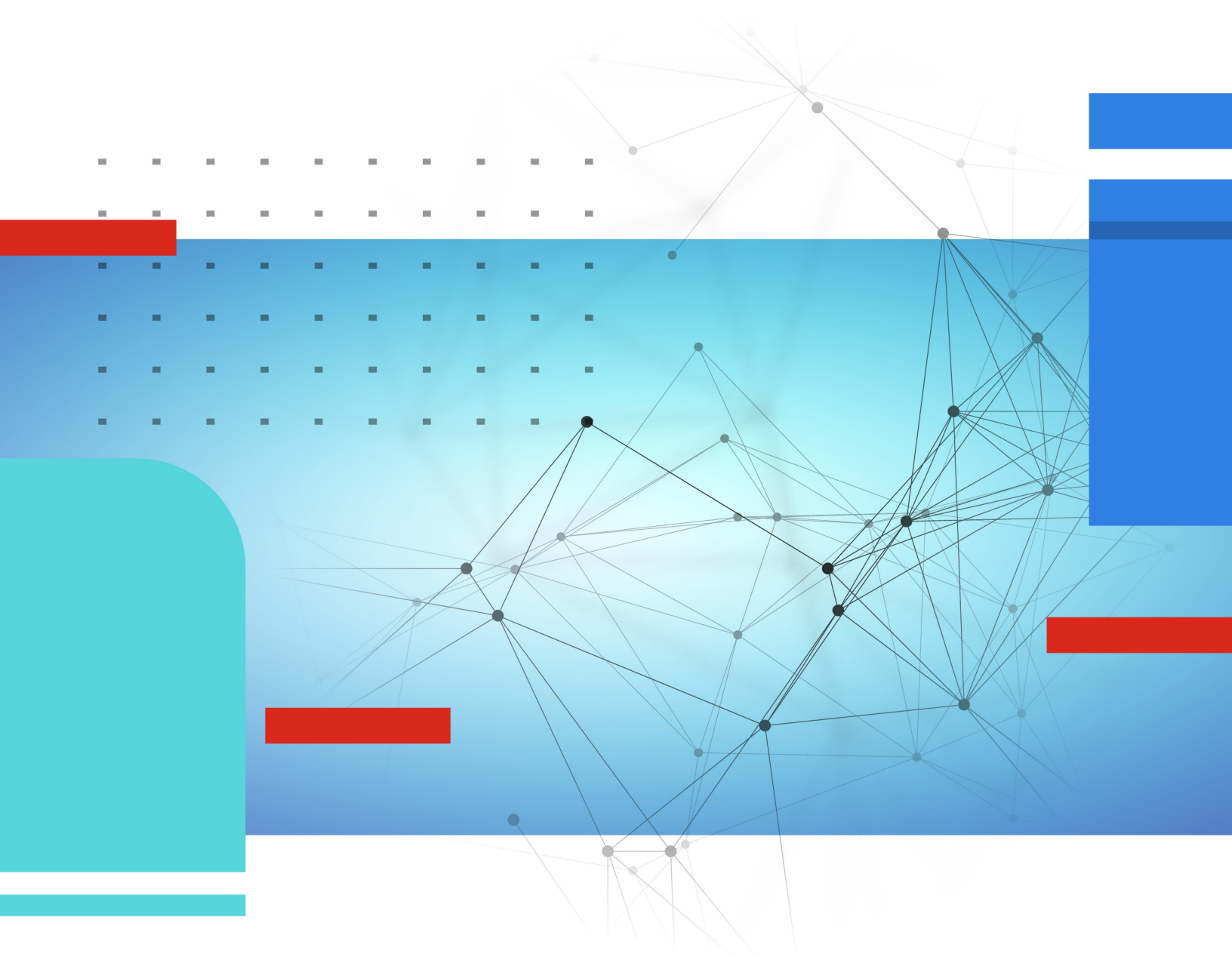




Release Notes

FortiOS 7.6.1



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



November 28, 2024

FortiOS 7.6.1 Release Notes

01-761-1084726-20241128

TABLE OF CONTENTS

Change Log	6
Introduction and supported models	7
Supported models	7
FortiGate 6000 and 7000 support	7
Special notices	8
FortiManager support for updated FortiOS private data encryption key	8
Hyperscale incompatibilities and limitations	9
FortiGate 6000 and 7000 incompatibilities and limitations	9
SSL VPN removed from 2GB RAM models for tunnel and web mode	9
2 GB RAM FortiGate models no longer support FortiOS proxy-related features	10
FortiGate VM memory and upgrade	10
Hyperscale NP7 hardware limitation	10
GUI access conflict with IPSec TCP tunnel on the same interface	11
Changes in CLI	12
Changes in GUI behavior	13
Changes in default behavior	14
Changes in default values	15
Changes in table size	16
New features or enhancements	17
Cloud	17
LAN Edge	18
Network	19
Operational Technology	21
Policy & Objects	21
SD-WAN	23
Security Fabric	25
Security Profiles	25
System	26
WiFi Controller	26
ZTNA	27
Upgrade information	29
Fortinet Security Fabric upgrade	29
Downgrading to previous firmware versions	31
Firmware image checksums	31
FortiGate 6000 and 7000 upgrade information	31
Default setting of cp-accel-mode is changed to none on 2GB memory models	32
Product integration and support	33
Virtualization environments	34
Language support	34
SSL VPN support	35

SSL VPN web mode	35
FortiExtender modem firmware compatibility	35
Resolved issues	38
Anti Spam	38
Anti Virus	38
Application Control	39
Data Loss Prevention	39
DNS Filter	39
Explicit Proxy	39
File Filter	40
Firewall	40
FortiGate 6000 and 7000 platforms	41
FortiView	42
GUI	42
HA	43
Hyperscale	44
ICAP	44
Intrusion Prevention	45
IPsec VPN	45
Log & Report	46
Proxy	47
REST API	48
Routing	49
Security Fabric	50
SSL VPN	51
Switch Controller	52
System	52
Upgrade	56
User & Authentication	56
VM	57
VoIP	58
Web Application Firewall	58
Web Filter	58
WiFi Controller	59
ZTNA	59
Common Vulnerabilities and Exposures	60
Known issues	61
New known issues	61
Hyperscale	61
Intrusion Prevention	61
Existing known issues	61
Endpoint Control	61
Firewall	62
FortiGate 6000 and 7000 platforms	62

FortiView	62
GUI	62
HA	63
Hyperscale	63
IPsec VPN	63
Log & Report	63
Proxy	64
REST API	64
Security Fabric	64
Switch Controller	64
System	64
Upgrade	65
User & Authentication	65
Web Filter	65
Built-in AV Engine	66
Built-in IPS Engine	67
Limitations	68
Citrix XenServer limitations	68
Open source XenServer limitations	68

Change Log

Date	Change Description
2024-11-28	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.6.1 build 3457.

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

Supported models

FortiOS 7.6.1 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60F, FG-61F, FG-70F, FG-71F, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60F, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, 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-XEN

FortiGate 6000 and 7000 support

FortiOS 7.6.1 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6001F, FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

- FortiManager support for updated FortiOS private data encryption key on page 8
- Hyperscale incompatibilities and limitations on page 9
- FortiGate 6000 and 7000 incompatibilities and limitations on page 9
- SSL VPN removed from 2GB RAM models for tunnel and web mode on page 9
- 2 GB RAM FortiGate models no longer support FortiOS proxy-related features on page 10
- FortiGate VM memory and upgrade on page 10
- Hyperscale NP7 hardware limitation on page 10
- GUI access conflict with IPSec TCP tunnel on the same interface on page 11

FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal private-data-encryption key. Instead administrators simply enable the command, and a random private-data-encryption key is generated.

Previous FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
12345678901234567890123456789abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
12345678901234567890123456789abc
Your private data encryption key is accepted.
```

New FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
Do you want to continue? (y/n)y
Private data encryption key generation succeeded!
```

FortiManager behavior

Support for the FortiGate private-data-encryption key by the Device Manager in FortiManager 7.6.2 and earlier is unchanged. It automatically detects the remote FortiGate private-data-encryption key status and prompts the

administrator to manually type the private key (see picture below). FortiManager 7.6.2 and earlier does not support the updated, random `private-data-encryption` key as the administrator will have no knowledge of the key generated in the FortiOS CLI command above. It will be supported in a later version of FortiManager.

Warning

The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

Status	Device Name	IP Address	Platform	Private Data Encryption K
?	FGVM02TM24009410	172.18.36.216	FortiGate-VM64	

1

Verify
Close

FortiOS upgrade behavior

If in FortiOS 7.4.5 or 7.6.0 the 32-digit hexadecimal private key is enabled, and then the FortiGate device is upgraded to 7.6.1, the 32-digit hexadecimal `private-data-encryption` key is preserved. As a result, FortiManager 7.6.2 and earlier is aware of the 32-digit hexadecimal `private-data-encryption` key and can continue to manage the FortiGate device. However, if the `private-data-encryption` key is enabled after an upgrade of FortiOS to 7.6.1, FortiManager 7.6.2 and earlier no longer can manage FortiGate devices running FortiOS 7.6.1.

Hyperscale incompatibilities and limitations

See [Hyperscale firewall incompatibilities and limitations](#) in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.6.1 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.6.1 features.

- [FortiGate 6000 incompatibilities and limitations](#)
- [FortiGate 7000E incompatibilities and limitations](#)
- [FortiGate 7000F incompatibilities and limitations](#)

SSL VPN removed from 2GB RAM models for tunnel and web mode

On FortiGate models with 2GB of RAM or below, the SSL VPN web and tunnel mode feature will no longer be available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See [SSL VPN to IPsec VPN Migration](#) for more information.



FortiGate models not listed above will continue to have SSL VPN web and tunnel mode support.

2 GB RAM FortiGate models no longer support FortiOS proxy-related features

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, starting from version 7.4.4, FortiOS no longer supports proxy-related features.

This change impacts the FortiGate 40F and 60F series devices, along with their variants. See [Proxy-related features no longer supported on FortiGate 2 GB RAM models](#) for more information.

FortiGate VM memory and upgrade

FortiGate virtual machines (VMs) are not constrained by memory size and will continue to support all available features after upgrading to FortiOS 7.6.0. However, it is recommended to setup VMs with at least 4 GB of RAM for optimal performance.

Hyperscale NP7 hardware limitation

Because of an NP7 hardware limitation, for CGN traffic accepted by a hyperscale firewall policy that includes an overload with port block allocation (overload PBA) IP Pool, only one block is allocated per client. The setting of the hyperscale firewall policy `cgn-resource-quota` option is ignored.

Because of this limitation, under certain rare conditions (for example, only a single server side IP address and port are being used for a large number of sessions), port allocation may fail even if the block usage of the client is less than its quota. In cases such as this, if the client has traffic towards some other servers or ports, additional port allocation can become successful. You can also work around this problem by increasing the IP Pool block size (`cgn-block-size`).

GUI access conflict with IPsec TCP tunnel on the same interface

In FortiOS version 7.6.1, the default IKE TCP port has been changed to port 443 on new deployments. See Bug ID 1051144 in [Changes in default values on page 15](#).

This may affect GUI access for interfaces bound to an IPsec tunnel in the scenario that the GUI admin port is also using port 443.

In case GUI connectivity is lost, connect to the FortiGate by:

1. Connecting from an interface that is not bound to an IPsec tunnel.
2. Connecting to the interface using SSH, if SSH is enabled.
3. Connecting to the FortiGate from console.

