>To enable in the CLI:</p> <pre>config system global set gui-app-detection-sdwan enable end</pre>
761565	<p>Change the encryption and decryption method of backup files to AES-GCM method. The backup configuration file encrypted by the new algorithm in 7.2.1 cannot be restored on FortiGates running FortiOS 7.2.0 and earlier.</p>
771952	<p>The 15-day evaluation period for a FortiGate VM is replaced with a permanent evaluation VM license. When spinning up a new FortiGate VM, the user will have a choice of logging in to FortiCare to activate the VM trial or to upload a full license. Each FortiCare account is entitled to one evaluation VM license.</p> <p>Limitations of the evaluation VM license include:</p> <ul style="list-style-type: none">• There is only support for low encryption operation, except for GUI management access and FortiManager communications.• There is a maximum of one CPU and 2 GB of memory.• There is a maximum of three interfaces, firewall policies, and routes.• There is no FortiCare support. <p>The evaluation VM license is applicable to all private cloud (VMware ESXi, KVM, and so on) and all BYOL public cloud instances.</p>
773165	<p>By default on a new deployment, the FortiGate will use the certificate named Fortinet_GUI_Server for HTTPS administrative access. This certificate is generated and signed by the built-in Fortinet_CA_SSL certificate, which dynamically updates the SAN field of the Fortinet_GUI_Server certificate with IP addresses of all interfaces enabled for HTTPS. After installing the Fortinet_CA_SSL CA certificate on a PC, administrators can access the FortiGate GUI through a browser without any warnings.</p>
783487	<p>Prior to 7.2.1, after an HA failover due to memory utilization, the original primary device will not fail over back to the primary after memory has dropped below the threshold. Starting in 7.2.1, the original primary device will fail over back to the primary once its memory usage drops below the threshold.</p>

Bug ID	Description
796546	<p>Loopback interfaces are no longer allowed to be configured as gateway interfaces on static routes. Upon upgrade, static route configurations with loopbacks as gateway interfaces will be removed.</p> <p>Affected use case: a loopback interface may be used in a static route so that the route can be advertised by BGP using network or redistribute static. This scenario can no longer be configured.</p> <p>Workaround: instead of creating a static route using a loopback interface, create a black hole route for the same destination. Then, advertise the network in BGP using network or redistribute static.</p>
802757	<p>In order for unlicensed FortiGate VMs to be managed by FortiManager, FortiOS enables high encryption on the FGFM protocol for a secure connection between the FortiGate and FortiManager. Upon being added into the device manager, FortiManager can install VM licenses to the managed FortiGate VMs.</p>

New features or enhancements

More detailed information is available in the [New Features Guide](#).

Bug ID	Description
535099	When editing an SSID interface within <i>WiFi & Switch Controller > SSIDs</i> , an address group containing wireless clients' MAC addresses and an address group policy (disable, allow, or deny) can be configured for the client MAC address filtering feature.
652281	Disable all proxy features on FortiGate models with 2 GB of RAM or less by default. Mandatory and basic mandatory category processes start on 2 GB memory platforms. Proxy dependency and multiple workers category processes start based on a configuration change on 2 GB memory platforms.
688237	<p>Add support for a FortiGate to manage a Procend 180-T DSL transceiver (FN-TRAN-DSL) that is plugged into an SFP port.</p> <p>The management of the DSL transceiver includes the ability to program the physical layer attributes on the DSL module, retrieve the status and statistics from the module, support firmware upgrade of the module, and reset the module. The following VDSL profiles are supported: 8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a.</p> <p>Supported platforms: FG-80F, FG-81F, FG-80F-BP, FGR-60F, and FGR-60F_3G4G.</p>
695712	<p>Add <i>FortiView Internal Hubs</i> monitor page that displays internal host connections based on NetFlow data received from managed switches behind the FortiGate. Drilling down on a host allows users to see all the connections made from the device to various destinations.</p> <p>The FortiLink interface can be configured as a NetFlow collector so that underlying switches can send NetFlow data to it.</p> <pre>config system interface edit fortilink set switch-controller-netflow-collect {enable disable} next end</pre>
697160	<p>IPv6 dynamic addresses can be retrieved from Cisco ACI SDN connectors. IPv6 addresses imported from Cisco ACI to the Fortinet SDN Connector VM can be imported into the FortiGate as IPv6 dynamic addresses. The Fortinet SDN Connector VM must be running version 1.1.10 or later.</p> <pre>config firewall address6 edit <name> set type dynamic set sdn <ACI_connector> next end</pre>

Bug ID	Description
727383	Add CLI support for IPv6 addresses in Internet Service Database (ISDB), and allow them to be configured in firewall policies.
735929	Add REST API in both FortiNAC and FortiGate that is used by FortiNAC to send user logon/logoff information to the FortiGate. A new dynamic firewall address type (FortiNAC tag) is added to FortiOS, which is used to store the device IP, FortiNAC firewall tags, and FortiNAC group information sent from FortiNAC via the REST API when user logon/logoff events are registered. The FortiNAC tags connector under <i>Security Fabric > Fabric Connectors</i> is deprecated. For upgrade support, the FSSO FortiNAC user type can still be configured from the CLI.
739174	<p>For a FortiGate with a valid Security Rating license, the separate Security Rating package downloaded from FortiGuard adds support for PSIRT vulnerabilities, which allows the security rating result to highlight them. If the security rating result highlights a vulnerability with a critical severity, then the FortiGate GUI displays a new warning message in the header and a new notification under the bell icon. Both GUI enhancements link to the <i>System > Fabric Management</i> page to encourage updating any affected Fortinet Fabric devices to the latest firmware releases to resolve the critical vulnerabilities.</p> <p>A new <i>View Vulnerability</i> link in the header is visible for global administrators, and a new tooltip for the <i>critical vulnerability</i> label on the <i>System > Fabric Management</i> page both link to the Security Rating page and highlight the critical vulnerability. On the <i>Security Rating</i> page, the search bar supports using the PSIRT keyword to filter for PSIRT vulnerabilities, and the security panel provides a link to the <i>System > Fabric Management</i> page when a PSIRT vulnerability is selected.</p>
739182	Allow FortiClients to learn the available ZTNA services from the FortiGate ZTNA portal. The services that can be learned include HTTP/HTTPS web services, TCP forwarding services, and web portals. The FortiClient must connect to the FortiGate using a DoT or DoH tunnel. Then, it can retrieve the service mapping in JSON format.
743804	Add a RADIUS option to allow the FortiGate to set the RADIUS accounting message group delimiter to a comma (,) instead of a plus sign (+) when using RSO. The default delimiter is still a plus sign.
745135	<p>Provide three sizes of internet service databases, and an option to choose between full, standard, or mini databases. Only FortiGate 30 and 50 series models can configure mini size.</p> <pre> config system global set internet-service-database {mini standard full} end </pre>
750320	<p>Add command to add ZTNA virtual hosts and domains to the FortiGates local DNS database. Each virtual host and domain is mapped to the VIP defined for the corresponding access proxy. Each virtual host can only be used in one access proxy.</p> <pre> config firewall access-proxy edit <name> set add-vhost-domain-to-dnsdb {enable disable} next end </pre>

Bug ID	Description
753742	Improve the Security Fabric backend to allow physical topology, logical topology, and security rating report information to be gathered through distributed means through each downstream FortiGate device. This results in less delays and memory usage on the Fabric root, and less API calls to the downstream devices.
760932	The SAP external Fabric connector allows the FortiGate to connect to an SAP controller to synchronize dynamic address objects and ports for SAP workloads. These address objects can be used in firewall policies to grant access control to dynamic SAP workloads.
764957	<p>Add automation trigger for certificate expiry by introducing <code>local-certificate-near-expiry</code> event type if a user-supplied local certificate used for SSL VPN, deep inspection, or other purpose is about to expire. This trigger relies on a VPN certificate setting in the CLI configuration setting for the certificate log expiring warning threshold:</p> <pre>config vpn certificate setting set cert-expire-warning <integer> end</pre> <p>Where <code><integer></code> is the certificate log expiring warning threshold, in days (0 - 100, default = 14). The local certificate expiry trigger can be used with an email notification action, for example, to remind an administrator to re-sign or load a new local certificate to avoid any service interruptions.</p>
766158	In a video filter profile, when the FortiGuard category-based filter and YouTube channel override are used together, by default a video will be blocked if it matches either category or YouTube channel and the action is set to block. This enhancement enables the channel action to override the category action. A category can be blocked, but certain channels in that category can be allowed when the <code>override-category</code> option is enabled.
773555	Add option to push updates to external threat feeds through the REST API. When configuring a <i>FortiGuard Category</i> , <i>Malware Hash</i> , <i>IP Address</i> , or <i>Domain Name</i> threat feed from the <i>Security Fabric > External Connectors</i> page, select the <i>Push API</i> update method to provide the code samples needed to perform add, remove, and snapshot operations.
775285	Enhance LAN extension on the FortiGate to allow a remote FortiGate (FortiGate Connector) to provide remote connectivity back to the FortiGate (FortiGate Controller) over a backhaul connection. A FortiGate deployed at a remote location will discover the FortiGate Controller and form an IPsec tunnel (or multiple tunnels when multiple links exists on the FortiGate Connector) back to the FortiGate Controller. A VXLAN is established over the IPsec tunnels to create an L2 network between the FortiGate Controller and the network behind the FortiGate Connector.
775287	Allow an administrator to deregister a FortiGate if the device has been registered for three or more years. After the device is deregistered, all associated contracts are also deregistered.
775288	<p>Enhance IP address management (IPAM) in the GUI and the CLI to allow multiple pools and assign them to different interfaces based on name and/or role using IPAM rules.</p> <p>In the GUI of a FortiGate not in a Security Fabric or on the root FortiGate of a Security Fabric, IPAM pools can be defined under <i>Network > IPAM > IPAM Settings</i>, and IPAM rules can be defined under <i>Network > IPAM > IPAM Rules</i>.</p> <p>In the CLI of a FortiGate not in a Security Fabric or on the root FortiGate of a Security Fabric, IPAM pools can be defined as follows where a.b.c.d/x is the IP/netmask of the subnet:</p>

