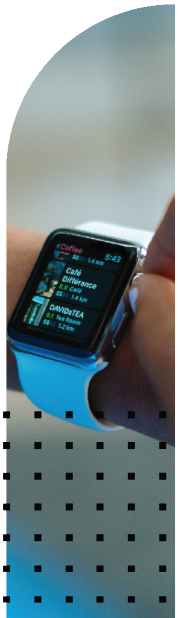
Release Notes

FortiOS 7.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 30, 2021
FortiOS 7.0.0 Release Notes
01-700-661162-20210330

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-03-30	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.0.0 build 0066.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.0 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300E, FG-301E, FG-400E, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`:
  - in FortiOS 6.2.6 and later, set `unsupported-ssl` to `block`.
  - in FortiOS 6.4.3 and later, set `unsupported-ssl-negotiation` to `block`.

Part numbers of unsupported FG-10xF, FGR-60F, and FGR-60F-3G4G Generation 2 models

The following part numbers are Generation 2 models that do not support FortiOS 7.0.0:

- FG-100F-Gen2 P24589-20
- FG-101F-Gen2 P24605-20
- FGR-60F-Gen2 P25210-21
- FGR-60F-3G4G-Gen2 P25587-21

Changes in CLI

Bug ID	Description
570152	Remove redundant `set override` attribute for logging in `config log fortianalyzer override-setting` and `config log syslogd override-setting`.
587183	Remove the intelligent mode option from the IPS global configuration: `config ips global` `  set intelligent-mode {enable | disable}` `end`
640488	Add option to configure the maximum memory usage on the FortiGate's proxy for processing resources, such as block lists, allow lists, and external resources. `config system global` `  set proxy-resource-mode {enable | disable}` `end`
640620	In the `wireless-controller arrp-profile` configuration, the `include-weather-channel` and `include-dfs-channel` options have changed from `yes`/`no` to `enable`/`disable`.
645241	Remove `prp-port-out` and `prp-port-in` settings from `system npu` and replace with the following:. `config system npu setting prp` `  set prp-port-in port-list` `  set prp-port-out port-list` `end`
657726	Remove option to rate images by URL for web filter profile in the GUI and CLI.
666855	FortiOS supports verifying client certificates with RSA-PSS series of signature algorithms, which causes problems with certain clients. Add attribute to control signature algorithms related to client authentication (only affects TLS 1.2): `config vpn ssl settings` `  set client-sigalgs {no-rsa-pss | all}` `end`
673049	When `localid-type address` is configured, users have the option to directly set an ID for IPv4 or IPv6 addresses. `config vpn ipsec phase1` `  set localid-type address` `  set localid <string>` `end`

Bug ID	Description
673747	Support IPv6 in `execute restore` and `execute backup` commands to TFTP and FTP servers.
675511	Update `diagnose debug application virtual-wan-link` to `diagnose debug application sdwan`.
677552	Add `failover-hold-time` to avoid flips caused by monitor interface failure, in seconds (0 - 300, default = 0). `config system ha` `set failover-hold-time <integer>` `end`
682561	Add command, `get system instance-id`.
687197	Allows administrators to set requirements for any number of new characters in a new password, as opposed to a minimum of 4 unique new characters. `config system password-policy` `set min-change-characters <integer>` `end` The `set change-4-characters {enable | disable}` option has been removed.
690981	Daily hit counts for central NAT and DNAT can now be displayed in the CLI using the following commands: `# diagnose firewall iprope show 10000d <index>` `# diagnose firewall iprope show 100000 <index>`
695259	Rename the following setting: `config system dns` `set dns-over-tls {disable | enable | enforce}` `end` To: `config system dns` `set protocol {cleartext | DoT | DoH}` `end`
695979	Support wildcard MAC addresses in firewall address for users to easily use pattern matching, like vendor prefix, to define a group of addresses. The MAC address range is now defined by specifying <start> - <end> in a single field, instead of defining a `start-mac` and `end-mac`. Multiple addresses can be defined in a single line. `config firewall address` `edit "address"` `set type mac` `set macaddr 00:0c:29:8d:7e:e3 00:0c:**:8d:7*:e3 00:0c:29:8d:7e:e3-00:22:29:8d:7e:e` `next` `end`