To ensure continued functionality, users are recommended to either:

- Choose an alternative interface for GUI access by configuring:

```
config system global
    set admin-sport <port>
end
```

- Customize the `ike-tcp-port` to a value other than 443:

```
config system settings
    set ike-tcp-port <port>
end
```


Changes in CLI

Bug ID	Description
974985	Before 7.6.0, the <code>adv-interval</code> accepted values from 1 to 255 seconds. Starting with FortiOS 7.6.0, <code>adv-interval</code> accepts values in milliseconds, ranging from 250 to 255000. This change allows for quicker VRRP failovers. For more information, see Configure the VRRP hello timer in milliseconds .
1009740	<p>Renamed the server-type setting's <code>iot-query</code> option to <code>vpatch-query</code>.</p> <pre>config system central-management config server-list edit <id> set server-type {update rating vpatch-query iot-collect} set server-address <x.x.x.x> next end end</pre>
1017835	<p>Application bandwidth tracking in the CLI has been relocated from the <code>system</code> to <code>global</code> settings. To enable application bandwidth tracking:</p> <pre>config system global set application-bandwidth-tracking enable end</pre>
1035072	<p>The options <code>empty-cert-action</code>, <code>user-agent-detect</code>, and <code>client-cert</code> have been removed from <code>system.access-proxy</code>. Instead, they are added to the following configuration commands:</p> <pre>config firewall access-proxy-virtual-host set empty-cert-action <action> user-agent-detect {enable disable} client-cert {enable disable} end config firewall vip set type access-proxy set empty-cert-action <action> user-agent-detect {enable disable} client-cert {enable disable} end</pre>

Changes in GUI behavior

Bug ID	Description
834860	Users are allowed to create a policy using IP or MAC addresses directly from the FortiView pages and Log Viewer. This feature streamlines the policy creation process, making it more efficient and user-friendly.
966534	GUI support for configuring SCIM client has been added under the <i>User & Authentication > SCIM Clients</i> page.
969758	Added GUI support for creating Internet Service Group. This allows users to create and manage Internet Service Groups more intuitively and efficiently, providing a more user-friendly experience.
976480	Added GUI support for creating local-in policies. This allows users to create local-in policies more intuitively and efficiently, providing a more user-friendly experience.
976976	In an IPsec dial-up VPN configuration using IKEv2, users can now configure Remote Gateway Match and security posture tags within the VPN tunnel configuration in the GUI.
987210	GUI Enhancement for Firewall Policy Management. Users have the option to apply logical and operations among various policy objects within the GUI, providing a more detailed level of control over the configuration of firewall policies.
988573	The Backup heartbeat interfaces option is added to the <i>System > HA</i> page.
1000836	FortiGate EMS connector settings now supports configuring FortiClient Cloud access key within the GUI.

Changes in default behavior

Bug ID	Description
1043962	<p>Auto Firmware Upgrade Control</p> <p>In FortiOS version 7.4.5 and later, the option to control automatic firmware upgrades has been updated. Previously, this option was enabled only on entry-level models and disabled by default on all other models, allowing users to manually control firmware upgrades. In version 7.4.5 and later, this option is now enabled by default on all FortiGate models, including FortiGate-VMs. This means the system will automatically upgrade to the latest firmware unless manually configured otherwise. If you prefer to manage firmware upgrades manually, please review and adjust the auto-upgrade settings according to your requirements.</p>
1061121	<p>Starting with FortiOS 7.6.1, the default neighbor detection method has been updated. Previously, the default method was FortiLink. With this release, the default neighbor detection method is now LLDP.</p>
1066082	<p>Starting with version 7.6.1, a password is required when setting up a new HA member. If upgrading from a previous version without an HA password, the system will skip the password check. However, any subsequent modifications to the system.ha settings will enforce the password check and require the HA password.</p> <hr/> <div><p>The password should be added across all cluster members and must be the same for all members.</p></div> <hr/> <p>To set the password:</p> <pre>config system ha set password <passwd> end</pre>
1091890	<p>The default behavior for the following manage- options will now be enabled. For users upgrading to 7.6.1, it will only be enabled if IPAM is currently disabled. If IPAM is enabled, existing configurations will remain unchanged to avoid disruptions.</p> <pre>config system ipam set status {enable disable} set manage-lan-addresses {enable disable} set manage-lan-extension-addresses {enable disable} set manage-ssid-addresses {enable disable} end</pre>

Changes in default values

Bug ID	Description
1051144	<p>Before FortiOS version 7.6.1, IPSec dialup VPN by default has <i>Auto</i> mode enabled where if UDP connection is blocked then the client connection will fallback to TCP using port 4500. Some environments may have TCP port 4500 blocked locally or by their ISP, therefore the default IPSec TCP IKE port is now changed to 443.</p> <p>Previous CLI Behavior</p> <pre>config system settings set ike-tcp-port 4500 end</pre> <p>New CLI Behavior</p> <pre>config system settings set ike-tcp-port 443 end</pre> <p>This change applies to new FortiGate configurations only. Upon upgrade, the old <code>ike-tcp-port</code> value will be retained.</p> <p>For information about possible conflict with GUI access on port 443, please see GUI access conflict with IPSec TCP tunnel on the same interface on page 11.</p>

Changes in table size

Bug ID	Description
1030001	On the 200-400 series FortiGates, increase the number of VDOMs from 10 to 25. On the 500-900 series FortiGates, increase the number of VDOMs from 10 to 50.
1042266	On high-end FortiGate models, increase the number of policy routes and policy routes6 from 2048 to 5000.
1059858	On entry-level FortiGate models, increase the number of firewall on-demand-sniffer to 6.
1064311	On 90xG FortiGate models, increase the number of firewall addresses and firewall addresses6 from 20000 to 40000.
1073677	On 90xG FortiGate models, increase the number of zones from 200 to 500.

New features or enhancements

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

Cloud

See [Public and private cloud](#) in the New Features Guide for more information.

Feature ID	Description
1007607	AzureSDN connectors support IPv6 address objects.
1029721	FortiOS Azure SDN connector moves private IP on the trusted NIC during A/P HA failover.
1031828	<p>Introduce GraphQL bulk query to FortiGate on Azure to reduce the number of API queries going out to Azure and as a result, reducing the time taken to resolve SDN connector Dynamic objects in a large environment.</p> <p>Configure the <code>FGT_VM64_AZURE</code> SDN connector and firewall address objects. The following IP address filters are supported:</p> <pre>Spoke_1 (AZ) # show config firewall address edit "AZ" set uuid 6b18eb16-7069-51ef-c174-58f82ee3d1b2 set type dynamic set sdn "6899_AutoScale_1" next end Spoke_1 (AZ) # set filter <key1=value1> [& <key2=value2>] [<key3=value3>]</pre> <p>Available filter keys are:</p> <pre><Vm><Tag><Size><Location><SecurityGroup> <Vnet><Subnet><ResourceGroup><ApplicationSecurityGroup><Vmss><Subscription> <LoadBalancer><ApplicationGateway> <ServiceTag><Region> <K8S_Cluster><K8S_Namespace><K8S_ServiceName><K8S_NodeName> <K8S_PodName><K8S_Region><K8S_Zone><K8S_Label.></pre>
1055813	FortiGate-VM supports AWS Nitro TPM 2.0 specification.

Feature ID	Description
1061195	FortiOS version 7.6.1 supports the use of MLX5/4 and the upcoming MANA NIC on Azure Dv6/Ev6 instance types.
1071411	Azure SDN connectors support GraphQLbulk queries.

LAN Edge

See [LAN Edge](#) in the New Features Guide for more information.

Feature ID	Description
1005045	Previously, VLAN optimization could only be enabled or disabled. The new VLAN pruning feature selectively allows only necessary VLANs on the path between destinations on auto-generated trunks, reducing traffic congestion and enhancing network performance.
1039228	<p>Added support for VLANs over a FortiExtender configured as a LAN extension. VLAN support is configured on the FortiGate Access Controller using the GUI or using these CLI commands:</p> <pre> config extension-controller extender-profile edit <FortiExtender Profile> set extension lan-extension config lan-extension config downlinks edit <id> set type port set port <port> set pvid <vlanid> next end end next end </pre> <p>Where <code>port</code> is the VLAN interface added to the FortiExtender interface and <code>vlanid</code> is the desired VLAN ID.</p>
1058402	FortiOS now includes advanced Wireless Intrusion Detection System (WIDS) options, enhancing the detection and reporting of a wider range of wireless threats. This upgrade boosts security, providing customers with superior detection against potential intrusions.
1059461	<p>The FOS WiFi Controller now includes a <code>called-station-id-type</code> setting, allowing customization of the <code>Called-Station-Id</code> attribute in RADIUS <i>Access-Request</i> packets to use MAC:SSID, IP:SSID, or APName:SSID formats, enhancing network configuration flexibility.</p> <pre> conf wireless-controller vap edit <name> set called-station-id-type {mac ip apname} next </pre>

Feature ID	Description
	end
1060780	FortiAP now supports console, SSH, or HTTPS login using remote user accounts from a third-party TACACS server, enhancing flexibility and security in account management.
1068898	FortiGate now generates accounting messages when WiFi clients connect to an SSID with MPSK created through the FortiGuest self-registration portal, enhancing network management and user accountability.
1078491	The FortiOS WiFi controller now supports pushing RADIUS server settings using TCP or TLS protocols to FortiAP's for Local-Bridge mode Captive Portal SSIDs, enhancing security and reliability compared to the previous UDP-only support.

Network

See [Network](#) in the New Features Guide for more information.

Feature ID	Description
961038	Add 2.5G and 5G speed options for the 10/1 GigE RJ45 interfaces (port1-16) on the FortiGate 2600F platform. Also add an auto option (the new default) that automatically adjusts the port speed. Existing port speed configurations will be maintained during the firmware upgrade.
1032512	Support including denied multicast sessions in the session table. This feature allows the creation of sessions for denied multicast traffic, enabling subsequent packets to be directly matched and dropped, reducing CPU usage and improving performance. <pre>config system setting set ses-denied-multicast-traffic {disable enable} end</pre>
1040296	To support VRF route leaking, on FortiGates with NP6 and NP7 processors, you can use the following command to enable accelerated NPU inter-VDOM links without enabling multi-VDOM mode. <pre>config system global set single-vdom-npuvlink {enable disable} end</pre>
1040394	Enhanced flexibility and performance in network with smaller configurable TTL for UDP traffic on hyperscale firewall VDOMs. Previously, the minimum TTL for UDP traffic was set at 120 seconds for Hyperscale firewall VDOMs. This enhancement removes that restriction, allowing users to configure the TTL to 1 second or more. This change offers greater flexibility in network management and enhances network performance.

Feature ID	Description
1048011	Extended VRF ID Range for Enhanced Network Scalability. Previously, up to 252 Virtual Routing and Forwarding (VRF) instances could be configured per VDOM, with VRF IDs ranging from 0 to 251. With this enhancement, the VRF ID range has been extended to 0-511, allowing for a minimum of 512 unique VRFs per VDOM. This enhancement allows for greater scalability and flexibility in network configurations.
1049910	FortiGate now supports inspecting 802.1ah packets within a virtual wire pair configuration. This enhancement enables deep packet inspection and UTM scanning. By leveraging this capability, FortiGate can effectively analyze and inspect the 802.1ah header, perform the necessary inspection, and then re-add the header, ensuring robust protection against a wide range of cyber threats.
1060303	Previously, local-out traffic could not specify a Virtual Routing and Forwarding (VRF) instance, but now it can, allowing for traffic segregation, optimized routing, and enhanced policy enforcement, which improves network organization, security, and performance.
1061705	Introducing a new FortiGate feature that disables IP address translation within the SIP payload in 464XLAT environments. This ensures SIP packets with IPv4 information reach user equipment without translation, preventing RTP connection issues and improving the reliability of SIP-based services.
1067117	<p>Added support for specifying the outgoing interface and VRF for a web proxy forward server or a web proxy isolator server, such as Fortisolator.</p> <pre> config web-proxy forward-server edit <name> set interface-select-method specify set interface <port> set vrf-select <vrf-id> next end config web-proxy isolator-server edit <name> set interface-select-method specify set interface <port> set vrf-select <vrf-id> next end </pre>
1071614	The <code>hw-session-sync-dev</code> option now supports multiple physical interfaces, up to twice the number of Network Processors (NPs). Additionally, it now shares the ports between hardware and software session-sync devices. This enhancement increases reliability and flexibility in network configurations.
1082763	PIM now supports all VRFs (up to 511) and is aware of IPv4 multicast routing/forwarding over a single overlay, enhancing network scalability and flexibility compared to the previous VRF 0-only support.