Bug ID	Description
	<pre> config system ipam config pools edit <name> set subnet <a.b.c.d/x> next end end </pre> <p>In the CLI of a FortiGate not in a Security Fabric or on the root FortiGate of a Security Fabric, IPAM rules can be defined as follows (device and interface fields accept * wildcard inputs):</p> <pre> config system ipam config rules edit <rule_name> set device {<FortiGate_serial_number> *} set interface {<name> *} set pool <pool_name> next end end </pre>
779304	YAML can be selected as file format when backing up or restoring configurations from the GUI.
780993	When registering using FortiCare, users can select a <i>Government</i> end user type for parity with the registration process using the support portal.
784630	<p>Support BGP Autonomous System (AS) numbers as input in asdot and asdot+ format from RFC 5396 for the following CLI commands:</p> <ul style="list-style-type: none"> • BGP AS • BGP neighbour/neighbour group local AS • BGP neighbour/neighbour group remote AS • Route map set AS path <p><code>get router info bgp summary</code> and other BGP router commands still display the AS numbers in asplain format.</p>
784665	<p>Add option for a FortiGate to use FortiManager as an override server for IoT query services.</p> <pre> config system central-management config server-list edit 1 set server-type {iot-query iot-collect} next end end </pre>
786329	Extend VCI (vendor class identifier) support in DHCP to allow for VCI pattern matching as a condition for IP or DHCP option assignment. This allows the mapping of a single IP address, IP ranges of a pool, and dedicated DHCP options to a specific VCI string.

Bug ID	Description
786559	Add <code>fgFwAuthUserTables</code> table for SNMP to gather information about authenticated users, which are users authenticated by the user authentication methods supported on the FortiGate. This table supports SNMP VDOM access control and OIDs for IPv4 and IPv6 authenticated users.
787019	Perform FortiExtender auto firmware provisioning using CLI commands to allow a federated upgrade of a FortiExtender upon discovery and authorization by the FortiGate. The FortiExtender will be upgraded to the latest firmware from FortiGuard, based on the matching FortiExtender firmware version that matches each FortiOS firmware version.
787020	Add information and logs to record and trace connection failures to the EMS server.
787021	<p>In an SD-WAN scenario when DSCP tags are used to mark traffic from the branch to the hub, it is sometimes desirable for the hub to mark the reply traffic with the same DSCP tags. A setting has been added to the firewall policy configurations to allow the DSCP tag to be copied to the reply direction.</p> <pre> config firewall policy edit <id> set diffserv-copy {enable disable} next end </pre>
787477	<p>Ensure that session synchronization happens correctly in the FGCP over FGSP topology.</p> <ol style="list-style-type: none"> 1. When the session synchronization filter is applied on FGSP, the filter will only affect sessions synchronized between the FGSP peers. 2. When virtual clustering is used, sessions synchronized between each virtual cluster can also be synchronized to FGSP peers. The peers' <code>syncvd</code> must all be in the same HA <code>vcluster</code>.
789032	<p>Embed SLA information into ICMP probes, which consists of three parts:</p> <ol style="list-style-type: none"> 1. Embed spokes' SLA information (latency, jitter, packet loss) into the ICMP probes that the spokes send to the hub. In turn, the hub will read the embedded ICMP probes to gather SLA information on each overlay from each spoke. 2. Allow SD-WAN to change the IKE route's priority according to SLA status (within SLA or out of SLA) on IPsec overlays. 3. Allow a recursively resolved BGP route to inherit the priority from its parent. <p>By passing SLA information to the hub, the hub can route traffic to the spoke symmetrically based on the overlay that is in SLA on the spoke.</p>
789811	FortiOS has been enhanced with support for round-robin mode and Receive Packet Steering (RPS) on the IPsec interface. This ensures that the encrypted and decrypted IPsec packets are evenly distributed across all available CPUs, addressing the issue of uneven CPU usage.
790243	Inline scanning is supported when the FortiGate is licensed with the FortiGuard AI-Based Sandbox Service (FAIS). It works similar to inline scanning for the FortiSandbox appliance, by holding a file up to 50 seconds for the verdict to be returned. Timed out scans can either be set to block, log, or ignore. Inline scanning can be enabled from the GUI on the <i>Cloud Sandbox</i> configuration page.
791091	Add settings to disable a FortiGate administrator account with a customized access profile from running <code>execute ssh</code> and <code>execute telnet</code> , thus restricting jump host capability using SSH and Telnet from the FortiGate to another host.

Bug ID	Description
	<pre> config system accprofile edit <name> set system-execute-ssh {enable disable} set system-execute-telnet {enable disable} next end </pre>
791129	<p>Add the underlay link cost property to the IPsec VPN tunnel phase 1 configuration and enhance IPsec VPN to exchange the link cost with a remote peer as a private notified payload in the phase 1 negotiation of IKEv1 and IKEv2. This avoids possible health check daemon process load issues and improves network scalability in a large-scale SD-WAN networks with ADVPN.</p> <pre> config vpn ipsec phase1-interface edit <name> set link-cost <0 - 255> next end </pre>
791732	<p>Allow <code>interface-select-method</code> and <code>interface</code> to be configured for FortiClient EMS Fabric connectors.</p>
792170	<p>The FortiGate explicit web proxy supports the Cross-Origin Resource Sharing (CORS) protocol, which allows the FortiGate to process a CORS preflight request and an actual CORS request properly, in addition to a simple CORS request when using session-based, cookie-enabled, and captive portal-enabled SAML authentication. This allows a FortiGate explicit web proxy user with this specific configuration to properly view a web page requiring CORS with domains embedded in it other than its own domain.</p>
792204	<p>Update libssh2 to support DH parameters larger than 2048.</p>
793303	<p>Add a system action automation action type to back up the configuration of the FortiGate to the disk revisions, reboot the FortiGate, or shutdown the FortiGate. This action type allows these actions to occur even if the FortiGate is in conserve mode and allows the automation stitch to bypass the CLI user confirmation prompts, which the CLI script action does not support.</p> <pre> config system automation-action edit <name> set action-type system-actions set system-action {reboot shutdown backup-config} next end </pre>
793304	<p>Enhance the scheduled automation trigger to execute only once at a specific date and time in the future. This trigger may be useful to support one-time automated FortiGate system actions in the future, such as a configuration backup to disk, reboot, or shut down.</p> <pre> config system automation-trigger edit <name> set trigger-type scheduled set trigger-frequency once set trigger-datetime <YYYY-MM-DD HH:MM:SS> next end </pre>

Bug ID	Description
	<pre> next end </pre>
794494	Proxy auto-config (PAC) files can be downloaded for an explicit proxy through the FortiGate's captive portal using HTTPS to ensure a secure download.
795820	Support Layer 3 roaming between different VLANs and subnets on the same or different wireless controller for bridge mode SSIDs. A client connected to the bridge mode SSID on one FortiAP can roam to the same SSID on another FortiAP managed by the same or different FortiGate wireless controller and continue to use the same IP.
795821	<p>Support WiFi 6 Release 2 security enhancements by adding support for Hash-to-Element (H2E) only and Simultaneous Authentication of Equals Public Key (SAE-PK) for FortiAP models that support WPA3-SAE security modes.</p> <pre> config wireless-controller vap edit <name> set ssid <ssid> set security wpa3-sae set sae-h2e-only {enable disable} next end config wireless-controller vap edit <name> set ssid <ssid> set security wpa3-sae set sae-pk {enable disable} set sae-private-key <private_key> next end </pre>
795822	<p>Enhance the FortiGate ZTNA access proxy to act as an inline cloud access security broker (CASB) by providing access control to software as a service (SaaS) traffic using ZTNA access control rules. This enhancement introduces a new FortiGuard Inline CASB Database (ICDB) that includes all FQDNs related to specific SaaS applications and corresponding FortiGuard packages for FortiOS and FortiClient. The inline CASB feature is included with the FortiClient ZTNA license. No separate license is needed for inline CASB.</p> <p>Previously, ZTNA SaaS access control was possible using the TCP forwarding access proxy configuration on FortiGate and FortiClient:</p> <ul style="list-style-type: none"> On the FortiGate, users would need to search all hostnames used by a SaaS application, configure these hostnames as FQDN addresses, and configure these addresses as part of the ZTNA TCP forwarding settings. In FortiClient, users would need to manually add all the hostnames as destinations for ZTNA connection rules or use FortiClient EMS to push those rules to FortiClient.