Changes in GUI behavior

Bug ID	Description
690715	Allow users to create a virtual wire pair policy that includes multiple virtual wire pairs. This reduces overhead in creating multiple similar policies for each virtual wire pair. This feature is supported in NGFW and policy mode.
691699	Improve the Fabric automation configuration to simplify the workflow for managing multiple chained actions, and to make it clearer which order the actions will be processed in. Enhancements include: • New flow for creating and managing automation stitches, triggers, and actions. • New *Manage Components* view to manage automation triggers and actions from the list page. • Allow multiple log IDs and log field filters for the FortiOS Event Log trigger. • Add *Any* report type trigger for the Security Rating report. • Simplify URI configuration for cloud actions. • Add JSON parameter support for Slack and Microsoft Teams notifications.
696731	Add the following updates to the navigation menu: **1.** Re-order the *System* and *Security Fabric* menus. **2.** Merge *SD-WAN Zones*, *SD-WAN Rules*, and *Performance SLAs* under a single *SD-WAN* menu item. **3.** Merge *Traffic Shapers*, *Traffic Shaping Policies*, and *Traffic Shaping Profiles* under a single *Traffic Shaping* menu item. **4.** Introduce tabs for the *SD-WAN* and *Traffic Shaping* pages.

Changes in default behavior

Bug ID	Description
230997	Do not allow `match-vip` in firewall policies when the action is set to accept.
537354	Interface egress shaping offload to NPU when `shaping-offload` is enabled.
598614	When a group and a `user-peer` is specified in an SSL VPN authentication rule, and the same group appears in multiple rules, each group and `user-peer` combination can be matched independently.
670676	When there are multiple ECMP routes to a BGP next hop that requires recursive resolution, the previous behavior selects only the first ECMP route for the resolution. In this enhancement, all ECMP routes are considered for the next hop recursive resolution.
673609	The auto-join FortiCloud re-try timer has changed from 600 seconds to 60 seconds.
690712	When there is an IGMP query from 0.0.0.0 coming to the FortiGate, the FortiGate will not allow this query to change its IGMP querier role.

Changes in table size

Bug ID	Description
665668	Increase IPIP tunnel table size from 256 per VDOM and 512 globally to 1024 per VDOM and 1024 globally.
698043	VLAN pooling in SSIDs allows load-balancing users into various VLANs. To service larger deployments, FortiGate 2U and high-end models now support up to 64 VLANs.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
489956	Add a new LAG implementation so each session uses the same NP6 and XAUI for ingress and egress direction to avoid the fast path congestion (the default value is `disable`). `config system npu` `  set lag-out-port-select {enable | disable}` `end` Add a new algorithm in the NPU driver to the bond algorithm list (AGG_ALGORITHM_NPU).
497049	Support HTTP2 in proxy mode by adding the ability to inspect HTTP2 via ALPN. `config firewall ssl-ssh-profile` `  edit <name>` `  set supported-alpn {http1-1 | http2 | all | none}` `  next` `end`
520385	Allow denied sessions to be offloaded by the NPU when session-denied traffic is also enabled. This enables sessions to be offloaded for packets that are denied by the firewall policy, which can help reduce CPU usage. `config system npu` `  session-denied-offload {enable | disable}` `end`
609692	Add new setting to enable auto provisioning of FortiSwitch firmware upon authorization. On FortiGate models with a disk, up to four images of the same FortiSwitch model can be uploaded. On FortiGate models without a disk, one image of the same FortiSwitch model can be uploaded.
611992	Add a specific `auth-timeout` field in the SSL VPN monitor.
618359	In scenarios where the FortiGate is sandwiched by load-balancers and SSL processing is offloaded on the external load-balancers, the FortiGate can perform scanning on the unencrypted traffic by specifying the `ssl-offloaded` option in the protocol options profile. This was previously supported in proxy mode only, but now it is also supported in flow mode.
621725	Add settings to enable flow control and pause metering. Pause metering allows the FortiSwitch to apply flow control to ingress traffic when the queue is congested and to resume once it is cleared.
621728	On supported managed switch ports, the FortiGate allows the port to be configured with a forward error correction (FEC) state of Clause 74 FC-FEC for 25 Gbps ports, or Clause 91 RS-FEC for 100 Gbps ports. `config switch-controller managed-switch` `  edit <serial number>` `  config ports`