Operational Technology

See [Operational Technology](#) in the New Features Guide for more information.

Feature ID	Description
1000362	<p>FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G include a general purpose input output (GPIO) module, also known as, a digital I/O (DIO) module. Added support for SNMP traps or notifications and automation stitch notifications when DIO module alarm functionality is activated, that is, when a change in any digital input is detected and the digital output is activated. Notification support depends on previously configured <code>config system digital-io</code> and <code>execute digital-io set-output</code> settings prior to event notification.</p> <p>SNMP and automation stitch notifications can be configured using these CLI commands on FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G devices only:</p> <ul style="list-style-type: none"> For automation stitch support, in <code>config system automation-condition</code> added new options <code>set condition-type input</code> and <code>set input-state open close</code> For SNMP support, in <code>config system snmp community</code> added new option <code>set events dio</code>
1075708	<p>FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G include a general purpose input output (GPIO) module, also known as, a digital I/O (DIO) module. This module is used for activating a digital output when triggered by a change in any digital input. For example, when a switch change from open to closed or a voltage change from low to high is detected, then a digital output is activated. In this example, the digital input is connected to a cabinet door and the output is connected to a buzzer.</p> <p>Added CLI support for configuring the above DIO alarm functionality on FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G devices only:</p> <ul style="list-style-type: none"> <code>config system digital-io:command</code> to configure input mode <code>execute digital-io set-output:command</code> to configure output mode <code>diag sys digital-io state:command</code> to check current input/output status

Policy & Objects

See [Policy and objects](#) in the New Features Guide for more information.

Feature ID	Description
1003586	<p>Added support for a web proxy isolator server, such as Fortisolator, in proxy policies and added a new <i>Isolate</i> action in proxy-policy to distinguish isolated traffic from normal traffic in logs. Isolators are fundamentally the same as web proxy forward servers because both will redirect HTTP/HTTPS requests to a HTTP/HTTPS proxy server. However, isolators have the specific function of isolating potentially unsafe traffic from a user environment.</p> <p>The following CLI commands have been added to support isolator servers:</p> <pre>config web-proxy isolator-server</pre>

Feature ID	Description
	<pre> edit <name> set addr-type {ip ipv6 fqdn} set ip <any_ip> set ipv6 <IPv6 addr> set fqdn <string> set port <port> next end config firewall proxy-policy edit <id> set action isolate set isolator-server <name> next end </pre>
1027037	Support Fully Qualified Domain Name (FQDN) address groups within the Internet Service Database (ISDB), addressing the challenge of frequently changing IP addresses and ensuring accurate and reliable firewall policies.
1040199	The current Port block allocation (PBA) and Fixed port range (FPR) IP Pool mechanisms use a sequential port selection algorithm, assigning the next available non-conflicting port within the specified range. This enhancement introduces the <code>port-random</code> firewall policy option for enabling a randomized port selection algorithm, making the allocation process less predictable, thus enhancing security.
1046509	FortiOS has introduced a new dynamic address object subtype, RSSO, which can be used in both the source and destination fields of firewall policies. This enhancement allows for more granular and precise policies based on RSSO group membership, enhancing security and flexibility in managing network traffic and enforcing policies.
1058411	Introducing a new ISDB entry for Fortinet SOCaaS, Fortinet-FortiGuard.SOCaaS. This feature enables customers to configure policies for devices to forward data to SOCaaS collectors without relying on DNS. By eliminating the dependency on DNS, this enhancement reduces the risk of DNS mapping failures, ensuring a more reliable and seamless data forwarding process.
1058516	<p>Hyperscale FortiOS now supports a configurable interim log for PBA NAT logging. This enables continuous access to PBA event logs during an ongoing session, providing comprehensive logging throughout the session's lifespan.</p> <pre> config firewall ippool edit <name> set type cgn-resource-allocation set pba-interim-log next end </pre> <p>The <code>log-interval</code> range is 600 to 86400 seconds. Default is 0 which disables interim logging. Interim logging is supported by the NP7 hardware log module and host hardware logging. Interim logging is also compatible with per-session, per-mapping, and per-session ending logging modes and works with the NetFlow and syslog log formats.</p>

Feature ID	Description
	Interim logging for PBA sessions was added to mainstream FortiOS version 7.6.0.
1070831	A new default local-in-policy has been added with internet service source enabled for Malicious-Malicious.Server, Tor-Exit.Node, and Tor-Relay.Node. This policy is designed to utilize these 3 ISDB sources to identify known malicious threat actors and prevent them from accessing any interface on the FortiGate on any service and port.
1085702	Previously, MAP-E utilized the RA IPv6 prefix for deployment. With this enhancement, MAP-E can now operate in DHCPv6-PD environments, providing greater flexibility, improved automation, and scalability in network configurations.

SD-WAN

See [SD-WAN](#) in the New Features Guide for more information.

Feature ID	Description
951494	<p>In this enhancement, support for a new FortiGuard SLA Database (SLA Database), which includes popular SaaS and Internet destinations and recommended settings that can be selected as probe servers for SD-WAN Performance SLA configuration in the GUI using the <i>Performance SLA</i> and <i>SLA Target</i> fields in the <i>New Performance SLA</i> page and in the CLI using these commands:</p> <pre>config system sdwan config health-check edit <health-check name> set fortiguard enable set fortiguard-name <target-name-from-SLA-Database> next end end</pre> <p>The FortiGate requires a valid SD-WAN Network Monitor (SWNM) entitlement to be applied for the FortiGuard SLA Database to be downloaded or updated.</p>
1002494	<p>In this enhancement, an SD-WAN wizard is added to the <i>SD-WAN > SD-WAN Zones</i> page to provide guided configuration of these settings for a simple SD-WAN setup (maximum of two members can be added in the SD-WAN wizard):</p> <ul style="list-style-type: none"> • <i>Interface</i> • <i>Networking</i> • <i>Performance SLA</i> • <i>SD-WAN Rule</i> <p>After the wizard is used, a default static route using the newly created SD-WAN interface must still be configured.</p> <p>The FortiGate requires a valid SD-WAN Network Monitor (SWNM) entitlement to be applied for the SD-WAN wizard to be visible.</p>

Feature ID	Description
1025701	<p>In this enhancement, support has been added for passive application performance monitoring (APM) by measuring and logging these metrics per TCP session:</p> <ul style="list-style-type: none"> • Network response time • Server response time • Original retransmits • Reply retransmits • SYN retransmits • SYN-ACK retransmits • Original or reply resets <p>These passive measurements are configured in firewall policies with the SD-WAN zone as the destination interface using these CLI commands:</p> <pre>configure firewall policy edit < entry > set app-monitor < enable disable > next end</pre> <p>Upon enabling this feature, NPU offloading for the firewall policy is disabled automatically. This feature assists with monitoring performance of TCP traffic and locating potential network issues. TCP metrics can be displayed using <code>diag sys session list</code> in the CLI and in forward traffic logs displayed in either the CLI or the GUI.</p> <p>SD-WAN traffic steering remains independent from the measured TCP session metrics.</p>
1048430	<p>Hubs are not necessarily connected to all the same underlay transports as Spokes. For ADVPN 2.0, added support for shortcuts between Spokes using transports to which Hubs are not connected using overlay placeholders. For example, if Spokes are configured with an overlay over the Internet and an overlay over MPLS using this tunnel interface as a placeholder since it is not established with the Hub, ADVPN 2.0 allows a shortcut tunnel to be established over MPLS if this path is in-SLA and is the best quality. Each Spoke should be configured with these CLI commands:</p> <pre>config vpn ipsec phase1-interface edit <placeholder_phase1_interface_name> set type dynamic ... set net-device enable ... set auto-discovery-dialup-placeholder enable next end</pre>
1071495	<p>Users can now specify an SD-WAN zone as an interface in the following policies:</p> <ul style="list-style-type: none"> • Local-in policy • DoS policy • Interface policy • Multicast policy • TTL policy

Feature ID	Description
	<ul style="list-style-type: none"> Central SNAT map <p>This update simplifies policy management and boosts operational efficiency.</p>

Security Fabric

See [Security Fabric](#) in the New Features Guide for more information.

Feature ID	Description
980693	Add Known Exploited Vulnerabilities (KEVs) information to IoT/OT vulnerabilities stored in the user/device store, and display KEV counts and warnings accordingly on the GUI Asset Identity Center page, thereby enhancing security visibility for users.
1034551	OCI SDN connectors support IPv6 address objects.
1038134	GCP SDN connectors support IPv6 address objects.
1039660	Users can now hide non-relevant Security Rating tests, streamlining the user experience by displaying only pertinent information.
1039849	OCI SDN connectors support IPv6 for dynamic firewall addresses and high availability failover.

Security Profiles

See [Security profiles](#) in the New Features Guide for more information.

Feature ID	Description
968707	In this enhancement, risk level rating is added to the FortiGuard URL rating service. FortiGate can query the rating service to retrieve the risk score for a URL. This risk score rates the likelihood that a website has malicious intent. This risk score and level can be used in a webfilter profile to apply a block or monitor action, or it can be used as a match criteria for a web proxy policy.
1027296	<p>A new <code>ocr-only</code> option has been added to the ICAP profile, allowing you to forward only image files (such as JPEG, JPG, PNG) relevant for OCR scanning to the ICAP server, such as FortiProxy. This selective forwarding applies exclusively to responses, not web requests. This feature enhances overall system efficiency by reducing processing time and optimizing resource usage.</p> <pre> config icap profile edit <name> set ocr-only enable next end </pre>

Feature ID	Description
1068910	<p>Streamline IoT/OT device detection. With this new feature, there's no longer a need to apply an Application Control profile. Users can now simply enable or disable IoT or OT categories directly for device detection. If these signatures aren't excluded in any policy interfaces, a built-in application list is automatically created and applied. This ensures the relevant IoT or OT categories are active, optimizing the IPS functionality and reducing the overall configuration complexity for users.</p> <pre> config system interface edit <name> set device-identification enable set exclude-signatures {ot iot} next end </pre>

System

See [System](#) in the New Features Guide for more information.

Feature ID	Description
812576	Previously, customers had to register each Fortinet device to their FortiCare account individually. This new feature simplifies the process with a one-click solution, allowing customers to register all Fortinet devices in the same security fabric group at once. It lists all unregistered fabric components (FGT, FAP, FSW) and provides a <i>Register All</i> option, saving time and effort.
861843	Support Firmware Upgrade Report. This enhancement allows users to perform sanity checks by comparing configurations and statistics before and after a firewall upgrade, thereby enhancing the upgrade process and providing detailed assurance of successful upgrades.
1053978	Subscriptions and FortiGuard settings are now organized into separate tabs with clear distinctions between licensed, expired, and available-for-purchase subscriptions, providing customers with a more intuitive and informative layout.
1061119	This enhancement reduces ipshelper CPU usage during the database update process, optimizing system performance and ensuring smoother operations.
1087866	Added route monitoring to FGSP, enhancing network stability by detecting route prefix withdrawals. This prevents traffic loss in complex environments and improves the UTM scanning experience.

WiFi Controller

See [Wireless](#) in the New Features Guide for more information.

Feature ID	Description
1043784	In FortiOS, the WiFi controller supported the MPSK feature on a WPA2-Personal SSID by applying an MPSK profile or enabling RADIUS MAC authentication. However, for a WPA3-SAE SSID, the MPSK feature was only supported through the application of an MPSK profile. This enhancement allows WPA3-SAE SSIDs to utilize RADIUS MAC authentication to implement the MPSK feature.
1044322	The FortiGate WiFi Controller now supports uploading the portal servers certificate to the FortiAP. This allows the FortiAP to use the same server certificate to secure the HTTPS POST actions. With the corresponding CA imported on users devices, authentication is smoother and free of security warnings, enhancing the user experience.