Bug ID	Description
	<p>With this enhancement and service, users can configure the ZTNA access proxy with a new SaaS proxy access type and conveniently specify SaaS application destinations by application name or by application group name without needing to manually search for and enter FQDNs specific to each SaaS application. Currently, CLI commands must be used for the configuration. Users can configure the SaaS application destination by adding support for SaaS in <code>config firewall proxy-address</code>, which can be used in <code>config firewall proxy-policy</code>. The FortiGate traffic log has been enhanced with a new log field, <code>saasname</code>.</p> <p>Support for this feature will be available in a future version of FortiClient and FortiClient EMS</p>
796798	<p>Support wireless controller VAP <code>set rates-11ac-mcs-map</code> and <code>set rates-11ax-mcs-map</code> commands to configure 802.11ac and 802.11ax Modulation and Coding Scheme (MCS) rates. These commands replace the <code>set rates-11ac-ss12</code>, <code>set rates-11ac-ss34</code>, <code>set rates-11ax-ss12</code>, and <code>set rates-11ax-ss34</code> VAP commands.</p>
796961	<p>Add attribute under <code>config switch-controller igmp-snooping</code> to configure the <code>query-interval</code> under FortiLink, and add a check to ensure the <code>query-interval</code> is less than the <code>aging-time</code> interval.</p>
797054	<p>When backing up configurations for the purpose of troubleshooting from a third party, it is helpful to sanitize the configuration file for passwords and secrets so they are not leaked. To streamline this process, the <i>Password mask</i> option on the <i>Backup System Configuration</i> page enables passwords and secrets to be obfuscated during the backup process. This can also be accomplished from the CLI by running:</p> <pre># execute backup obfuscated-config {flash ftp management-station sftp tftp usb} # execute backup obfuscated-full-config {ftp sftp tftp usb} # execute backup obfuscated-yaml-config {ftp tftp}</pre>
798310	<p>In addition to per-tunnel IPsec failover for FGSP peers, FGCP over FGSP is also supported. For additional redundancy, an FGCP cluster on one site may form FGSP peering with FGCP clusters on other sites. The FGCP over FGSP peers can still synchronize IPsec SAs and act as the primary gateway for individual tunnels for the same dialup servers. When failover happens within an FGCP cluster, tunnel traffic will fail over to the other FGCP cluster member. When an FGCP cluster fails, tunnel traffic will fail over to the other FGSP peer.</p>
798773	<p>Add options in IPv6 static and policy routes for parity with IPv4 static and policy routes.</p>
799621	<p>Support wireless authentication using SAML and a captive portal configured on a tunnel mode SSID.</p> <p>When a SAML user has been configured on the FortiGate, a user group containing this SAML user can be applied to a captive portal in a wireless tunnel mode SSID. When configured with both a captive portal exempt firewall policy to allow wireless clients to contact the SAML IdP and a firewall policy with the SAML user group applied to allow authenticated traffic, upon connecting to this SSID, wireless clients will be redirected to a login page for wireless authentication using SAML.</p>

Bug ID	Description
799971	<p>To synchronize Active Directory users and apply two-factor authentication using FortiToken Cloud, two-factor authentication can be enabled under the <code>user ldap</code> object definition. This enhancement reduces the number of the AD users returned by allowing the use of a group filter to synchronize only the users who meet the group filter criteria.</p> <pre> config user ldap edit <name> set dn <string> set two-factor {disable fortitoken-cloud} set two-factor-filter <string> next end </pre>
799987	<p>Add support for multitenant FortiClient EMS deployments that have the <i>Manage Multiple Customer Sites</i> setting enabled with multiple sites. Since a FortiClient EMS site is no longer unique using its serial number alone, the FortiGate configuration for FortiClient EMS connectors and related diagnostic commands have been enhanced to distinguish EMS sites using serial number and tenant ID:</p> <ul style="list-style-type: none"> Update <code>config endpoint-control fcitems</code> to predefine five FortiClient EMS Fabric connectors that are referred to using numerical IDs from 1 to 5. Administrators can configure the <code>status</code> and <code>name</code> settings, and to display the tenant ID retrieved from FortiClient EMS sites with <i>Manage Multiple Customer Sites</i> enabled. <p>A single tenant EMS server or the default site on a multitenant EMS server has a tenant ID consisting of all zeros (00000000000000000000000000000000).</p> <ul style="list-style-type: none"> Update the FortiClient EMS Fabric connector to retrieve specific ZTNA tags from each configured FortiClient EMS site. Update <code>diagnose endpoint record list</code> to return the <code>EMS tenant id</code> field retrieved from each respective FortiClient EMS server. Update ZTNA and EMS debug commands to accept the EMS serial number and tenant ID as parameters. <pre> # diagnose endpoint lls-comm send ztna find-uid <uid> <EMS_serial_ number> <EMS_tenant_id> # diagnose wad dev query-by uid <uid> <EMS_serial_number> <EMS_tenant_ id> </pre> <p>FortiClient 7.0.3 and later is required to use this feature.</p>
801700	<p>Add option to enable automatic firmware updates based on the FortiGuard upgrade path. When enabled, the FortiGate will look for an upgrade path and perform an upgrade at a time within the time period specified by the administrator. The upgrade will only be performed on a patch within the same major release version.</p> <pre> config system fortiguard set auto-firmware-upgrade {enable disable} set auto-firmware-upgrade-day {sunday monday tuesday wednesday thursday friday saturday} set auto-firmware-upgrade-start-hour <integer> </pre>

Bug ID	Description
	<pre> set auto-firmware-upgrade-end-hour <integer> end </pre>
801701	Certain unused WAD proxy processes are not started by default on FortiGate models with 2 GB of RAM or less to reduce memory usage. These process will only start when relevant proxy features are configured.
801707	<p>During FGSP per-tunnel failover for IPsec, the same IPsec dialup server configured on each FGSP member may establish tunnels with dialup clients as the primary gateway. The IPsec SAs are synchronized to all other FGSP peers that have FGSP synchronization for IPsec enabled. Other FGSP members may establish a tunnel with other clients on the same dialup server and synchronize their SAs to other peers.</p> <p>Upon the failure of the FGSP member that is the primary gateway for a tunnel, the upstream router will fail over the tunnel traffic to another FGSP member. The other FGSP member will move from standby to the primary gateway for that tunnel and continue to forward traffic.</p> <pre> config vpn ipsec phase1-interface edit <name> set fgsp-sync {enable disable} next end </pre>
801708	In conjunction with support for FGSP per-tunnel failover for IPsec, configuring DPD (dead peer detection) on an FGSP member is now permitted. This allows a failed FGSP member to send out DPD probes during failover to detect the unreachable remote peer and flush the corresponding tunnels.
802702	When local-out traffic such as SD-WAN health checks, SNMP, syslog, and so on are initiated from an interface on one VRF and then pass through interfaces on another VRF, the reply traffic will be successfully forwarded back to the original VRF.
802785	Add the ability to toggle 802.11d support for 2.4 GHz radios using a FortiAP profile. 802.11d only applies to the 802.11g band (2.4 GHz band). By default, this option is always enabled. When 802.11d is enabled, the FortiAPs broadcast the country code in beacons, probe requests, and probe responses. The ability to disable 802.11d on the FortiAPs provides backwards compatibility with old or legacy Wi-Fi clients in the 802.11g band (2.4 GHz band) that failed to associate to a FortiAP with 802.11d enabled.
803326	Vendor-Specific Attributes (VSAs) can be used with TACACS authentication and authorization in wildcard system administrator access to FortiGates from browsers and SSH. The new VSAs allows the FortiGate to perform group matching, and overwrite VDOM settings under <code>system admin</code> .
803336	<p>Add option for private key retention during SCEP renewal.</p> <pre> config vpn certificate local edit <name> set enroll-protocol scep set private-key-retain {enable disable} next end </pre>