Bug ID	Description
	`` edit <name> set fec-state {disabled | cl74 | cl91} next end next end ```
622053	Add RADIUS CoA support for SSL-VPN. After receiving a `Disconnect Request(40)` from a RADIUS server, the SSL VPN daemon will search related sessions according to user name and RADIUS server name to log off the specific user (including web and tunnel session).
630468	Make the following enhancements to the antiphishing profile: • Allow username and password field patterns to be fetched from FortiGuard. • Add DNS support for domain controller IP fetching. • Add support to specify a source IP or port for the fetching domain controller. • Add LDAP server as a credential source. • Block or log valid usernames regardless of password match. • Add literal custom patterns type for username and password.
634006	OpenSSL updated to 1.1.1j for security fixes.
635344	Add *XAuth User* to VPN chart in the PDF report.
637108	In 6.2, stream-based AV scan was added in proxy mode for HTTP(S). This is now supported for FTP(S), SFTP, and SCP. The stream-based scan optimizes memory utilization for large archive files like ZIP, TAR.GZ, and so on by decompressing the files on the fly and scanning files as they are extracted. Smaller files can also be scanned directly on the proxy-based WAD daemon, improving traffic throughput.
637552	Enhance freestyle log filtering so that users can specify more powerful filters. The config free-style setting is added to log filters for each log device. For example: ``` config log memory filter config free-style edit 1 set category {event | virus | webfilter | attack | spam | anomaly | voip | dlp | app-ctrl | waf | gtp | dns | ssh | ssl | file-filter | icap} set filter <string> set filter-type include next end end ``` The filter string can be a legal regular filter string. For example, `((srcip 172.16.1.1) or (dstip 172.16.1.2)) and (dstport 80 443 50-60).`
638352	To avoid large number of new IKEv2 negotiations from starving other SAs from progressing to established states, the following enhancements have been made to the IKE daemon: • Prioritize established SAs. • Offload groups 20 and 21 to CP9.

Bug ID	Description
	• Optimize the default embryonic limits for mid- and high-end platforms. The IKE embryonic limit can now be configured in the CLI. `config system global` `  set ike-embryonic-limit <integer>` `end`
641077	After authorizing a FortiAP, administrators can also register the FortiAP to FortiCloud directly from the FortiGate GUI.
641524	Add interface selection for IPS TLS protocol active probing. `config ips global` `  config tls-active-probe` `  set interface-selection-method {auto | sdwan | specify}` `  set interface <interface>` `  set vdom <VDOM>` `  set source-ip <IPv4 address>` `  set source-ip6 <IPv6 address>` `  end` `end`
644218	The host protection engine (HPE) has been enhanced to add monitoring and logging capabilities when the HPE is triggered. Users can enable or disable HPE monitoring, and configure intervals and multipliers for the frequency when event logs and attack logs are generated. These logs and monitors help administrators analyze the frequency of attack types and fine-tune the desired packet rates in the HPE shaper. `config monitoring npu-hpe` `  set status {enable | disable}` `  set interval <integer>` `  set multiplers <m1>, <m2>, ... <m12>` `end` The interval is set in seconds (1 - 60, default = 1). The multiplies are twelve integers ranging from 1 - 255, the default is `4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, 8`. An event log is generated after every (interval × multiplier) seconds for any HPE type when drops occur for that HPE type. An attack log is generated after every (4 × multiplier) number of continuous event logs.
644235	Support reference to any action results in chained actions of automation stitches.
647800	AWS and Azure now support FIPS ciphers mode.
648595	A custom IKE port and IKE NAT-T port can be specified to replace the default UDP/500 and UDP/4500 respectively for IKE negotiation. `config system settings` `  set ike-port <1024-65535>` `  set ike-natt-port <1024-65535>` `end`