ZTNA

See [Zero Trust Network Access](#) in the New Features Guide for more information.

Feature ID	Description
998798	<p>A ZTNA web portal is added for accessing applications directly within the portal without requiring FortiClient to be installed on the endpoint or a client certificate check. The ZTNA portal handles authentication and authorization of traffic destined for the protected resources. It is implemented entirely in WAD.</p> <pre> config ztna web-portal edit < name > set vip <vip name> set host <Virtual host name> set auth-portal {enable disable} set vip6 <Virtual IPv6 name> set auth-rule <rule> next end config ztna web-portal-bookmark edit < name > set users <users> set groups <groups> config bookmarks edit < name > set apptype {ftp rdp sftp smb ssh telnet vnc web} set url <string> set host <name or IP> set description <Description> set port <remote port> set sso {enable disable} next end next end next </pre>

Feature ID	Description
	end
1069002	Added <code>ztna-ems-tag-negate</code> to ZTNA proxy policy.

Upgrade information

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

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 29 and Upgrading all devices in the FortiOS Administration Guide.

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 7.6.1 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 7.6.1
FortiManager	• 7.6.1
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 and later
FortiAP	• 7.2.2 and later

FortiAP-U	• 6.2.5 and later
FortiAP-W2	• 7.2.2 and later
FortiClient EMS	• 7.0.3 build 0229 and later
FortiClient Microsoft Windows	• 7.0.3 build 0193 and later
FortiClient Mac OS X	• 7.0.3 build 0131 and later
FortiClient Linux	• 7.0.3 build 0137 and later
FortiClient iOS	• 7.0.2 build 0036 and later
FortiClient Android	• 7.0.2 build 0031 and 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.



When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.6.0, use FortiClient 7.6.0.

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. FortiGate devices
4. Managed FortiExtender devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.6.1. When Security Fabric is enabled in FortiOS 7.6.1, all FortiGate devices must be running FortiOS 7.6.1.

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*.

FortiGate 6000 and 7000 upgrade information

Upgrade FortiGate 6000 firmware from the management board GUI or CLI. Upgrade FortiGate 7000 firmware from the primary FIM GUI or CLI. The FortiGate 6000 management board and FPCs or the FortiGate 7000 FIMs and FPMs all run the same firmware image. Upgrading the firmware copies the firmware image to all components, which then install the new firmware and restart. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

On a standalone FortiGate 6000 or 7000, or an HA cluster with `uninterruptible-upgrade` disabled, the firmware upgrade interrupts traffic because all components upgrade in one step. These firmware upgrades should be done during a quiet time because traffic can be interrupted for a few minutes during the upgrade process.

Fortinet recommends running a graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.



Fortinet recommends that you review the services provided by your FortiGate 6000 or 7000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.6.1:

1. Use the following command to set the `upgrade-mode` to `uninterruptible` to support HA graceful upgrade:

```
config system ha
    set uninterruptible-upgrade enable
end
```



When upgrading from FortiOS 7.4.1 to a later version, use the following command to enable uninterruptible upgrade:

```
config system ha
    set upgrade-mode uninterruptible
end
```

2. Download the FortiOS 7.6.1 FG-6000F, FG-7000E, or FG-7000F firmware from <https://support.fortinet.com>.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
For example, check the FortiGate dashboard or use the `get system status` command.
5. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

Default setting of `cp-accel-mode` is changed to `none` on 2GB memory models

This change disables CP acceleration to lower system memory usage thus can prevent some unexpected behavior due to lack of memory.

Previous FortiOS CLI behavior:

```
config ips global
    set cp-accel-mode advanced
end
```

New FortiOS CLI behavior after upgrade:

```
config ips global
    set cp-accel-mode none
end
```

This change will cause performance impact as CPU will do the pre-match (pattern match) inside IPS (CPU) instead of hardware engine (cp module in SOC4). Some customers could expect an increase in CPU utilization as a result.

FortiGate and FortiWiFi 4xF/6xF families are affected by this change.

Product integration and support

The following table lists FortiOS 7.6.1 product integration and support information:

Web browsers	<ul style="list-style-type: none">• Microsoft Edge 112• Mozilla Firefox version 113• Google Chrome version 113 <p>Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.</p>
Explicit web proxy browser	<ul style="list-style-type: none">• Microsoft Edge 112• Mozilla Firefox version 113• Google Chrome version 113 <p>Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiController	<ul style="list-style-type: none">• 5.2.5 and later <p>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C</p>
Fortinet Single Sign-On (FSSO)	<ul style="list-style-type: none">• 5.0 build 0319 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none">• Windows Server 2022 Standard• Windows Server 2022 Datacenter• 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• Novell eDirectory 8.8
AV Engine	<ul style="list-style-type: none">• 7.00034
IPS Engine	<ul style="list-style-type: none">• 7.01026

See also:

- [Virtualization environments on page 34](#)
- [Language support on page 34](#)
- [SSL VPN support on page 35](#)
- [FortiExtender modem firmware compatibility on page 35](#)

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	<ul style="list-style-type: none">8.2 Express Edition, CU1
Linux KVM	<ul style="list-style-type: none">Ubuntu 22.04.3 LTSRed Hat Enterprise Linux release 8.4SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	<ul style="list-style-type: none">Windows Server 2022
Windows Hyper-V Server	<ul style="list-style-type: none">Microsoft Hyper-V Server 2022
Open source XenServer	<ul style="list-style-type: none">Version 3.4.3Version 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 113 Google Chrome version 112
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 112
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 112
macOS Ventura 13.1	Apple Safari version 16 Mozilla Firefox version 103 Google Chrome version 111
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.

FortiExtender modem firmware compatibility

The following table lists the modem firmware file name and version for each FortiExtender model and its compatible geographical region.

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-101F-AM	FEM_EM06A-22-1-1	FEM_EM06A-22.1.1-build0001.out	America
FEX-101F-EA	FEM_EM06E-22-01-01	FEM_EM06E-22.1.1-build0001.out	EU
	FEM_EM06E-22.2.2	FEM_EM06E-22.2.2-build0002.out	EU

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-201E	FEM_06-19-0-0-AMEU	FEM_06-19.0.0-build0000-AMEU.out	America and EU
	FEM_06-19-1-0-AMEU	FEM_06-19.1.0-build0001-AMEU.out	America and EU
	FEM_06-22-1-1-AMEU	FEM_06-22.1.1-build0001-AMEU.out	America and EU
	FEM_06-22-1-2-AMEU	FEM_06-22.1.2-build0001-AMEU.out	America and EU
FEX-201F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-201F-EA	FEM_07E-22-0-0-WRLD	FEM_07E-22.0.0-build0001-WRLD.out	World
	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-202F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-202F-EA	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-211E	FEM_12-19-1-0-WRLD	FEM_12-19.1.0-build0001-WRLD.out	World
	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-0-AMEU	FEM_12-22.0.0-build0001-AMEU.out	America and EU
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEV-211F_AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEV-211F	FEM_12-22-1-0-AMEU	FEM_12-22.1.0-build0001-AMEU.out	World
FEX-211F-AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEX-212F	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEX-311F	FEM_EM160-22-02-03	FEM_EM160-22.2.3-build0001.out	World
	FEM_EM160-22-1-2	FEM_EM160-22.1.2-build0001.out	World

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-511F	FEM_RM502Q-21-2-2	FEM_RM502Q-21.2.2-build0003.out	World
	FEM_RM502Q-22-03-03	FEM_RM502Q-22.3.3-build0004.out	World
	FEM_RM502Q-22-04-04-AU	FEM_RM502Q-22.4.4-build0005_AU.out	Australia
	FEM_RM502Q-22-1-1	FEM_RM502Q-22.1.1-build0001.out	World
	FEM_RM502Q-22-2-2	FEM_RM502Q-22.2.2-build0002.out	World

The modem firmware can also be uploaded manually by downloading the file from the Fortinet Customer Service & Support site. The firmware file names are listed in the third column of the table.

To download the modem firmware:

1. Go to <https://support.fortinet.com/Download/FirmwareImages.aspx>.
2. From the *Select Product* dropdown, select *FortiExtender*.
3. Select the *Download* tab.
4. Click *MODEM-Firmware*.
5. Select the FortiExtender model and image name, then download the firmware file.

Resolved issues

The following issues have been fixed in version 7.6.1. To inquire about a particular bug, please contact [Customer Service & Support](#).

Anti Spam

Bug ID	Description
1050805	When spam mail is received from the server, POP connection times out.

Anti Virus

Bug ID	Description
1044961	On FortiGate, the Scanunit does not work as expected due to zlib data check issue.
1054835	Large file downloads take longer than expected due to a WAD process issue.
1055609	Files sent between FortiGate and FortiSandbox are dropped due to a connection issue.
1058701	On FortiGate, the <code>av-mem-limit</code> does not work as expected when <code>set av-failopen pass</code> configured due to a memory usage issue.
1062753	The incorrect percentage is displayed in the <i>Files Uploaded Today</i> widget to <i>Sandbox</i> .
1068321	MMDB and AVAI DBs are unsigned after upgrading from version 7.0.15 to version 7.2.9.
1070864, 1082877	The scanunit shows error messages that do not provide enough detail when corrupt AV engine or DB events occur.
1073326	Entry-level FortiGate's with 2GB of memory encounter a memory usage issue and do not operate as expected caused by the scanunit initiating an AV engine restart.
1078882	Scanunit tries to scan with no payload, resulting in an error message from FortiNDR and generating an error on FortiGate.

Application Control

Bug ID	Description
951150	The Zoom meeting remote control feature is not blocked during meetings.
990540	FortiGate does not generate traffic logs for established or denied TCP sessions that lack application data.
1060562	The application control profile is missing on the GUI for FortiGate models with 2GB of memory.
1064413	When using SD-WAN load balancing, some sites are slow or inaccessible when the Application Control action is set to <i>Allow</i> .
1066078	Application control cannot detect Facebook as <i>Social Media</i> when certificate-inspection is used.
1066567	Tencent.Meeting application is not blocked by the inline IPS when using HTTP or Socks5 proxy.

Data Loss Prevention

Bug ID	Description
908279	The DLP incorrectly detects a .pdf file as a .mpeg file and blocks the download.
984784	When a DLP profile is set to MAPI, there is a slow connection between Outlook and the Exchange server.
1049719	The DLP dictionary with a regex configuration does not deny an accent mark on FortiGate.

DNS Filter

Bug ID	Description
1058866	DNS translation does not work as expected when a resolved IP matches the external block list entry.
1086355	DNS query logs are not visible on FortiGate when traffic uses VIP for DNS traffic.

Explicit Proxy

Bug ID	Description
900911	When <code>secure-web-proxy</code> is enabled, if the client disconnects without sending any data as soon as the TCP connection with FortiGate is established, a WAD process signal 11 error occurs.

Bug ID	Description
1056600	FortiGate experiences a WAD process issue and produces a <code>wad_find_fwdsrvr_by_key</code> error.
1076642	Unable to load pages with cloudflare protected websites with auth enabled, if Auth scheme is set to Form-Based in explicit proxy.

File Filter

Bug ID	Description
1011320	Adding File Filter to a firewall policy will impact performance.
1095866	Filefilter block corrupts file on NetApp Files share instead of completely blocking it.