Bug ID	Description
805611	<p>Support custom replacement message groups for each ZTNA virtual host. The <code>%%ZTNA_DETAIL_TAG%%</code> variable can be used in replacement messages.</p> <pre> config firewall access-proxy-virtual-host edit <name> set host <string> set replacemsg-group <string> next end </pre>
805870	<p>Add setting to enforce ZTNA trusted client before the user can successfully establish a SSL VPN tunnel when connecting to FortiGate SSL VPN in tunnel mode, and has a device certificated issued by EMS.</p> <pre> config vpn ssl setting set ztna-trusted-client {enable disable} end </pre>
805871	<p>Add support in Azure FG-VM to generate a unique vWAN cluster/group ID and display a line with the Azure NVA name and the generated cluster/group ID in <code>get system status</code>. This line is only displayed for FortiGate instances that are NVA VMs. FortiManager uses the cluster/group ID to display FortiGate VM instances from the same vWAN as a group.</p>
805872	<p>Allow FortiManager to apply a license to a BYOL FortiGate VM instance. For example, when launching a BYOL FortiGate VM on Azure, the FortiGate receives a serial number with the FGVMEV prefix and a VM license with an invalid status by default. This unlicensed FortiGate VM can register to a FortiManager for authorization and management. Subsequently, the FortiManager can apply a VM license to the FortiGate VM instance.</p>
806166	<p>Add NetFlow support on EMAC VLAN interface.</p>
806628	<p>Added endpoint to return HA non-synchronized checksum. The HA checksum calculation module has new parameter to switch between the regular checksum calculation and the non-synchronized checksum calculation.</p> <pre> # diagnose sys ha checksum show-nonsync [global vdom_name] </pre>
806993	<p>Enhance the ZTNA access proxy to determine whether a client device that does not have FortiClient installed is a mobile device that is considered unmanageable, or is not a mobile device that is considered unknown and tag the device as either <code>ems-tag-unmanageable</code> or <code>ems-tag-unknown</code> respectively. The FortiGate WAD process achieves this by either matching device TLS fingerprints against a library or learning information from the HTTP User-Agent header if the <code>set user-agent-detect</code> setting is enabled. These new tags allow for ZTNA access control of unmanaged devices using <code>config firewall proxy-policy</code>. Also, enhance the <code>set empty-cert-action</code> setting by adding an <code>accept-unmanageable</code> option to allow unmanageable clients to continue ZTNA proxy rule processing.</p>
807431	<p>In proxy mode antivirus profiles, add option under HTTP to customize the action for files with unknown content encoding (default = block).</p> <pre> config antivirus profile edit <name> </pre>

Bug ID	Description
	<pre>set feature-set proxy config http set unknown-content-encoding {block inspect bypass} end next end</pre>
809701	<p>Support auto revision backup on FortiSwitch upon log out or firmware upgrade in FortiLink mode (both settings are disabled by default).</p> <pre>config switch-controller switch-profile edit <name> set revision-backup-on-logout {enable disable} set revision-backup-on-upgrade {enable disable} next end</pre>
812209	<p>This enhancement builds on the AWS SDN connector, which uses the AWS security token service (STS) to connect to multiple AWS accounts concurrently. To enhance security, the SDN connector supports the use of an External ID, which allows the target account owner to permit the role to be assumed by the source account only under specific circumstances.</p>
813346	<p>Improve GTPv2 message filtering to include all GTPv2 message types, based on 3GPP TS 29.274. Also, by adding message types UE Registration Query request (61) and UE Registration Query response (62), FortiOS Carrier can now filter all GTPv0 and GTPv1 message types based on 3GPP release 3GPP TS 29.060.</p>

Upgrade information

Supported upgrade path information is available on the [Fortinet Customer Service & Support site](#).

To view supported upgrade path information:

1. Go to <https://support.fortinet.com>.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
 - *Current Product*
 - *Current FortiOS Version*
 - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.2.1 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.2.1
FortiManager	• 7.2.1
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP FortiAP-S FortiAP-U FortiAP-W2	• See Strong cryptographic cipher requirements for FortiAP on page 29
FortiClient* EMS	• 7.0.3 build 0229 or later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 or later
FortiClient* Mac OS X	• 7.0.3 build 0131 or later
FortiClient* Linux	• 7.0.3 build 0137 or later
FortiClient* iOS	• 7.0.2 build 0036 or later
FortiClient* Android	• 7.0.2 build 0031 or later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 4.2.0 and later for post-transfer and inline scanning

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice
17. FortiDeceptor
18. FortiAI/FortiNDR
19. FortiTester
20. FortiMonitor



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.1. When Security Fabric is enabled in FortiOS 7.2.1, all FortiGate devices must be running FortiOS 7.2.1.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in, go to *Support > Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 and later need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

FortiGate VM VDOM licenses

FortiGate VMs with one VDOM license (S-series, V-series, FortiFlex) have a maximum number of two VDOMs. An administrative type root VDOM and another traffic type VDOM are allowed in 7.2.0 and later. After upgrading to 7.2.0 and later, if the VM previously had split-task VDOMs enabled, two VDOMs are kept (the root VDOM is an administrative type).

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the `set vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

GUI firmware upgrade does not respect upgrade path

When performing a firmware upgrade that requires multiple version jumps, the *Follow upgrade path* option in the GUI does not respect the recommended upgrade path, and instead upgrades the firmware directly to the final version. This can result in unexpected configuration loss. To upgrade a device in the GUI, upgrade to each interim version in the upgrade path individually.

For example, when upgrading from 7.0.7 to 7.0.12 the recommended upgrade path is 7.0.7 -> 7.0.9 -> 7.0.11 -> 7.0.12. To ensure that there is no configuration loss, first upgrade to 7.0.9, then 7.0.11, and then 7.0.12.

Product integration and support

The following table lists FortiOS 7.2.1 product integration and support information:

Web browsers	<ul style="list-style-type: none">• Microsoft Edge 109• Mozilla Firefox version 98• Google Chrome version 99 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	<ul style="list-style-type: none">• Microsoft Edge 44• Mozilla Firefox version 74• Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	<ul style="list-style-type: none">• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	<ul style="list-style-type: none">• 5.0 build 0308 and later (needed for FSSO agent support OU in group filters)• Windows Server 2019 Standard• Windows Server 2019 Datacenter• Windows Server 2019 Core• Windows Server 2016 Datacenter• Windows Server 2016 Standard• Windows Server 2016 Core• Windows Server 2012 Standard• Windows Server 2012 R2 Standard• Windows Server 2012 Core• Windows Server 2008 64-bit (requires Microsoft SHA2 support package)• Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)• Windows Server 2008 Core (requires Microsoft SHA2 support package)• Novell eDirectory 8.8
AV Engine	<ul style="list-style-type: none">• 6.00276
IPS Engine	<ul style="list-style-type: none">• 7.00234

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	<ul style="list-style-type: none"> 8.1 Express Edition, Dec 17, 2019
Linux KVM	<ul style="list-style-type: none"> Ubuntu 18.0.4 LTS Red Hat Enterprise Linux release 8.4 SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	<ul style="list-style-type: none"> 2012R2 with Hyper-V role
Windows Hyper-V Server	<ul style="list-style-type: none"> 2019
Open source XenServer	<ul style="list-style-type: none"> Version 3.4.3 Version 4.1 and later
VMware ESXi	<ul style="list-style-type: none"> Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 98 Google Chrome version 99
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 98 Google Chrome version 99
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 98 Google Chrome version 99
macOS Monterey 12.2	Apple Safari version 15 Mozilla Firefox version 98 Google Chrome version 99
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 7.2.1. To inquire about a particular bug, please contact [Customer Service & Support](#).

Anti Virus

Bug ID	Description
722304	AV does not block malicious file uploads to the MS Exchange server (OWA).
727067	FortiGate should fix the interface between FortiGate and FortiAnalyzer for the CDR file.
794575	If FortiGate Cloud is selected as sandbox server under <i>Security Fabric > Fabric Connectors</i> , an anti virus profile with settings to <i>Send files to FortiSandbox for inspection</i> does not get saved in the GUI.
805655	A scanunit crash with signal 11 occurs for SMTP and QP encoding.
823677	When a FortiGate with DLP patterns configured is connected to FortiSandbox, scanunit crashes when the FortiSandbox extension reloads or worker shuts down.

Application Control

Bug ID	Description
787130	Application control does not block FTP traffic on an explicit proxy.

Data Leak Prevention

Bug ID	Description
807327	A scanunit crash occurs after upgrading to 6.4.9.

DNS Filter

Bug ID	Description
744572	In multi-VDOM with default <code>system fortiguard</code> configuration, the DNS filter does not work for the non-management VDOM.
790974	When the DNS static domain filter entry's action set to allow, it skips DNS translation.
796052	If local-in and transparent requests are hashed into the same local ID list, when the DNS proxy receives a response, it finds the wrong query for requests with the same ID and domain.
798562	DNS filter does not work when the FortiGate is working as a DNS server.
800497	In flow mode with <code>set status disable</code> in the static domain filter, the entry still works when enabled in the DNS filter.

Endpoint Control

Bug ID	Description
775742	Upgrade EMS tags to include classification and severity to guarantee uniqueness.
803198	Intermittent FortiOS failure when using a redundant EMS configuration because the EMS FQDN was resolved once before, and when DNS entry expires or the DNS is used for load balancing.

Explicit Proxy

Bug ID	Description
770440	Explicit web proxy encounter lots of WAD crashes.
774442	WAD is NATting to the wrong IP pool address for the interface.
778339	Improve logic of removing HTTP Proxy-Authorization/Authorization header to prevent user credential leaking.
794124	HTTPS websites are not accessible if <code>certificate-inspection</code> is set in a proxy policy.
794255	Microsoft website (microsoft.com) cannot be mapped to the Microsoft-Web ISDB name for proxy policy.
796364	Renaming a ClearPass dynamic address object that is configured in a proxy policy causes the address not to be matched.
798647	Explicit web proxy firewall policy can not pass through HTTP traffic.
801602	In agentless NTLM authentication, the source IP in <code>user domain-controller</code> is not applied.