Bug ID	Description
648602	When creating a Cisco ACI direct connector, configuring multiple IPs allows the FortiGate to connect to the server in a round-robin fashion. Only one server will be active and the remaining will serve as backups if the active one fails.
650416	On IBM VPC Cloud, users can deploy their BYOL FortiGate VMs in unicast HA. HA failover triggers routing changes and floating IP reassignment on the IBM Cloud automatically via the API.
651866	FortiSwitch events now have their own category on the *Events* log page.
652003	In a tenant VDOM, allow `lldp-profile` and `lldp-status` to be configurable on a leased switch port.
652503	By configuring the service chain and service index, NSX-T east-west traffic can be redirected to a designated FortiGate VDOM. `config nsxt setting` `set liveness {enable | disable}` `set service <service name>` `end` `config nsxt service-chain` `edit <ID>` `set name <chain name>` `config service-index` `edit <forward index>` `set reverse-index <value>` `set name <index name>` `set vd <VDOM>` `next` `end` `next` `end` The default value for `reverse-index` is 1. The `vd` setting is required.
654032	The route tag is a mechanism to map a BGP community string to a specific tag. The string may correspond to a specific network that a BGP router advertised. Using this tag, an SD-WAN service rule can be used to define specific handling of traffic to that network. In this enhancement, IPv6 route tags are now supported.
655388	When units are out-of-sync in an HA cluster, the GUI will now compare the HA checksums and display the tables that caused HA to be out-of-sync. This can be visualized in the HA monitor page and the *HA Status* widget.
655942	Add new commands `execute telnet-options` and `execute ssh-options` to allow administrators to set the source interface and address for their connection.
656039	Allow SD-WAN duplication rules to specify SD-WAN service rules to trigger packet duplication. This allows SD-WAN duplication to occur based on an SD-WAN rule instead of the source, destination, or service parameters in the duplication rule.
657598	In an application control list, the `exclusion` option allows users to specify a list of applications they wish to exclude from an entry filtered by category, technology, or others.

Bug ID	Description
	`config application list` `edit <list>` `config entries` `edit 1` `set category <ID>` `set exclusion <signature ID> ... <signature ID>` `next` `end` `next` `end`
657812	When an SSL inspection profile is configured to protect the SSL server, multiple sites can potentially be deployed on the same protected server IP. This change adds support for multiple SSL certificates to attach to a SSL profile, allowing inspection based on matching SNI in the certificate.
658096	Add four new SNMP OIDs for polling the number of packets and bytes that conform to traffic shaping, or are discarded by traffic shaping.
658206	New REST API `POST /api/v2/monitor/vpn/ike/clear?mkey=<gateway_name>` will bring down IKE SAs tunnel the same way as `diagnose vpn ike gateway clear`.
658525	The limit of BGP paths that can be selected and advertised has increased to 255 (originally 8).
659105	Add a toggle to return node IP addresses only in dynamic firewall addresses for Kubernetes SDN connectors.
659127	Add support to deploy FortiGate-VMs that are paravirtualized with SR-IOV and DPDK/vNP on OCI shapes that use Mellanox network cards.
659346	Add additional information such as DHCP server MAC, gateway, subnet, and DNS to wireless DHCP logs.
660250	Add global option `fortiipam-integration` to control FortiIPAM. When enabled, ipamd will run and report to FortiIPAM to allow automatic IP address/subnet management. `config system global` `set fortiipam-integration {enable | disable}` `end`
660273	By default, the FortiGate uses the outbound interface's IP to communicate with a FortiSwitch managed over layer 3. The `switch-controller-source-ip` option allows the switch controller to use the FortiLink fixed address instead.
660283	Add system event logs for the execution of CLI commands. When `cli-audit-log` is enabled under `system global`, the execution of `execute`, `config`, `show`, `get`, and `diagnose` commands will trigger system event logs.
660295	Provide specific SNMP objects (OIDs) that allow the status of the mobile network connection to be monitored.