Firewall

Bug ID	Description
996622	On FortiGate, the IPv6 real server shown as DOWN by the health check but it is considered UP in the kernel.
1007029	On FortiGate, connections are disrupted between client email exchange servers and a virtual server when HTTP2 support is enabled.
1007566	When the FortiGate has thousands of addresses and hundreds address groups, the GUI can take a few minutes to search for a specific address inside the address group dialog.
1028356	Reordering the DNAT policies in the central NAT causes a false hit count.
1030516	An internet interface with egress/outbound shaping encounters a performance issue with sla after rebooting.
1036676	When a loopback interface has an IP that matches a VIP's <code>extip</code> with an <code>extintf "any"</code> , FortiGate will match the VIP but the oif loopback causes an unintended policy 0 match and drops.
1047208	The FortiGate virtual server does not setup an http2 connection with a WebSocket server due to a WAD process issue.
1050864	No route is found when the FTP server connects back to FTP client in FTP active mode.
1051891	The SNMP <code>fglpsAnomalyDetections</code> counter does not increase if the DoS policy is configured in a no management VDOM.
1055733	The F5 HTTP/S monitors for the web server in FortiGate do not function as expected due to HTTP 0.9 traffic.
1057080	On the <i>Firewall Policy</i> page, search results do not display in an expanded format.
1058494	When <code>snat-hairpin-traffic</code> is enabled, SNAT is not automatically applied to hairpin traffic,

Bug ID	Description
	causing a SNAT mismatch in <code>strict-dirty-session-check</code> .
1059989	Modifying the shaping profile, whether it is assigned to an interface or not, results in IPsec tunnels going down.
1060452	FortiGate in policy-based mode showing the incorrect policy ID in forward traffic logs.
1062333	FortiGate does not reply to an ARP request when VIP is disabled due to an <code>iplist</code> reference issue.
1064748	When a VIP load balancer is configured to use an IPPool and has <code>http-multiplex</code> enabled, FortiGate performs SNATs using the outgoing interface instead of the IPPool.
1068393	Incorrect matching of zones and SD-WAN zones occurs where interfaces do not exist.
1078662	Incorrect checksum for fragments after QTM.
1079590	Intermittent reply traffic is not sent out of FortiGate.
1081542	On FortiGate, packets are dropped when ASIC offloading is enabled.
1052334	The firewall policy name length validation does not work with Korean characters.
1088905	The Virtual Server HTTP <code>healthcheck</code> uses the IP address as a Host even when the full URL is configured in <code>http-get</code> .

FortiGate 6000 and 7000 platforms

Bug ID	Description
986845	On FortiOS, the <i>Security Fabric</i> widget does not display information on blade status.
997161	On FortiGate 6000 FPCs and FortiGate 7000 FPMs the node process may consume large amounts of CPU resources, possibly affecting FPC or FPM performance. (You can run the <code>diagnose sys top</code> command from an FPC or FPM CLI to view CPU usage.) This problem may be caused by security rating result submission.
1016439	Enabling or disabling a vcluster causes some backup routes (<code>proto = 20</code>) to be lost when a routing table has a significant amount of routes (over 10000 routes).
1032573	In an HA configuration, FortiGate does not respond to SNMP queries causing the device to display as being DOWN.
1035601	An SNMP query for policy statistics returns 0 on MBD.
1037965	When applying a script to a configuration, the updated configuration is applied to the FIM but is not fully synchronized on the FPCs.
1048808	If the secondary reboots, after it rejoins the cluster SIP sessions are not resynchronized.
1056894	On FortiGate, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.
1057499	FIM interfaces are DOWN after restoring the root VDOM configuration due to a speed issue.

Bug ID	Description
1060619	CSF is not working as expected.
1081015, 1086953	The secondary 7K slot 3 (FPM) has no ISDB database and will not update.
1086889	FIM encounters a split-brain scenario after rebooting.
1088402	On FortiGate 6K/7K FGSP clusters, the configuration does not synchronize properly with <code>standalone-config-sync</code> enabled.

FortiView

Bug ID	Description
1009287	On the <i>Dashboard > FortiView Sessions</i> page, closing a large number of FortiView sessions (+100) can take longer than expected and result in a CPU usage issue.
1029254	When trying to filter by device using the <i>1 week</i> filter option, the <i>User device store query error (error code: -1)</i> error message is displayed.
1077555	On FortiGate, the <i>Top Threat - WAN</i> does not show the correct information for the IPS Logs.

GUI

Bug ID	Description
885427	On the <i>Network > Interfaces</i> page, the SFP port is grayed out on the faceplate diagram even though the port is working. This is purely a GUI display issue and does not affect system operation. Workaround: View the SFP port information and status using the <code>interface list</code> in the CLI.
989512	When the number of users in the <i>Firewall User</i> monitor exceeds 2000, the search bar, column filters, and graphs are no longer displayed due to results being lazily loaded.
991573	In the <i>Assets</i> widget preview window of the <i>Asset & Identities</i> widget, clicking the <i>Refresh</i> button does not update the data.
1009143	On FortiOS, the time displayed in the CLI and in the GUI do not match.
1018682	When creating a firewall policy, applications groups with custom application signatures cannot be saved using the GUI.
1035356	The WAN interface is accessible in the GUI under certain interface configurations even though it is not allowed in the configuration file.
1044745	On the <i>Dashboard > User & Devices</i> page on a VDOM, the <i>Address</i> column shows multiple devices with the FortiGate VLAN gateway instead of the Client IP.

Bug ID	Description
1050865	When updating an administrator password in the GUI, the password expiration date does not update when the new password is created.
1052040	The <i>IP/Netmask</i> column of HA management port hangs in the GUI.
1056800	On FortiOS, IPSec localid cannot be deleted using the GUI.
1057628	<i>Catch WebSocket</i> errors from <i>PerMessageDeflate</i> occur when the client abruptly closes the connection.
1058473	Expired licenses are still displayed in the GUI after 30 days.
1058608	FortiGate Cloud still shows as <i>Activated</i> in the GUI, even when logged out.
1068202	On low end models, the service list is empty when selecting members for a Service Group.
1071907	In the GUI, there is no setting for the type option for the <i>npu_vlink</i> interface.
1092475	GTP-profile do not display in the GUI when Central SNAT is enabled.

HA

Bug ID	Description
824651	Certificate upload causes HA checksum mismatch.
965217	In an HA configuration, FortiGate may experience intermittent heartbeat loss causing unexpected failover to the secondary unit.
1007516	Rx_dropped is observed on <i>ha1</i> and <i>ha2</i> interfaces and randomly experiences flapping.
1009939	When bandwidth is low, the <i>tftp backup</i> command on the secondary unit does not work as expected when it should be able to reach the server.
1026794	The HA secondary FortiGate logical topology page shows the <i>FAZ</i> connected interface as <i>FortiAnalyzer</i> .
1036139	FortiGate encounters a memory usage issue caused by <i>cmdbsvr</i> and <i>hasync</i> .
1047094	The HA Secondary unit cannot communicate with FortiGate Cloud when it uses <i>standalone-mgmt-vdom</i> using the HA Primary unit.
1052320	In a vCluster configuration, traffic stops after a VDOM failover.
1054041	On FortiGate's in an HA environment, DHCP clients can not get an IPv4 address from the server with <i>vcluster</i> .
1055336	Using the <i>Test User Credentials</i> button from the Radius Server in the GUI does not honor the custom <i>nas-id-type</i> .
1056138	On FortiGate 120G and 121G models in an HA cluster, if the <i>ha</i> or <i>mgmt</i> interface is used as the heartbeat interface, the HA cluster may not synchronize and the GUI HA page may not load.

Bug ID	Description
1056651	Static routes configured under the secondary unit's <code>standalone-mgmt-vdom</code> do not take effect.
1060006	The <code>standalone-config-sync</code> conf-member kept out-of-synchronization after an upgrade and configuration change.
1060023	FortiGate in an HA environment encounter a CPU usage issue in the softirq on FGSP cluster members with more than 200000 session running.
1061492	The HA secondary device sends GARP with the wrong MAC address after the vcluster is removed.
1064728	More sessions on a FGCP secondary unit than the primary unit.
1067274	Reply packets are misdirected in an asymmetric L3 FGSP configuration.
1070745	Sessions may not fail back to the original FGSP peer that owns the session if either the interface name for the <code>monitor-interface</code> or <code>pingsvr-monitor-interface</code> is 7 characters or longer.
1070901	The <code>fgsp_route_health</code> status is incorrect when configuring a <code>monitor-interface</code> or <code>link-monitor-interface</code> with a long interface name.
1084662	FFDB signatures keep flapping on all blades except the master FIM of the primary chassis.
1085371	SNMP v3 times out in FortiGate Azure/AWS in HA setup.
1092547	FortiGate in an HA configuration keeps rebooting continuously during a firmware upgrade.

Hyperscale

Bug ID	Description
1042512	On FortiGate, the <i>CGN Resource Quota</i> field allows an invalid value to be set.
1047362	The <i>sw session</i> and <i>log2host netflow</i> logs cannot be seen even though template is present. Data packet displays an error saying <i>template not found</i> .
1075915	The NP can get stuck after many hours of traffic with <code>mse hash tbl</code> caused by a <code>mse depfail</code> .

ICAP

Bug ID	Description
1072282	ICAP may encounter a <i>400 Bad Request</i> error with certain websites due to an absent reason-phrase when converting from HTTP/2 to HTTP/1.

Intrusion Prevention

Bug ID	Description
891295	FortiGate experiences a performance issue with geography-type addresses matching in NGFW policy mode.
1001860	On the <i>Security Profiles > Intrusion Prevention</i> page, when a new IPS filter is created with no filter selected, the <i>Details</i> column of the IPS Signatures and Filters table is blank instead of <i>All Attributes</i> .
1016531	FortiGate encounters a memory usage issue in the IPS engine when <code>av-failopen</code> is set to <code>pass</code> .
1040783	FortiGate encounters CPU usage issue due to IPSEngine utilization when using an <code>app-ctrl utm</code> profile.
1066151	Forticron runs <code>diagnose ips debug disable all</code> and <code>diagnose ips ssl debug none</code> constantly due to a processing issue.
1086789	FortiGate encounters a CPU usage issue caused by the IPS engine.

IPsec VPN

Bug ID	Description
1002345	IKE daemon randomly does not operate as expected during phase1 rekeying depending on soft rekey margin, timing, and packet ordering.
1018749	IPsec inserted SA's are not deleted successfully after flushing all tunnels.
1020690	The <i>IPsec Aggregate</i> interface displays as DOWN on the <i>Network > Interfaces</i> and the <i>Policy & Objects > Firewall Policy</i> pages when the member including the Dialup VPN is actually UP. This is purely a GUI display issue and does not affect system operation. The correct status is shown on the <i>VPN > IPsec Tunnels</i> page.
1023871	IPsec IKEv2 with SAML cannot match the Entra ID group during EAP due to a buffer size issue.
1024558	IPsec interfaces created on <code>802.1ad + 802.3ad</code> interfaces with NP offloading enable do not work as expected after a firmware upgrade.
1027537	On the SOC4 platform, L2TP & ETHERIP traffic does not traverse through an IPsec tunnel with NP offload enabled.
1031963	The firewall <code>hit</code> and <code>bytes</code> counts display values of 0 in a policy-based VPN.
1039988	When performing a SAML authentication, <code>authd</code> gets stuck in a loop due to a CPU usage issue.
1041019	When QKD dialup is enabled, IKE SA cannot establish a connection and generates an error.
1042324	The Phase1 monitor BGP remains active when the tunnel is DOWN.
1049015	FortiOS does not enable all available IPsec drivers.
1050646	FortiGate does not always send the full Server Certificate Chain causing disconnections with IKEv2

Bug ID	Description
	VPN using the native Windows client.
1054953	If <i>IKEv2</i> is selected during the VPN FortiClient Remote Access wizard setup in the GUI, the Extensible Authentication Protocol (EAP) configuration cannot be selected using the GUI.
1057165	The IPsec tunnel with QKD experiences flapping each time a DHCP configuration/interface update occurs.
1058691	The IPsec VPN tunnel on the branch unit does not terminate even when the remote gateway IP address becomes unavailable.
1059778	IPsec does not work as expected when the traffic path is <code>spoke dialup to hub1</code> , then from <code>hub1</code> to another site using a site-to-site tunnel.
1060048	Throughput is limited in Site to Site VPN connections between the FW1kF and the FWVM Google Cloud platform.
1061925	IPsec tunnels are flushed when unrelated changes are made in the system.
1073995	Authentication for native iOS IPsec VPN user with FortiToken 2FA does not work as expected.
1075112	FortiGate enters into conserve mode due to IKED encountering a memory usage issue.
1076636	Unexpected behavior in IKED occurs when a peer attempts to negotiate with two different gateway profiles simultaneously.
1077122	The Phase2 SA is present in the kernel but there is no IKE Phase1 SA after an HA upgrade.
1080164	The <code>tcp-mss</code> setting on the tunnel interface does not take affect for IPv6 traffic.
1080420	The IPsec tunnel with FlexVPN Cisco (ASR1006 Cisco IOS XE Software, Version 17.09.05a) is down after 1 minute.
1081951	FortiGate encounters a steadily increasing IKED memory usage issue after upgrading to version 7.4.5.
1082624	EAP doe snot work as expected for local users inherited from the policy. RADIUS users can authenticate and the tunnel can be established.