Bug ID	Description
802829	Explicit proxy encounters a 504 timeout after <code>CONNECT</code> in 7.2.0 GA.
811251	WAD daemon may crash upon user log off when using two type of messages (UI and group) at the same time.
816879	When an explicit proxy is enabled with IP pools, certificate inspection probe sessions use the interface IP instead of IPs from the configured IP pool. Therefore, when an interface IP is not allowed to connect externally, the probe session fails and causes traffic to not work.

Firewall

Bug ID	Description
599638	Get unexpected count for <code>established session count</code> , and <code>diagnose firewall iprope clear</code> does not work as expected.
677855	<code>cmdbsrv</code> and other processes take CPU resources upon every configuration change in devices with over ten thousand firewall policies.
750081	Traffic can pass through an EMAC VLAN interface but cannot be offloaded.
752267	<i>Load Balance Monitor</i> detects a server in standby mode as being down.
770383	In multi-VDOM mode, nothing is exported to the NetFlow collector.
777231	<i>Dashboard > FortiView Traffic Shaping</i> page sometimes displays an undefined traffic shaper. This is cosmetic and does not impact functionality.
781144	On the <i>Edit Virtual Server</i> dialog under <i>Policy & Objects > Virtual Servers</i> , a <i>Duplicate entry found</i> error is displayed for the <i>Virtual server IP</i> and <i>Virtual server port</i> fields when there are no duplicate entries.
791735	The number of sessions in <code>session_count</code> does not match the output from <code>diagnose sys session full-stat</code> .
794648	Cannot set <code>src-vendor-mac</code> in policy. The <code>src-vendor-mac</code> policy setting is not lost after upgrading from 7.0.5 and is still in the <code>iprope</code> .
794901	Unable to create a <code>geography</code> type address object and get a <code>Can not be geography address when it is a member of addrgrp used by ipsec_tunnel! error</code> .
797017	The FortiGate does not refresh the <code>iprope</code> group for central SNAT policies after moving a newly created SNAT policy.
797318	NAT64 is not forwarding traffic to the destination IP.
798587	NGFW security policy is missing <code>internet-service6</code> and <code>internet-service6-src</code> options.
801483	Packet drops noticed in the network when FortiGate is running 7.2.0 GA.
802834	On the <i>Traffic Shaping > Traffic Shapers</i> tab, the <i>Bandwidth Utilization</i> column indicates zero traffic when there is traffic present.

Bug ID	Description
803270	Unexpected value for <code>session_count</code> appears.
806113	The <i>Traffic Shaping Policies</i> edit dialog shows configured reverse shapers as disabled. This is a cosmetic issue and the reverse shaper is configured as defined.
806904	IPv6 source with the same 32-bit prefix always NATs to the same IPv4 address.
820622	IPS engine crashes in NGFW policy mode with <code>internet-service-name</code> in a security policy.

FortiView

Bug ID	Description
787886	The tooltip for the <i>Bandwidth</i> column always displays the receiving bandwidth as zero on the <i>Dashboard > FortiView Traffic Shaping</i> page.
804177	When setting the time period to <i>now</i> filter, the table cannot be filtered by policy type.
811095	Threat type <i>N/A - Static URL Filter</i> is showing on sources that do not have the URL filter enabled.
819924	Information disappears after some time on the FortiView pages.

GUI

Bug ID	Description
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI <i>Forward Traffic</i> log page can take time to load if there is no specific filter for the time range.
740508	Bandwidth widget shows incorrect traffic on FG-40F.
741745	On certain pages, the loading spinner in the GUI is slow to load, and the page remains blank for a long time.
746618	Export port link status is not correct on tenant VDOM <i>FortiSwitch Ports</i> page.
750727	Log viewer negate filter does not work as expected for <i>Application Name</i> column.
774159	Signature not found in IPS database message when editing the IPS profile from the policy.
778844	<i>Dashboard</i> and <i>Managed FortiAPs</i> pages can take a long time to load when there are over 1000 FortiAPs configured.
781310	<i>Policy & Objects > DNAT & Virtual IPs</i> page can take more than 30 seconds to load if there are more than 25 thousand virtual IPs.
787550	HTTPSD daemon crashes frequently with <code>signal 6 (aborted)</code> at <code>api_v2_page_result</code> .

Bug ID	Description
787565	When logged in as guest management administrator, the custom image shows as empty on the user information printout.
792045	FortiGate failed to view matched endpoints after viewing it successfully several times.
798161	<i>System > Certificates</i> page keeps spinning when trying to access it from Safari.
799160	<i>Modem 1 Health</i> is incorrectly displayed as <i>Disconnected</i> in the <i>Diagnostics and Tools</i> pane of the <i>FortiExtenders</i> page.
800632	Search bar on <i>Addresses</i> page does not complete loading and return a result when format is <IP>-<number>.
800959	CPU usage is visible in the <i>Sessions</i> widget when it should not appear there.
802292	Logs sourced from FortiAnalyzer Big Data show the incorrect time.
806218	<code>GetNode</code> exiting due to uncaught error and <code>/tmp/admin_server.crt</code> errors in the crash log when rebooting.
810225	An <i>undefined</i> error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
821606	Unable to change the member order for SD-WAN rules in the GUI.
821734	<i>Log & Report > Forward Traffic</i> logs do not show the <i>Policy ID</i> if there is no <i>Policy Name</i> .
822991	On the <i>Log & Report > Forward Traffic</i> page, using the filter <i>Result : Deny(all)</i> does not work as expected.

HA

Bug ID	Description
722703	ISDB is not updating; last update attempt is stuck at an older date.
734040	Need a way for FortiManager to retrieve an HA-specific configuration of a secondary device through the primary device.
744033	HA <code>out-of-sync</code> messages appear in logs instead of <code>sync</code> messages when the FortiGate is in synchronization.
750087	Multicast convergence on HA failover.
750978	Interface link status of HA members go down when <code>cfg-revert</code> tries to reboot post <code>cfg-revert-timeout</code> .
779180	FGSP does not synchronize the <code>helper-pmap</code> expectation session.
779587	When an authentication log on length is longer than the <code>hasync</code> packet length and when there is a large number of logons, <code>hasync</code> is busy.

Bug ID	Description
781463	FortiGate does not respond to ARP request for <code>management-ip</code> on interface if the interface IP is changed.
782734	Cluster is out-of-sync due to switch controller managed switch checksum mismatch.
786592	Failure in self-pinging towards the management IP.
794707	Get invalid IP address when creating a firewall object in the CLI; it synchronized to the secondary in FGSP <code>standalone-config-sync</code> .
799659	Unusually large uptime and HA behavior occurs.
799765	Multicast is failing after HA failover.
801872	Unexpected HA failover on AWS A-P cluster when <code>ipsec-soft-dec-async</code> is enabled.
803354	After HA-AP failover, the FortiExtender WAN interface of the new primary cannot get the LTE IP address from FortiExtender.
803697	The <code>ha-mgmt-interface</code> stops using the configured <code>gateway6</code> .
805663	After upgrading, rebooting the primary in HA (A-A) results in unusually high bandwidth utilization on redundant interfaces.
806660	Internet service database object cannot be synchronized to the secondary unit after a FortiGuard update.
807322	AWS HA does not update the prefix list in the route table.
810175	<code>set admin-restrict-local</code> is not working for SSH.
812090	FGCP with in-band management mode does not send logs to newly added syslog server after being switched from out-of-band.
816883	High CPU usage on secondary device, and CPU lacks the AVX feature needed to load <code>libdpdk.so</code> .
817942	Secondary cluster member's iprope traffic statistics are not updated to the original primary after an A-P HA failover.

Hyperscale

Bug ID	Description
810025	Using EIF to support hairpinning does not work for NAT64 sessions.
812844	Default static route does not work well for hyperscale VDOM.

Intrusion Prevention

Bug ID	Description
698247	Flow mode web filter <code>ovrd</code> crashes and socket leaks in IPS daemon.
771000	High CPU in all cores with device running with one interface set as a one-arm sniffer.
779377	IPS fails to load a configuration if an NGFW policy uses the unrated category group or category of 0.
809691	High CPU usage on IPS engine when certain flow-based policies are active.
813998	IPv6 static routes are not generated for IP-based URL entries in one-arm IPS URL filtering solution.