Bug ID	Description
660596	Because pre-standard POE devices are uncommon in the field, `poe-pre-standard-detection` is set to `disable` by default. Upgrading from previous builds will carry forward the configured value.
660624	When enabling the Security Fabric on the root FortiGate, the following FortiAnalyzer GUI behavior has changed: • If a FortiAnalyzer appliance is enabled, then the dialog will be for the *FortiAnalyzer* connector. • If a FortiAnalyzer appliance is disabled but *FortiAnalyzer Cloud* is enabled, then the dialog will be for the *Cloud Logging* connector. • If neither the FortiAnalyzer appliance or FortiAnalyzer Cloud are enabled: • If the device has a FAZC (standard FortiAnalyzer Cloud subscription) or AFAC (premium subscription) entitlement, then the dialog will be for the *Cloud Logging* connector. • If the device does not have a FAZC or AFAC entitlement, then the dialog will be for the *FortiAnalyzer* connector. • When *FortiAnalyzer Cloud* is enabled and the FortiAnalyzer appliance is disabled, then the *Cloud Logging* connector will not let you switch to the *FortiGate Cloud* FortiAnalyzer.
660653	The Wi-Fi Alliance Agile Multiband Operation (MBO) feature enables better use of Wi-Fi network resources in roaming decisions and improves overall performance. This enhancement allows the FortiGate to push the MBO configuration to managed APs, which adds the MBO information element to the beacon and probe response for 802.11ax.
661105	Support FGSP four-member cluster session synchronization and redundancy.
661131	Enabling IGMP snooping on an SSID allows the wireless controller to detect which FortiAPs have IGMP clients. The wireless controller will only forward a multicast stream to the FortiAP where there is a listener for the multicast group.
661252	Add object synchronization improvements: • Simplify the conflict resolution procedure so a multi-step wizard is no longer required. All conflicts appear in one table for all FortiGates in the Fabric and supported tables. • Add an object diff feature to display the difference between FortiGate objects that are in conflict. • Add new CLI command for the root FortiGate: `config system csf` `  set fabric-object-unification {default | local}` `end` When set to `default`, objects will be synchronized in the Security Fabric. On downstream FortiGates, if `configuration-sync` is set to `local`, the synchronized objects from the root to downstream FortiGates is not applied locally. However, the device will still send the configuration to lower FortiGates. • The `fabric-object {enable | disable}` command was added to the following tables: • `firewall.address` • `firewall.address6` • `firewall.addrgrp`

Bug ID	Description
	• `firewall.addrgrp6` • `firewall.service.category` • `firewall.service.group` • `firewall.service.custom` • `firewall.schedule.group` • `firewall.schedule.onetime` • `firewall.schedule.recurring` Enabling `fabric-object` on the root starts synchronizing this object as a Fabric object to downstream devices. Disabling `fabric-object` makes the object local to the device. • Add setting to define how many task worker process are created to handle synchronizations (1 - 4, default = 2). The worker processes dies if there is no task to perform after 60 seconds. `config system csf` `set fabric-workers <integer>` `end`
662437	When a FortiSwitch upgrade is stuck due to connectivity issues, the following command allows the process to be cancelled. `# execute switch-controller switch-software cancel {all | sn | switch-group}`
663206	When an AliCloud SDN connector is configured, dynamic address objects can support Kubernetes filters based on cluster, service, node, pod, and more.
663530	IoT background scanning is disabled by default. Users can enable this option on the *FortiLink Interface* page in the GUI or with the `switch-controller-iot-scanning` in the CLI.
663877	Add *Application Bandwidth* widget: • It can be added to a dashboard to display bandwidth utilization for the top 50 applications. • The favorites will be included even if they are not in the top 50. • A firewall policy must have an application profile configured so the widget can capture information. • A new CLI was added.
664312	Integrate Broadcom bnxt_en 1.10.1 driver to drive new vfNIC to replace 1.9.2 version. The following new cards are supported: • [BCM57508] = { "Broadcom BCM57508 NetXtreme-E 10Gb/25Gb/50Gb/100Gb/200Gb Ethernet" } • [BCM57504] = { "Broadcom BCM57504 NetXtreme-E 10Gb/25Gb/50Gb/100Gb/200Gb Ethernet" } • [BCM57502] = { "Broadcom BCM57502 NetXtreme-E 10Gb/25Gb/50Gb Ethernet" } • [BCM57508_NPAR] = { "Broadcom BCM57508 NetXtreme-E Ethernet Partition" } • [BCM57504_NPAR] = { "Broadcom BCM57504 NetXtreme-E Ethernet Partition" } • [BCM57502_NPAR] = { "Broadcom BCM57502 NetXtreme-E Ethernet Partition" } • [BCM58812] = { "Broadcom BCM58812 NetXtreme-S 2x50G Ethernet" } • [BCM58814] = { "Broadcom BCM58814 NetXtreme-S 2x100G Ethernet" }