Log & Report

Bug ID	Description
979200	In a Policy-Based NGFW, if there is no rule hit in <code>central-snat</code> and session never gets established, there will be no traffic log.
1001583	The GUI experiences a performance issue and reverts to the last input when multiple ports are added to a filter for destination ports.
1024570	The SSH deep-inspection with <code>unsupported-version bypass > log information</code> is not showing.

Bug ID	Description
1024990	Some traffic logs show local-out traffic with the vdom-name.
1031342	On the <i>Security Traffic Log > Security</i> tab, the <i>Details</i> page displays data with a <i>1/500 log fetched</i> prompt.
1034824	On the <i>Log & Report > Forward Traffic</i> page, application icons may not display in the <i>Application Name</i> column.
1044092	When filtering forward traffic logs using FortiAnalyzer as a source, data takes longer than expected to load and generates a memory error message.
1045253	FortiGate logs are not transferred into FortiGate Cloud Log server.
1050071	The <code>unset pac-file-data</code> from <code>pac-policy</code> does not generate a system event log and the <code>pac-file-data</code> is deleted.
1053334	The <code>appcat</code> log field is not included in the IoT signature logs.
1053412	Alert email displays an error for <i>FDS-license-expiring</i> .
1060204	When the threat feed download times out, a system event log is not generated.
1060316	Event logs are generated with <i>CLEAR TEXT PASSWORD</i> when using the <code>diagnose test authserver tacacs*... command</code> .
1074236	FortiGate cannot connect to FortiAnalyzer due to a hostname resolution issue.
1083537	The FortiAnalyzer serial number disappears from the FortiGate configuration when the OFTP session disconnects.
1086191	An error condition is observed in the <code>fgtlogd</code> daemon when FortiCloud uses FortiAnalyzer-Cloud for backend logging.
1087067	On the Log Viewer page, the UTM log <i>Matching log</i> page keeps loading under the <i>Log Details > Security</i> tab.
1088385	FortiGate intermittently loses the FortiAnalyzer serial number and is required to verify again the FortiAnalyzer serial number and certificate.
1091064	Forward traffic does not contain the <code>poluuid</code> and <code>polycname</code> fields.

Proxy

Bug ID	Description
916178	FortiGate encounters an issue with the WAD daemon when deep inspection and SSL exemption are enabled while visiting a server with an expired certificate.
979502	On FortiGate, when the <code>waps</code> file is broken, the WAD process does not start.
1018780	FortiGate encounters a memory usage issue caused by the WAD process after an upgrade.
1020828	An HTTP2 stream issue causes an error condition in the WAD.

Bug ID	Description
1042055	On FortiGate, an interruption occurs in the WAD process when in proxy-mode causing the unit to go into memory conserve mode.
1043423	Unexpected behavior is observed in the WAD user info history daemon with no data in messages, caused by erroneous memory allocation.
1047441	On FortiGate, the WAD process may not work as expected with H2 traffic when creating UTM logs.
1048296	FortiGate experiences an HTTP2 framing error when accessing websites using proxy mode with deep inspection configured due to a frame sizing issue in the WAD process.
1051875	The IP SNI check for <code>strict sni-server-cert-check</code> is skipped due to a WAD process issue.
1054052	The WAD process does not load a self-sign certificate when <code>set admin-server-cert self-sign</code> is configured in an explicit proxy.
1056127	An error condition occurs in the WAD process due to a rare error case during the SSL handshake.
1057442	On FortiGate, erroneous memory allocation is observed in the WAD process.
1057488	On FortiGate, unexpected behavior is observed in the WAD process during the HTTP session freeing.
1060812	When Proxy-mode inline IPS scanning is enabled, the botnet check within the IPS profile does not work as expected when the IPS profile is applied to a proxy-based inspection policy using certificate inspection.
1062516	The WAD process does not work as expected when FortiGate is configured as a HTTP load balancer with an HTTP session and changes are made to the virtual server live.
1064758	The <i>Protocol</i> option <code>tcp window size</code> in a proxy policy does not work as expected.
1067014	All wad-workers encounter a gradual memory usage issue, <code>/proc/pid/maps</code> shows increasing symbolic links to <code>/tmp/casb_shm</code> .
1067942	An error occurs in the WAD process when DoH traffic is sent to a transparent proxy after enabling HTTP policy redirect, and without having a transparent proxy configured.
1069896	A wad-worker experiences a memory usage issue increase over several days.
1078385	FortiGate experiences a memory usage issue in the WAD process when sending AVDBs updates from the config daemon to workers.

REST API

Bug ID	Description
1014694	The <code>count</code> and <code>start</code> API request attributes that required for some API endpoints are skipped, causing the REST API to not function as expected.
1057999	REST API returns an HTTP 500 error when <code>ssl-static-key-ciphers</code> is enabled under

Bug ID	Description
	global system settings.
1060135	The API Swagger doc cannot be generated due to incorrect attributes.
1074529	FortiGate is unable to rename the <code>Address</code> object with API <code>cmdb/firewall/address/</code> and Workspace mode transactions.

Routing

Bug ID	Description
969992	On FortiGate, SCTP traffic does not follow the routing table.
981876	The VRRP primary randomly stops sending VRRP advertisement messages for a few seconds.
1003756	When creating a rule on the <i>Network > Routing Objects</i> page, the <i>Prefix-list</i> is set to <code>0.0.0.0 0.0.0.0</code> when an incorrect format is entered in the <i>Prefix</i> field.
1006753	When renewing the LTE WWAN IP, some packets are sent using the old IP address causing traffic to drop.
1011816	The BGP neighbor range with a space in the name is ignored.
1023109	The vlan interface and IPsec tunnel interface are not displayed in the GUI after an upgrade.
1027847	FortiGate does not include the <code>ecmp-max-paths</code> setting in the configuration.
1029460	Creating a BGP IPv4 network prefix or neighbor in the GUI unintentionally creates an empty IPv6 network prefix.
1041812	In a hub and spoke HA configuration, <i>SD-WAN</i> pages take longer than expected to load in the GUI when there are a large number of spokes (~350) configured.
1042909	When creating a new static route on the <i>Network > Static Routes</i> page, the <i>Priority</i> field still displays when the <i>Destination</i> is switched from <i>Subnet</i> to <i>Internet Service</i> .
1046169	On FortiGate, outgoing traffic goes through the wrong interface for local-in traffic coming on an SDWAN interface.
1048338	On FortiGate in an HA setup the secondary HA passive device generates unexpected logs.
1049721	When BGP enables local-as-replace-as and there is a network loop condition, the NLRI's as-path is increased indefinitely.
1051709	On FortiOS, the <i>Routes</i> widget does not list out IPv6 routes with non-zero VRF's.
1057135	The gateway/offload value of offloaded one-way UDP sessions is reset when unrelated routing changes are made.
1057474	FortiGate does not generate a PIM register after stopping and starting a multicast stream.
1057504	FortiGate encounters a multicast routing issue in a VRRP environment.

Bug ID	Description
1058616	On FortiOS, the secondary HA device does not display the <i>SD-WAN Rules</i> tab on the <i>Network > SD-WAN</i> page.
1060456	When hovering over a vlan interface on the <i>SD-WAN Rules</i> tab on the <i>Network > SD-WAN</i> page, the interface shows as disabled in the SD-WAN rule even though it is active.
1061899	Packet are duplicated if the latency between SD-WAN channels differs by more than 250ms.
1069060	Routes are not displayed correctly when the BGP configuration is in a specific order.
1071662	Shortcuts are not created for ADVPN2.0 and BGP on loopback for segregated transports.
1078608	The SD-WAN <code>probe-timeout</code> value is reset to 60000 after rebooting.
1085271	An IGMP membership report with a 0.0.0.0 source does not work as expected in kernel 4.19.13.
1085897	During a graceful restart towards Cisco Nexus causes BGP VPNv4 routes not to enter FIB.
1086828	SD-WAN logs show the parent interface instead of the shortcut interface.
1091628	The secondary IP of an interface is removed from the routing table of other VDOMs when a new VDOM is created.

Security Fabric

Bug ID	Description
873222	The automation email does not show the output of some commands.
948322	After deauthorizing a downstream FortiGate from the <i>System > Firmware & Registration</i> page, the page may appear to be stuck to loading. Workaround: perform a full page refresh to allow the page to load again.
987531	Threat Feed connectors in different VDOMs cannot use the source IP when using internal interfaces.
1007607	When creating a new IPv6 address, SDN connectors cannot be added for dynamic addresses.
1019284	When optimizing a security rating, resolving an alert for one rating causes another alert to appear for another rating and the alerts cycle between both ratings continuously.
1040700	The external connector only allows users to specify the interface in the root vdom and not the vdom it is configured in.
1042972	Cannot test an automation stitch that uses the <i>Schedule</i> trigger from the GUI.
1054407	The Security Rating report does not show test results for downstream FortiGates when the <i>All FortiGates</i> view is selected.
1055616	The <i>Threat feed loaded</i> does not run immediately after restarting FortiGate.

Bug ID	Description
1056262	With a FortiGate configured with a <code>root-vdom</code> and a <code>mgmt-vdom</code> , when an automation stitch is configured for a compromised host with IP-Ban action, the IP is banned from the <code>mgmt-vdom</code> .
1057862	FortiGate models with 2GB of memory that manage many extension devices (FortiSwitches and FortiAPs) may enter conserve mode due to the GUI process experiencing a memory usage issue over time.
1058589	Webhook requests use the same <code>Content-Type: application/json</code> in HTTP headers for all requests, even if it has a custom header.
1075080	The <i>Duplicate Firewall Objects</i> security rating does not work as expected, even it should be passed.
1082980	The AZURE type dynamic firewall address takes longer than normal to resolve itself, even with the correct filter value in the robot test bed.
1088000	The <code>fsvr</code> listens on port 8013 and provides a certificate with <code>set allowaccess fabric</code> .

SSL VPN

Bug ID	Description
943971	On the <i>VPN > SSL-VPN Settings</i> page, when renaming a selected <i>Restrict Access Host</i> object, the object is deselected.
998219	Internet services cannot be used (IPv4 and IPv6) as destination in SSL VPN policies with dual stack enabled.
1042457	Duplicate log entries are created for SSL VPN when the tunnel is up or down.
1046374	An unauthenticated user mismatch occurs with the user.
1047705	SAML login from a Windows FortiClient is blocked when <code>sslvpn-webmode</code> is disabled in the <code>config system global</code> command.
1061165	SSL VPN encounters a signal 11 interruption and does not work as expected due to a word-length heap memory issue.
1066564	SSL VPN SMB is inaccessible when using <i>Web Mode</i> .
1078149	Internal resources cannot be accessed using FortiClient after a network disruption.
1079185	Incorrect maximum values present in CLI schema files.
1082427	The OS checklist for SSL VPN in FortiOS does not include macOS Sequoia 15.0.
1094825	Unexpected behavior caused by SSL VPN when multiple routes are configured with the same address.