IPsec VPN

Bug ID	Description
636602	Tunnel to spoke is down on hub after enabling FortiClient access.
765868	The packets did not pass through QTM, and SYN packets bypass the IPsec tunnel once traffic is offloaded. Affected platforms: NP7 models.
771935	Offloaded transit ESP is dropped in one direction until session is deleted.
773221	Traffic that goes through IPsec based on a loopback interface cannot be offloaded.
775011	In VPN peering using IKEv2, the signature and <code>aes256-sha256</code> proposals fail between the FortiGates and Palo Alto firewalls.
781403	IKE is consuming excessive memory.
787949	FortiGate sends duplicate SNMP traps if the tunnel is brought down on the local side.
790486	Support IPsec FGSP per tunnel failover.
793863	File downloads over L2TP IPsec VPN failed when using the VIP mapped to the internal server.
796546	IPv6 traffic through IPsec tunnel from learned BGP routes is not forwarding to Prisma Cloud provider.
798709	Shortcut fails to be triggered by interested traffic.
803010	The <code>vpn-id-ipip</code> encapsulated IPsec tunnel with NPU offloading cannot be reached by IPv6.
803336	VPN certificate private key changes on SCEP renewal.
803686	Tooltip in <i>Dashboard > Network IPsec</i> widget only displays one address for the local and remote addresses of the phase 2 selector.
810988	GUI does not allow IP overlap for a tunnel interface when <code>allow-subnet-overlap</code> is enabled (CLI allows it).
814366	There are no incoming ESP packets from the hub to spoke after upgrading.
815969	Cannot apply dialup IPsec VPN settings modifications in the GUI when <code>net-device</code> is disabled.

Log & Report

Bug ID	Description
692237	FortiOS is truncating the group field to 35 characters in traffic logs.
699019	The source IP under <code>config log fortiguard setting</code> is not respected.
740157	Event log is missing when the FortiGate Cloud Sandbox server is connected, disconnected, or switched.
769300	Traffic denied by security policy (NGFW policy-based mode) is shown as <code>action="accept"</code> in the traffic log.
770352	On the <i>Log & Report > Forward Traffic</i> page, filters applied to an interface name with a comma (,) do not show the correct filtered results for that interface.
781357	Add upgrade code for using free-style filter in miglogd for FortiOS 7.0 and later.
788724	The secondary FortiGate did not send the logs to the syslog server (<code>sendmmsg</code> failed to send data).
789459	Empty log <i>Summary</i> tab for <i>System Events</i> and <i>Security Events</i> pages.
790893	Free-style filter for UTM logs does not work when <code>set forward-traffic</code> is disabled.
795595	<i>Date/Time</i> filter changes after setting the time.
797789	FortiGate goes into conserve mode because fgtlogd occupies too much memory.
803262	Anti-spam logs are empty when the log source is FortiCloud (adding a time filter may return a result).
806914	<code>RADVD unloaded interface</code> message appears in system event log when changing a configuration on the FortiGate.
807661	In a FortiAnalyzer with lots of logs, the log view shows <i>no result</i> if the user scrolls down to the bottom of the list.
814427	FortiGate error in FortiAnalyzer connectivity test on secondary device after upgrade.
815150	Negating a range or subnet does not work in the GUI log display.

Proxy

Bug ID	Description
678815	WAD crashes with signal 11 if the client sends a client hello containing a key share that does not match the key share that the server prefers.
760471	WAD crashes and there is high memory after upgrading.

Bug ID	Description
766158	Video filter FortiGuard category takes precedence over allowed channel ID exception in the same category.
768278	WAD crashes frequently, authentication stops, and firewall freezes once proxy policy changes are pushed out.
781161	WAD has signal 11 crash due to invalid reading after freeing WAD user information daemon.
785927	Unexpected behavior in WAD when multiple DHCP servers are configured.
786939	The <code>scan-botnet-connections</code> block setting does not work for TCP:443 with proxy-based inspection.
789703	WAD continually crashing at signal 11.
791662	FortiGate is silently dropping server hello in TLS negotiation.
792505	Memory leak identified for WAD worker <code>dnsproxy_conn</code> causing conserve mode.
793651	An expired certificate can be chosen when creating an SSL/SSH profile for deep inspection.
795321	WAD crash signal 11 and unit goes into conserve mode.
796910	Application wad crash (<code>Segmentation fault</code>), which is the first crash in a series.
800125	Even if the policy is set to deny FTP_PUT, file uploads are permitted when the UTM feature is enabled.
800436	In proxy inspection, IPS packet logging does not work as expected with HTTPS.
802935	FortiGate cannot block a virus file when using the HTTP PATCH upload method.
803136	<code>thumbnailPhoto</code> files are saved in the memory disk with the incorrect hash name.
803260	Memory increase suddenly and is not released until rebooting.
803380	Device is consuming high memory and going in conserve mode, possible due to a WAD memory leak.
805808	In proxy inspection mode with AV enabled, TCP traffic is dropped after a while.
807332	WAD does not forward the 302 HTTP redirect to the end client.
807431	File from AWS S3 fails to download with UTM, deep inspection, and proxy configured.
808072	When accessing a specific website using UTF8 content encoding (which is unexpected according to the RFC) the FortiGate blocks the traffic as an HTTP evasion when applying an AV profile with deep inspection.
809346	FTPS helper is not opening pinholes for expected traffic for non-standard ports.
811259	WAD memory leak occurs with IPS enabled.
815313	WAD crash occurred due to a certificate validation failure.
817750	WAD daemon keeps crashing when web proxy forward server group does not have a server list.
822039	WAD crash occurs on FG-61E, FG-101F, FG-61F, FG-200E, and FG-401E during stress testing.

Bug ID	Description
822271	Unable to access a website when deep inspection is enabled in a proxy policy.
823814	When ZTNA access proxy is configured with <code>set empty-cert-action accept-unmanageable</code> , users may receive an error loading the page when the client certificate is not properly processed.

Routing

Bug ID	Description
618684	When HA failover is performed to the other cluster member that is not able to reach the BFD neighbor, the BFD session is down as expected but the static route is present in the routing table.
704322	After configuring static routes on IPsec tunnels using the <i>Network > Static Routes</i> page, a warning icon appears. This is cosmetic and does not affect functionality.
720618	Passive health check is not report packet loss when it occurs in the network.
756955	Routing table does not reflect the new changes for the static route until the routing process is restarted when cmdbsrv and other processes take CPU resources upon every configuration change in devices with over ten thousand firewall policies.
769523	Multicast is not working in VRRP.
774136	VPN traffic is not being metered by DoS policy when using SD-WAN.
779113	A new route check to make sure the route is removed when the link monitor object fails on ARM based platforms.
787476	BGP <code>conditional-advertise</code> did not withdraw the route upon a condition state change.
787487	Default priority value in static route is set as 0, even though the range is 1- 65535 in transparent mode.
788793	Unable to receive BGP routes on redundant tunnel interfaces.
795213	On the <i>Network > SD-WAN</i> page, adding a named static route to an SD-WAN zone creates a default blackhole route.
796070	Incorrect SD-WAN kernel routes are used on the secondary device.
796409	GUI pages related to SD-WAN rules and performance SLA take 15 to 20 seconds to load.
797530	SD-WAN health check event log shows the incorrect protocol.
797590	GRE tunnel configured using a loopback interface is not working after changing the interface back and forth.
798245	ICMP traffic is using the incorrect VRF.
799969	BGP neighbor <code>advertisement-interval</code> can be set to 0 but not take effect in ZebOS.
805285	SIP-RTP fails after a route or interface change.

Bug ID	Description
806939	Routing issue with ADVPN and SD-WAN if IPsec aggregate interfaces are configured.
807635	BGP routes hit the wrong route map.
808840	After cloning a static route, the URL gets stuck with "clone=true".
809321	IS-IS LSP packets do not include the checksum and the authentication key ([Checksum: [missing]], [Checksum Status: Not present] and authentication "hmac-md5 (54), message digest]).
812982	SD-WAN performance SLAs on a dialup IPsec VPN tunnel do not work as expected.
816582	Connected subnet in VRF, other than VRF 0, gets an RPF failure after HA failover.
817670	IPv6 route redistribution metric value is not taking effect.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
741084	Entry-level FortiGate with Security Fabric enabled for 30 or more downstream FortiGates can go into conserve mode when loading the physical or logical topology pages, or running security rating reports.
753742	Add distributed security rating and topology reports.
778511	PPPoE interface is unable to accept Fabric connections.
782518	Threat feeds are showing that the connection status has not started when it should be connected.
788543	Topology tree shows <i>No connection</i> or <i>Unauthorized</i> for FortiAnalyzer while sending log data to FortiAnalyzer.
791324	<i>Test Automation Stitch</i> function only works on the root FortiGate, and is not working on the downstream FortiGate.
795687	On the <i>Fabric Management</i> page, some managed FortiSwitches are not shown.
798795	API that registers appliances to the Fabric stopped working.
799832	GCP bearer token is too long for the header in a <code>google-cloud-function</code> automation action.
801048	During the FortiOS initialization process, there is a small chance that other services using UDP take the specific port that caused csfd initialization to fail.
803600	Automation stitch for a scheduled backup is not working.
807967	Add reliable message for creating event logs on upstream device for use by Report Runner.
815984	Azure SDN connector has a 403 error when the AZD restarts.

SSL VPN

Bug ID	Description
486837	SSL VPN with external DHCP servers is not working.
616896	Link in SSL VPN portal to FortiClient iOS redirects to legacy FortiClient 6.0 rather than the latest 6.2.
626311	SSL VPN users are remaining logged on past the <code>auth-timeout</code> value.
676278	Custom host check AV and firewall for macOS fails for FortiClient SSL VPN.
677031	SSL VPN web mode does not rewrite playback URLs on the internal FileMaker WebDirect portal.
697142	SharePoint server (de***.sc***.gov.sa) is not working on web-based VPN.
757726	SSL VPN web portal does not serve updated certificate.
763611	Slow upload speed on SSL VPN dual-stack configuration.
767832	After upgrading from 6.4.7 to 7.0.1, the Num Lock key is turned off on the SSL VPN webpage.
767869	SCADA portal will not fully load with SSL VPN web bookmark.
768323	Certain websites do not load properly in SSL VPN web mode.
768983	SSL VPN web mode access to the FortiGate GUI is slow after upgrading.
778034	FortiGate GUI in SSL VPN web mode is very slow.
780305	SSL VPN web mode is unable to redirect from port 62843 to port 8443.
780765	High CPU usage in SSL VPN using libssh2.
781581	Customer internal website is not shown correctly in SSL VPN web mode.
784887	A blank page appears after logging in to an SSL VPN bookmark.
787978	Unable to load NFMT routing display through SSL VPN web mode.
789117	SSL VPN web mode RDP bookmark always asks for credentials.
789267	SSO SSL VPN web mode user cannot connect to RDP intermittently.
789642	Unable to load Grafana application through SSL VPN web mode.
791700	SSL VPN crashes and disconnects users at the same time.
792075	SSL VPN web portal does not load internal e-learning website content.
792944	Internal redirect webpage is not working in SSL VPN web mode.
794800	SSL VPN /remote/logoutok screen loads in basic text.
794820	Slow performance to manage FortiGate through the bookmark configured in SSL VPN web mode.
795730	Non-Google CAPTCHA cannot be displayed in SSL VPN web mode.
796768	SSL VPN RDP is unable to connect to load-balanced VMs.

Bug ID	Description
797136, 797139	Internal site does not load completely using SSL VPN web mode bookmark.
799308	SSL VPN bookmark is not working.
799780	Website is not loading in SSL VPN web mode.
800751	Unable to download files over 2 GB to and from an SMB file share using SSL VPN web mode.
801308	FortiGuard should only provide an installer for FortiClient VPN, instead of the full FortiClient version.
801588	After Kronos (third-party) update from 8.1.3 to 8.1.13, SSL VPN web portal users get a blank page after logging in successfully.
802379	SSL VPN has memory leaks and crashes.
803576	Comments in front of <code><html></code> tag are not handled well in HTML file in SSL VPN web mode.
803622	High CPU in SSL VPN once SAML is used with FortiAuthenticator and an LDAP server.
805922	Unable to configure <code>ssl.root</code> as the <code>associated-interface</code> in a firewall address.
806143	JavaScript error in SSL VPN web mode.
807268	Many SSL VPN users are disconnected periodically, and <code>sslvpn</code> crashes.
808569	<code>sslvpn</code> crashes when no certificate is specified.
808634	SSL VPN daemon sometimes could not be recovered, even when setting the server certificate back from empty to a specific certificate.
809209	SSL VPN process memory leak is causing the FortiGate to enter conserve mode over a short period of time.
809473	When <code>sslvpn</code> debugs are enabled, the SSL VPN process crashes more often.
810715	Web application is not loading in the SSL VPN web mode.
811007	The auto-generated URL on the <i>VPN > SSL-VPN Settings</i> page shows the management IP of the FortiGate instead of the SSL VPN interface port IP as defined on the <i>VPN > SSL-VPN Realms</i> page when a realm is created.
812006	The PROD-MDN-WS1 SSL VPN portal is not loading properly, and cannot navigate within the page.
814040	SSL VPN bookmark configuration is added automatically after client logs in to web mode.
814708	The same SAML user failed to establish a tunnel when a stale web session exists with <code>limit-user-logins</code> enabled.
816716	<code>sslvpn</code> crashed when deleting a VLAN interface.
816881	TX packet loss on <code>ssl.root</code> interface.
817843	Logging out of SSL VPN tunnel mode does not clear the authenticated list.
826582	SSH via SSL VPN web mode does not work for some SSH servers.

Switch Controller

Bug ID	Description
774441	FortiLink topology only displays partially.
794026	The number of quarantined MAC addresses is stuck at 256 due to table size limitations on the FortiGate.
799860	FortiSwitch online/offline status is not consistent between the CLI and SNMP.
803307	The <i>Enable STP</i> security control description should be reworded to mention that Edge ports should have STP enabled once the network topology is stable.
805154	Switch controller preconfiguration of FortiSwitch 108F-POE is incorrect.
810550	When <code>config-sync</code> runs between a FortiGate and a managed FortiSwitch, RSPAN interfaces get deleted and re-added, which causes syslog errors from FortiSwitch.

System

Bug ID	Description
540389	Remote administrator password renewal shows remote token instead of new password (CLI and GUI).
716250	Incorrect bandwidth utilization traffic widget for VLAN interface based on LACP interface.
725273	<code>application newcli crashed with *** signal 11 (Segmentation fault) received ***.</code>
734912	When VDOMs are enabled, changing system settings causes the GUI to display a failure to save message.
736144	AirCard 340U LTE Modem does not work.
743831	When global daylight saving time (DST) is disabled, the system time in the GUI still shows the time with DST.
753912	FortiGate calculates faulty FDS weight with DST enabled.
756139	When split port is enabled on four 10 GB ports, only one LACP port is up, and the other ports do not send/receive the LACP PDU.
758490	The value of the <code>extra-init</code> parameter under <code>config system lte-modem</code> is not passed to the modem after rebooting the device.
761971	AirCard 340U LTE modem does not work on FG-61F.
764483	After restoring the VDOM configuration, <code>Interface <VLAN> not found in the list!</code> is present for VLANs on the aggregate interface.

Bug ID	Description
766058	FortiGate central management is configured on the backup mode ADOM, and any changes done on the FortiGate are not recorded in the FortiManager.
771331	Incorrect bandwidth utilization traffic widget for VLAN interface on NP6 platforms.
773829	Get /bin/cid crash when cid.tar.gz cannot be unpacked.
781960	A dhcpd crash log occurs.
782392	ICMP traceroute with more than one probe is not working, and drops are seen on NP6 platforms.
783241	Manually updating internet-service database may fail because there is no check of which internet-service database is being updated.
783939	IPv4 session is flushed after creating a new VDOM.
786255	Cached topology reports causes the FortiGate to run out of flash storage on entry-level models.
786998	When enabling the decrypted-traffic-mirror option on a VXLAN interface, the collector device will get a TCP Out-Of-Order packet.
787557	Sudo command is not working inconsistently.
787595	FFDB cannot be updated with exec update-now or execute internet-service refresh after upgrading the firmware in a large configuration.
789203	High memory usage due to DoT leak at ssl.port_1way_client_dox leak\wad_m_dot_conn leak\sni leak when the DoX server is 8.8.8.8.
790656	DNS fails to correctly resolve hosts using the DNS database.
792544	A request is made to the remote authentication server before checking trusthost.
793864	Repeated FortiDDNS failed messages are in the system event logs output.
796094	Egress traffic on EMAC VLAN is using base MAC address instead.
796398	BPDUs packets are blocked even though STF forwarding is enabled on FG-800D in transparent mode (UTP and SFP).
797428	SNMP status for NPU is not available on NP6xlite.
799255	Any configuration changes on FG-2601F causes cmbdr crash with signal 6 and traffic to stop flowing.
799487	The debug zone uses over 400 MB of RAM.
800294	Interface migration wizard fails to migrate interfaces when VLANs have dependencies within dependencies.
800295	NTP server has intermittent unresolvable logs after upgrading to 6.4.
801053	FG-1800F existing hardware switch configuration fails after upgrading.
801474	DHCP IP lease is flushed within the lease time.
801738	Kernel panic occurs on FG-2610F when collecting debug flow information.
802917	PPPoE virtual tunnel drops traffic after logon credentials are changed.

Bug ID	Description
805412	DHCPv6 authentication option offer is not accepted from the server.
805644	Trunk port is removed from the VLAN switch after rebooting.
807947	Unable to create new interface and VDOM link with names that contain spaces.
810104	Under certain trace condition scenarios, a kernel panic may be triggered on new kernel platforms after failover with HTTP CCS followed by SIP64 traffic.
810466	EHP and HRX drop on NP6 FortiGate, causing low throughput.
810583	Running <code>diagnose hardware deviceinfo psu</code> shows the incorrect PSU slot.
810622	Message regarding VDOM names longer than 11 characters is shown when <code>set long-vdom-name</code> is enabled.
811449	New DNS system servers with DoT enabled, applying a DNS filter to the FortiGate DNS server fails.
812499	When traffic gets offloaded, an incorrect MAC address is used as a source.
813223	Random kernel panic occurs when the following IPsec VPN phase 2 interface configuration is used: <pre> config vpn ipsec phase2-interface edit <name> set keylife-type both set keylifeseconds 28800 set keylifekbs 4608000 next end </pre>
813606	DHCP relay offers to iPhones is blocked by the FortiGate.
814002	FortiGate may enter kernel panic in HA environment and when sending multicast traffic on new kernel platforms.
815360	NP7 platforms may encounter a kernel panic when deleting more than two hardware switches at the same time.
816278	Memory increase due to iked process.
816823	NP6xLite test failed when running <code>diagnose hardware test pci</code> .
818461	When an aggregate is created after all VLANs and added to a software switch, all VLANs are lost after rebooting.
818811	NTurbo crash occurs when offloading SSL mirror traffic.
821773	Manual license for air-gap environments is lost after rebooting the FortiGate.