Switch Controller

Bug ID	Description
1035823	When trying to start and stop the FortiSwitch LED blink using the Security Fabric, the GUI shows a <i>Failed to send command</i> error.
1038646	The FortiSwitch registration status changes from <i>Not registered</i> to <i>Failed to fetch status</i> when it is deauthorized and then authorized.
1042390	On the <i>WiFi & Switch Controller > SSID</i> page, NAC policies using a Wildcard MAC Address cannot be saved using the GUI. Workaround: use the CLI to perform the operation.
1044150	Upgrading FortiSwitch from the FortiGate GUI does not work as expected when strict and moderate tunnel modes are configured.
1052908	When the name of the FortiSwitch does not match its serial number, it shows up as <i>not registered</i> on the <i>System > Firmware & Registration</i> and <i>Security Fabric > Fabric Connectors</i> pages.
1054445	When editing a dynamic port policy, saved changes are not shown in the GUI.
1055052	On FortiOS, NAC policies disappear from the GUI.
1069164	The incorrect timezone is shown for the managed switch.
1071594	The interface dialog takes longer than expected to load the FortiLink interface page when there are a large number of FortiSwitch VMs (300+).
1073340	On the <i>Firmware</i> page, the <i>Registration Status</i> shows a <i>Failed to fetch status</i> error for an online FortiSwitch. The CLI shows that its registered.
1074981	The FortiGate switch port configuration GUI does not allow the de-selection of all values for <i>Allowed VLANs</i> , <i>Security Policy</i> , or <i>QOS Policy</i> .
1077496	FortiGate encounters a CPU usage issue caused in the <code>flcfgd</code> when receiving multiple messages from the WAD daemon.
1092043	The dynamic VLAN is not visible in the GUI.

System

Bug ID	Description
776290	VLAN sub interface event logs for interface status changes are inaccurate.
894966	ACME certificates cannot be renewed manually before their expiration date.
901621	On the NP7 platform, setting the interface configuration using <code>set inbandwidth <x></code> or <code>set outbandwidth <x></code> commands stops traffic flow.
907752	On FortiGate 1000D models, the SFP 1G port randomly experiences flapping during operation.

Bug ID	Description
920320	FortiGate encounters increasing <code>Rx_CRC_Errors</code> on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices.
952104	FortiGate experiences packet loss when using an internal hardware switch.
960707	Egress shaping does not work on NP when applied on the WAN interface.
976314	After upgrading FortiGate and not changing any configuration details, the output of <code>s_duplex</code> in <code>get hardware nic port</code> command displays <code>Half</code> instead of <code>Full</code> . This is purely a display issue and does not affect system operation.
978290	FortiGate cannot communicate with ACME client and cannot generate certificate.
983467	FortiGate 60F and 61F models may experience a memory usage issue during a FortiGuard update due to the <code>ips-helper</code> process. This can cause the FortiGate to go into conserve mode if there is not enough free memory.
999816	FortiGate 100 models may become unresponsive and prevent access to the GUI, requiring a reboot to regain access due to an issue with the SOC3.
1006685	FortiGate enters a loop cycle and generates a large number of LCAP packets when FortiGate does not receive LCAP packets from a peer device.
1008022	After a restarting FortiGate from the GUI, the <code>auto-nego</code> SFP port settings are not reflected in FortiGate.
1011696	When a SIM card is ejected from a FortiGate using dual SIM cards, the log message does not indicate the slot number FortiOS is switching to.
1015347	After changing the admin profile scope to global, the vdom configuration in the admin user is not consistent with the GUI.
1018843	When FortiGate experiences a memory usage issue and enters into conserve mode, the system file integrity check may not work as expected and cause the device to shutdown.
1020602	After configuring a virtual wire pair (VWP) setting, it is not present in FortiGate after a reboot.
1020921	When configuring an SNMP trusted host that matches the management <i>Admin</i> trusted host subnet, the GUI may give an incorrect warning that the current SNMP trusted host does not match. This is purely a GUI display issue and does not impact the actual SNMP traffic.
1022935	FortiGate experiences a CPU usage issue when <code>dedicated-management-cpu</code> is enabled.
1025114	Insufficient free memory on entry-level Fortigate devices with 2 GB RAM may cause unexpected behavior in the IPS engine.
1029353	The SNMP trap is not sent out when a virus is detected on the antivirus scanner.
1029447	FortiGate encounters increasing <code>Rx_CRC_Errors</code> on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices.
1032018	The SFP+ port LED does not illuminate and displays a speed 10Mbps even though the link status up and speed is set to 1000Mbps.

Bug ID	Description
1032602	FortiGate encounters a memory usage issue on DNS proxy, resulting in FortiGate going into conserve mode.
1034286	FortiGate does not auto negotiate to <code>Full duplex</code> when connecting to FortiSwitch due to a duplication error.
1034821	On FortiGate, NP7 offloaded traffic does not use the updated MAC address from the ARP table to forward traffic using a GRE tunnel.
1039264	The DNS proxy does not forward the response after upgrading FortiGate.
1039564	When the configuration changes using the SSH, a <i>backup failed</i> alert is generated.
1044178	FortiGate does not return an ICMP message with type <i>unreachable</i> and code <code>packet too big</code> with the <code>vne-tunnel</code> .
1045301	Configuration revisions are missing multiple parts of the configuration.
1047996	FortiGate 4800F model split ports do not work as expected causing issues with LACP and MRU on split ports.
1048496	On FortiGate, the <code>snmp</code> daemon does not work as expected resulting in the SNMP queries timing out.
1049119	FortiGate encounters an interruption in the kernel due to a NULL pointer issue.
1050883	Backing up a configuration using SFTP with the domain username does not work when characters <code>@</code> and <code>\</code> are in the username.
1050908	In some scenarios, when FortiGate as a DHCP client sends out <code>DHCP-REQUEST</code> packets, the SRC IP address is set in the IP header.
1051961	On FortiGate, IP addresses cannot be assigned within a configured IP range due to a DHCP server issue.
1053536	On FortiGate, the console displays error messages when adding Pre and Post-login banners due to a rare error condition.
1054294	FortiGate reboots after a connected HA heartbeat cable is connected, or running the <code>diag hardware deviceinfo nic ha</code> command.
1055029	FortiGate cannot get updates from the public FortiGuard servers in FIPS-CC mode.
1055392	The traffic shaper does not take effect on the firewall policy when traffic is offloaded to NP7 due to a traffic management issue.
1055805	Duplicate SNMP traps are sent to <code>ha-direct</code> enabled trap servers when two <code>ha-mgmt-intf</code> are configured.
1056166	In the GUI, <i>Can not create query</i> , <i>check_create_cmf_query</i> , <i>firewall</i> , and <i>ippool_grp</i> errors are displayed.
1056174	FortiOS processes packets on a non-active port of a redundant link.
1056578	The DNS server does not operate as expected with <code>forward-only</code> mode enabled.

Bug ID	Description
1057131	A FortiGuard update can cause the system to not operate as expected if the FortiGate is already in conserve mode. Users may need to reboot the FortiGate.
1057625	FortiGate does not work as expected due to an interruption in the kernel.
1058397	On FortiGate 900 models, when the baudrate is configured, the changes are not applied and is set to 9600.
1059398	The <code>ptp</code> server does not work on the vlan interface.
1061155	Error messages are printed when assigning a transparent vdom to a vdom link interface.
1061334	FortiGate returns a string with a % sign for the OID <code>1.3.6.1.4.1.12356.101.4.8.2.1.8</code> (<code>fgLinkMonitorPacketLoss</code>).
1061413	<code>EXPIRE</code> dates are not displayed properly when executing the <code>get sys fortiguard-service status</code> command due to a formatting issue.
1061796	Inaccurate inbound and outbound traffic values on the <i>Bandwidth</i> widget for the EMAC VLAN interface.
1065047	An error is observed in the dnsproxy caused by the use of secondary dns-database zones.
1065553	FortiGate 80F-DSL models display the incorrect connected route.
1065969	FortiGate does not boot up after restoring a configuration file containing an invalid string format.
1066622	The source IP is not replaced as per the <code>set fmg-source-ip</code> after adding the device directly.
1066655	FortiGate 60F and 40F models become stuck after entering conserve mode and hbddev and console access is lost.
1068150	The DHCP relay uses the wrong interface to send DHCP offer packets to the client.
1069554	Upgrading directly from 7.2.4 or earlier versions to 7.2.9, or directly from 7.0.11 or earlier to 7.2.9 is not supported. Users must upgrade following the recommended upgrade path to avoid system hanging.
1071749	Write permission violation log observed in FortiGate in a rare case caused by the host check plugin used in FortiClient/browser side.
1072320	On FortiGate 400E models, the <i>Link/Activity</i> LED for the <i>MGMT & HA</i> port does not go out even after an <code>exec shutdown</code> command.
1072437	FortiWiFi 61F models experience a memory usage issue caused by the WAD daemon.
1072787	When accessing an IPv6 test site using the IPoE from an iPhone, the IPv6 connection does not work as expected.
1075032	On FortiGate, NP7 offloaded traffic does not use the MAC address of a new default gateway to forward traffic using the EMAC-VLAN interface.
1075585	Shared copper WAN1 and WAN2 ports remain down when the interface speed is set to <code>100full</code> .
1079021	A CPU usage issue in the Softirq space on 40/160 CPU cores causes packets to drop.
1085736	FortiGate cannot restore the configuration file in the following sequence.

Bug ID	Description
	<ol style="list-style-type: none"> 1. <code>private-data-encryption</code> enabled with random key, and configuration is backed up. 2. <code>private-data-encryption</code> disabled. 3. <code>private-data-encryption</code> enabled again, with new random key. 4. Restore configuration file in step 1.
1087109	After a reboot, FortiGate shows the wrong date if the date was set manually prior to the reboot.
1092021	FortiGate logs out when deleting the secondary IP configured on an interface in work space mode.
1093042	FortiGate encounters a memory usage issue caused by the <code>snmpd</code> daemon.

Upgrade

Bug ID	Description
1056126	FortiGate does not boot up properly after an upgrade when it has a large number (500+) of VDOMs configured.

User & Authentication

Bug ID	Description
1003373	FortiGate experiences a gradual memory usage issue in the <code>fnbamd</code> process.
1004258	The Strict-SNI SSL Profile might block connections even if SNI and Certificate CN match.
1008709	EST http password are not encrypted properly in the configuration file.
1009884	FortiGate encounters a CPU usage issue in the <code>authd</code> process after a firmware upgrade.
1036265	The <code>reply-to</code> option under <code>config system alertmail</code> is removed even for custom mail-servers with 2-factor authentication after an upgrade.
1039663	The TACACS+ connection times out, irrespective of the <code>remoteauthtimeout</code> setting, due to an issue with the <code>ldapconntimeout</code> setting, after upgrading to version 7.4.4.
1039771	FortiOS may reply to an FTM push message using a different egress interface instead of the original interface.
1042326	On FortiGate, the <code>two-factor-email-expiry</code> setting in the <code>config system global</code> command is not applicable for administrators.
1042987	NTLM authentication does not work as expected after an upgrade.
1043222	CMPv2 IR does not work as expected due to server certification validation error conditions.
1044084	On the <i>Dashboard > Firewall User Monitor</i> page, the <i>Search</i> field does not display in the GUI when there are a large number (+1000) FSSO user logos.