Upgrade

Bug ID	Description
792831	[2062] fap_fsw_lst_req: buf of https is too small: 853 debug message appears in console when upgrading to certain builds.
803171	Upgrade takes longer than expected and get synchronization error caused by PPP when HA upgrades.

User & Authentication

Bug ID	Description
738846	FAS ends up in endless loop while synchronizing with LDAP when a special character (,) is part of a username.
754725	After updating the FSSO DC agent to version 5.0.0301, the DC agent keeps crashing on Windows 2012 R2 and 2016, which causes lsass.exe to reboot.
760740	REVERSE_INULL found in WanOpt explicit proxy, wad_user_info.c:wad_group_info_cache_free.
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.
782158	The ç character is not accepted by an LDAPS password change.
790941	When logged in with an administrator profile using a wildcard RADIUS user, creating a new dashboard widgets fails.
792924	Incorrect captive portal page certificate is used after upgrading.
804133	The diagnose test guest del <group_name> <user_ID> command does not work after upgrading.
808884	Device information is not fully detected on NP7.
810033	The samld process is killed if the SP certificate set has an ECC 384-bit public key.
813355	Additional information from user ID login should be displayed.
813407	Captive portal authentication with RADIUS user group truncates the token code to eight characters.
813987	No traffic is generated when creating an ACME certificate that uses a domain name with an uppercase letter.

VM

Bug ID	Description
764392	Incorrect VMDK file size in the OVF file for hw13 and hw15.
782073	IBM HA is unable to fail over route properly when route table has a delegate VPC route.
786278	Bandwidth usage is not shown when DPDK is enabled.
799536	Data partition is almost full on FG-VM64 platforms.
800473	FG-VM64 deployed with 6.4 loses configuration and license after upgrading to 7.2.1 (no issue if deployed with 7.0).
800935	ESXi VLAN interface based on LACP does not work.
803219	Azure SDN connector might miss dynamic IP addresses due to only the first page of the network interface being processed.
809963	Get cmdbsvr crash after concurrent performance test on FG-KVM32.

VoIP

Bug ID	Description
794517	VoIP daemon memory leak occurs when the following conditions are met: <ul style="list-style-type: none">• The SIP call is on top of the IPsec tunnel.• The call fails before the setup completes (session gets closed in a state earlier than <code>VOIP_SESSION_STATE_RUNNING</code>).

WAN Optimization

Bug ID	Description
804662	WANOpt tunnels are not established for traffic matching the profile.

Web Application Firewall

Bug ID	Description
795554	Inspecting all ports in an SSL/SSH inspection profile does not work with the WAF profile.

Web Filter

Bug ID	Description
743195	Disclaimer module does not load and breaks the website.
786448	Web filtering with WISP functionality is intermittent in flow mode.
798557	When a new URL filter entry is created and the list is re-ordered, the list position is not maintained.
801792	IPS daemon has socket FD leaks.

WiFi Controller

Bug ID	Description
790367	FWF-60F has kernel panic and reboots by itself every few hours.
795821	<p>The new <code>sae-h2e-only</code> WPA3-SAE SSID setting may cause a backward compatibility issue where some Wi-Fi devices may not associate with managed FortiAP units running previous firmware versions:</p> <ul style="list-style-type: none"> FortiAP 6.4.8, 7.0.5, 7.2.0 and earlier FortiAP-W2 6.4.8, 7.0.5, 7.2.0 and earlier FortiAP-S 6.4.8 and earlier FortiAP-U 6.2.4 and earlier <p>Solution:</p> <ul style="list-style-type: none"> FortiAP and FortiAP-W2 units may be upgraded to 7.2.1 if applicable FortiAP and FortiAP-W2 issue will be fixed in later 6.4 and 7.0 releases FortiAP-S issue will be fixed in a later 6.4 release FortiAP-U units may be upgraded to 6.2.5
796036	Manual quarantine for wireless client connected to SSID on multi-VDOM with <code>wtp-share</code> does not work.
807605	FortiOS exhibits segmentation fault on hostapd on the secondary controller configured in HA.

ZTNA

Bug ID	Description
792829	WAD re-challenges user authentication upon HA failover.
797433	WAD treats ZTNA SAML URL with multiple query characters as invalid and closes.
799530	Found wad crash at <code>wad_sched.c</code> upon device tag matching.

Bug ID	Description
799759	Applying a ZTNA rule in the GUI removes configured IP pools.
802715	ZTNA failed to match the policy when a tag is found for an endpoint in the EMS response.
808178	After upgrading from 7.0 to 7.2, the <code>client-cert</code> setting under <code>config firewall access-proxy</code> changed from <code>disable</code> to <code>enable</code> .

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
789153	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-38378
795784	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-26122
797229	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-27491
800259	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-29055
803283	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-47536
810989	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-38380
811492	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-35842
819640	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-30307
825695	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2022-35843
863856	FortiOS 7.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-29175

Known issues

The following issues have been identified in version 7.2.1. To inquire about a particular bug or report a bug, please contact [Customer Service & Support](#).

Anti Virus

Bug ID	Description
869398	FortiGate sends too many unnecessary requests to FortiSandbox and causes high resource usage.

Explicit Proxy

Bug ID	Description
803228	When converting an explicit proxy session to SSL redirect, traffic may be interrupted inadvertently in some situations.

GUI

Bug ID	Description
677806	On the <i>Network > Interfaces</i> page when VDOM mode is enabled, the <i>Global</i> view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
719476	FortiLink NAC matched device is displayed in the CLI but not in the GUI under <i>WiFi & Switch Controller > NAC Policies > View Matched Devices</i> .
825598	The FortiGate may display a false alarm message <code>TypeError [ERR_INVALID_URL]: Invalid URL</code> in the crashlog for the node process. This error does not affect the operation of the GUI.
833306	Intermittent error, <i>Failed to retrieve FortiView data</i> , appears on real-time <i>FortiView Sources</i> and <i>FortiView Destination</i> monitor pages.
835089	Unable to move SD-WAN rule ordering in the GUI (FortiOS 7.2.1). Workaround: move the SD-WAN rule ordering in the CLI.

HA

Bug ID	Description
823687	A cluster is repeatedly out-of sync due to external files (SSLVPN_AUTH_GROUPS) when there are frequent user logins and logouts.

Hyperscale

Bug ID	Description
824071	ECMP does not load balance IPv6 traffic between two routes in a multi-VDOM setup.
824733	IPv6 traffic continues to pass through a multi-VDOM setup, even when the static route is deleted.

IPsec VPN

Bug ID	Description
763205	IKE crashes after HA failover when the <code>enforce-unique-id</code> option is enabled.

Proxy

Bug ID	Description
799237	WAD crash occurs when TLS/SSL renegotiation encounters an error.

Routing

Bug ID	Description
833399	Static routes are incorrectly added to the routing table, even if the IPsec tunnel type is static.

Security Fabric

Bug ID	Description
825291	Security rating test for <i>FortiAnalyzer</i> fails when connected to FortiAnalyzer Cloud.

SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.
819754	Multiple DNS suffixes cannot be set for the SSL VPN portal.

System

Bug ID	Description
798303	The threshold for conserve mode is lowered.
832429	Random kernel panic may occur due to an incorrect address calculation for the internet service entry's IP range.
837730	Trusted hosts are not working correctly in FortiOS 7.2.1.
847077	Can't find xitem. Drop the response. error appears for DHCP OFFER packets in the DHCP relay debug.

User & Authentication

Bug ID	Description
825505	<p>After a few days, some devices are not displayed in the <i>Users & Devices > Device Inventory</i> widget and <i>WiFi & Switch Controller > FortiSwitch Ports</i> page's <i>Device Information</i> column due to a mismatch in the device count between the following commands.</p> <ul style="list-style-type: none">• <code>diagnose user device list</code>• <code>diagnose user device stats</code>• <code>diagnose user-device-store device memory list</code> <p>Workaround: restart the WAD process or reboot the FortiGate to recover the device count for the user device store list.</p>

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

ZTNA

Bug ID	Description
832508	<p>The EMS tag name (defined in the EMS server's <i>Zero Trust Tagging Rules</i>) format changed in 7.2.1 from <code>FCTEMS<serial_number>_<tag_name></code> to <code>EMS<id>_ZTNA_<tag_name></code>.</p> <p>After upgrading from 7.2.0 to 7.2.1, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled.</p> <p>Workaround: unset the <code>ztna-ems-tag</code> in the ZTNA firewall proxy policy, and then set it again.</p>

Built-in AV Engine

AV Engine 6.00276 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

Built-in IPS Engine

IPS Engine 7.00234 is released as the built-in IPS Engine. Refer to the [IPS Engine Release Notes](#) for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
 - XVA (recommended)
 - VHD
 - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.



www.fortinet.com

Copyright© 2024 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 Chief Legal Officer, 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.