Bug ID	Description
1045753	An ACME certificate enrollment error is generated without detailed error message information.
1050942	The Active Firewall-Authentication for 2FA FAC RADIUS users using PAP method does not work as expected after upgrading to version 7.4.4.
1060009	On FortiGate, RADSEC sent incorrect accounting packets due to a hashing issue.
1066264	RADIUS message authenticator checking is not optional under TLS.
1070560	Administrator authentication is bypassed when configuring the TACACS server.
1070743	FortiGate does not send a FortiToken activation code, preventing authentication.
1072870	FortiGate initiates LDAPS sessions that do not respect the <code>ssl-min-proto-version</code> option set under the <code>config system global</code> command.
1080234	For FortiGate (versions 7.2.10 and 7.4.5 and later) and FortiNAC (versions 9.2.8 and 9.4.6 and prior) integration, when testing connectivity/user credentials against FortiNAC that acts as a RADIUS server, the FortiGate GUI and CLI returns an <i>invalid secret for the server</i> error. This error is expected when the FortiGate acts as the direct RADIUS client to the FortiNAC RADIUS server due to a change in how FortiGate handles RADIUS protocol in these versions. However, the end-to-end integration for the clients behind the FortiGate and FortiNAC is not impacted.
1080510	When using SCEP, the auto renewal certificate is not initiated.
1086643	FortiGate Captive Portal does not send the full <i>Server Certificate Chain</i> .

VM

Bug ID	Description
953526	The FortiGate-VM OCI may not detect an extra port attached.
972520	The FortiGate-AWS HA secondary <code>awsd debug</code> result prints raw HTML content.
1012927	When FortiGate returns an <i>ICMP TTL-EXCEEDED</i> message, the <code>geneve</code> option field header is missing.
1046696	A FortiGate VM HA in Azure Cloud may intermittently go out of synchronization due to an issue in the daemon process.
1054244	FortiToken does not work as expected after moving a FortiGate-VM license to a new VM with the same serial number.
1058355	FortiGate VM Azure does not work as expected and enters into conserve mode in vWAN setup.
1061669	User may not be able to access FortiGate-KVM with a trial license when there are many <code>virtio_net</code> interfaces.
1066138	FortiGate VM performance drops when traffic passes through an inter-vdom link.
1067046	The <code>awsd</code> does not handle the <code>sts</code> error message and the dynamic firewall address list as expected.

Bug ID	Description
1070910	FortiFlex does not install successfully every time after the Day0 configuration using Port2 for the internet connection.
1072695	The VLAN interface is not reachable on a FortiGate VM running KVM with Intel 10G NIC (10Gb ethernet card).
1073016	The OCI SDN connector cannot call the API to the Oracle service when an IAM role is enabled.
1074600	Inadvertent traffic disruption observed on FortiGate-VM64 caused by a deadlock in the <code>newcli</code> process.
1082197	The FortiGate-VM on VMware ESXi equipped with an Intel E810-XXV network interface card (NIC) using SFP28 transceivers at 25G speed is unable to pass VLAN traffic when DPDK is enabled.
1094274	FortiGate becomes unresponsive due to an error condition when sending IPv6 traffic.

VoIP

Bug ID	Description
1070320	The SIP ALG does not create the expected session for SIP OPTIONS traffic.

Web Application Firewall

Bug ID	Description
1067320	The Web Application Firewall marks http/s traffic as a malformed constraint.
1071022	A matched pattern in the HTTP body cannot be blocked with a <code>waf</code> profile for some content types.

Web Filter

Bug ID	Description
537134	When a webfilter time-based quota is configured, once quota is reached, long sessions are not terminated.
1026023	The webfilter and traffic logs show the incorrect realservice IP address due to a WAD process issue.
1045884	When enabling the <code>log all search keywords</code> in the web filter profile and VDOM mode is disabled, the <i>Key Word</i> column is not populated with data.
1093624	The <code>iprope</code> lookup does not match <code>regex static urlfilter</code> entries.

WiFi Controller

Bug ID	Description
1013290	WIDS data is not removed from the CLI.
1028181	Wi-Fi devices would encounter service delay when roaming over captive-portal SSID with MAC-address authentication.
1033483	The secondary AC <code>wpad_ac</code> encounters a memory usage issue during stress tests with simulators.
1048928	Cannot retrieve DHCP IP's from the assigned VLAN when connecting Bridge SSID with RADIUS-based MAC authentication.
1049471	On FortiGate 90G and 120G models, traffic is dropped due to the MAC address of the VAP interface being updated with the old MAC address when HA is enabled.
1050915	When upgrading more than 30 managed FortiAPs at the same time using the <i>Managed FortiAP</i> page, the GUI may become slow and unresponsive when selecting the firmware.
1059964	RADIUS authentication in a WPA2-Enterprise SSID does not use <code>ha-mgmt-interface</code> when <code>ha-direct</code> is enabled.
1062060	Uzbekistan not in <code>-P</code> , Lower <code>-P</code> 5G power to 20dB EIRP and <code>-P w</code> 6G ch1-93 23dB EIRP not enabled.
1062730	On FortiGate, the <code>set max-clients</code> feature does not work as expected and allows more clients to connect than the maximum value configured.
1073390	FortiGate generates duplicate WiFi event logs when <code>set cw_acd multi-core(set acd-process-count)</code> is enabled.
1073588	Users cannot make any changes to <code>wtp-profile</code> due to an issue with the REST API connection to the <code>cmdbsvr</code> .
1075138	On FortiGate, the <i>Source IP</i> shown in the system logs is not referenced anywhere in the network.
1076738	The <code>user-group</code> is empty after clients pass local authentication with 2FA when connecting Enterprise+User-group SSIDs.
1089563	Client <code>vlanid</code> is lost after roaming between 2 APs when connecting a WPA-PSK(<code>mpsk+vlan</code>) SSID with <code>fast-bss-transition</code> enabled.

ZTNA

Bug ID	Description
1035072	FortiClient access to TCP-FWD with saml authentication does not redirect the loop if <code>set ztna vip</code> and <code>saml SP</code> use the same IP address.

Bug ID	Description
1053309	An interruption occurs in the WAD when accessing ZTNA TCP-forwarding service through a proxy-policy with a SAML user group and <code>h2-support</code> is disabled on the <code>firewall vip</code> .
1056179	PPPoE encounters a performance issue after an upgrade.
1075532	Long sessions without any authentications terminate after 5 hours.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1031370	FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2023-51385

Known issues

Known issues are organized into the following categories:

- [New known issues on page 61](#)
- [Existing known issues on page 61](#)

To inquire about a particular bug or report a bug, please contact [Customer Service & Support](#).

New known issues

The following issues have been identified in version 7.6.1.

Hyperscale

Bug ID	Description
1013892	On FortiGate's in an HA pair, the npd process do not work as expected when trying to manually update the threat feed.

Intrusion Prevention

Bug ID	Description
1076213	FortiGate's with 4GB memory might enter conserve mode during the FortiGuard update when IPS or APP control is enabled. Workaround: Disable the <code>proxy-inline-ips</code> option under <code>config ips</code> settings.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.1.

Endpoint Control

Bug ID	Description
1019658	On FortiGate, not all registered endpoint EMS tags are displayed in the GUI.
1038004	FortiGate may not display the correct user information for some FortiClient instances.

Firewall

Bug ID	Description
959065	On the <i>Policy & Objects > Traffic Shaping</i> page, when deleting or creating a shaper, the counters for the other shapers are cleared.
990528	When searching for an IP address on the <i>Firewall Policy</i> page, the search/filter functionality does not return the expected results.

FortiGate 6000 and 7000 platforms

Bug ID	Description
653335	SSL VPN user status does not display on the FortiManager GUI.
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
936320	When there is a heavy traffic load, there are no results displayed on any <i>FortiView</i> pages in the GUI.
950983	<i>Feature Visibility</i> options are visible in the GUI on a <code>mgmt-vdom</code> .
994241	On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.
998615	When doing a GUI-packet capture on FortiGate, the through-traffic packets are not captured.
1006759	After an HA failover, there is no IPsec route in the kernel.
1014826	SLBC does not function as expected with IPsec over TCP enabled.

FortiView

Bug ID	Description
1034148	The <i>Application Bandwidth</i> widget on the <i>Dashboard > Status</i> page does not display some external applications bandwidth data.

GUI

Bug ID	Description
853352	When viewing entries in slide-out window of the <i>Policy & Objects > Internet Service Database</i> page, users cannot scroll down to the end if there are over 100000 entries.
1047146	After a firmware upgrade, a VLAN interface used in IPsec, SSL VPN, or SD-WAN is not displayed on the interface list or the SD-WAN page and cannot be configured in the GUI.

HA

Bug ID	Description
851743	When running the <code>diag sys ha checksum cluster</code> command, a previous line result is added further down in the output instead of new line result when a FortiGate is configured with several VDOMs .

Hyperscale

Bug ID	Description
1030907	With a FGSP and FGCP setup, sessions do not show on the HA secondary when the FGSP peer is in HA.
1042011	On FortiGate, an login error message displays in the event log after completing an automation.
1093287	Using fixed-allocation IP Pools may cause NP7 NSS/PRP modules to become stuck, potentially disrupting traffic. Other PBA IP pools do not have this issue.

IPsec VPN

Bug ID	Description
735398	On FortiGate, the IKE anti-replay does not log duplicate ESP packets when SA is offloaded in the event log.
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.
995912	After a firmware upgrade, some VPN tunnels experience intermittent signal disruptions causing traffic to be re-routed.
1042371	RADIUS authentication with EAP-TLS does not work as expected through IPsec tunnels.

Log & Report

Bug ID	Description
611460	On FortiOS, the <i>Log & Report > Forward Traffic</i> page does not completely load the entire log when the log exceeds 200MB.

Proxy

Bug ID	Description
1023054	After an upgrade on a 2GB FortiGate device, the firewall policy does not switch from <i>Proxy-based</i> to <i>Flow-based</i> in the <i>Inspection mode</i> field.

REST API

Bug ID	Description
938349	Unsuccessful API user login attempts do not get reset within the time specified in <code>admin-lockout-threshold</code> .
993345	The router API does not include all ECMP routes for SD-WAN included in the <code>get router info routing-table</code> command.
1051870	After a firmware upgrade, some vlan interfaces attached to LAG interface are not displayed in the GUI.

Security Fabric

Bug ID	Description
1011833	FortiGate experiences a CPU usage issue in the <code>Node.js</code> daemon when there multiple administrator sessions running simultaneously.
1019844	In an HA configuration, when the primary FortiGate unit fails over to a downstream unit, the previous primary unit displays as being permanently disconnected.
1040058	The Security Rating topology and results does not display non-FortiGate devices.

Switch Controller

Bug ID	Description
961142	An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.

System

Bug ID	Description
947982	On NP7 platforms, DSW packets are missing resulting in VOIP experiencing performance issues during peak times.

Bug ID	Description
971466	FortiGateRugged 60 models may experience packet loss when directly connected to Cisco switch.
1041726	Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.
1046484	After shutting down FortiGate, the system automatically boots up again.
1047085	The FortiOS GUI is unresponsive due to a CPU usage issue with the <code>csfd</code> and <code>node</code> processes.
1058256	On FortiGate, interfaces with DAC cables remain down after upgrading to version 7.4.4.

Upgrade

Bug ID	Description
1043815	Upgrading the firmware for a large number (100+) of FortiSwitch or FortiAP devices at the same time may cause performance issues with the GUI and some devices may not upgrade. Workaround: pace out the upgrade schedule and upgrade devices in smaller batches.

User & Authentication

Bug ID	Description
802089	User groups from FortiManager are not synchronized across all units except the MBD.
1021719	On the <i>System > Certificates</i> page, the <i>Create Certificate</i> pane does not function as expected after creating a new certificate.
1082800	When performing LDAP user searches from the GUI against LDAP servers with a large number of users (more than 100000), FortiGate may experience a performance issue and not operate as expected due to the HTTPSD process consuming too much memory. User may need to stop the HTTPSD process or perform a reboot to recover. Workaround: Perform an LDAP user search using the CLI.

Web Filter

Bug ID	Description
1040147	Options set in <code>ftgd-wf</code> cannot be undone for a web filter configuration.
1058007	Web filter custom replacement messages in group configurations cannot be edited in FortiGate.

Built-in AV Engine

AV Engine 7.00030 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

Built-in IPS Engine

IPS Engine 7.001014 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.