Bug ID	Description
	• [BCM58818] = { "Broadcom BCM58818 NetXtreme-S 2x200G Ethernet" } • [NETXTREME_E_P5_VF] = { "Broadcom BCM5750X NetXtreme-E Ethernet Virtual Function" }
664826	When multi-VDOM mode is enabled, the threat feed external connector can be defined in global or within a VDOM. Global threat feeds can be used in any VDOMs, but are not editable within the VDOM. FortiGuard category and domain name based external feeds have added a category number field to identify the threat feed.
665186	Add Security Rating test, *Activate FortiCloud Services*, to check whether FortiCloud services can be activated for FortiAnalyzer Cloud, FortiManager Cloud, FortiClient EMS Cloud, and FortiSandbox Cloud. If the account has a valid subscription to a service or cloud appliance, but the Fabric connection to it on the FortiGate is not enabled, then the test fails.
665735	The user device store allows user and device data collected from different daemons to be centralized for quicker access and performance: `diagnose user-device-store device memory list` `diagnose user-device-store device memory query mac <value>` `diagnose user-device-store device memory query ip <value>` `diagnose user-device-store device disk list` `diagnose user-device-store device disk query <SQL WHERE clause>`
668362	Support multiple LDAP server configurations for Kerberos keytab and agentless NTLM domain controller in multiple forest deployments.
668487	In NGFW policy mode, application groups can be defined with the following filters: risk, protocols, vendor, technology, behavior, and popularity.
668991	Security Fabric rating reports can now be generated in multi-VDOM mode, against all VDOMs. The Security Rating is visible under Global scope.
669033	Backend update to support a TCP connection pool to maintain local-out TCP connections to the external ICAP server.
669158	The SD-WAN Network Monitor service now supports running a speed test based on a schedule. The test results are automatically updated in the interface `measured-upstream-bandwidth` and `measured-downstream-bandwidth` fields. When the scheduled speed tests run, it is possible to temporarily bypass the bandwidth limits set on the interface and configure custom maximum or minimum bandwidth limits. These configurations are optional.
669487	Web traffic over HTTP/HTTPS can be forwarded selectively by the FortiGate's transparent web proxy to an upstream web proxy to avoid overwhelming the proxy server. Traffic can be selected by specifying the proxy address, which can be based on a FortiGuard URL category.
670677	When a BGP next hop requires recursive resolution, the default behavior is to consider all other routes except BGP routes. The following option, when enabled, allows the recursive next hop resolution to use BGP routes as well. `config router bgp` `  set recursive-next-hop {enable | disable}`

Bug ID	Description
	`end`
671563	Add option to switch between *Peer* and *Peer Group* view on *PKI* user page.
672573	FortiExtender and VPN tunnel interfaces now support NetFlow sampling. VPN tunnel interfaces can be IPsec, IP in IP, or GRE tunnels. NetFlow sampling is supported on NPU and non-NPU offloaded tunnels.
673072	When a HTTP request requires authentication in an explicit proxy, the authentication can be redirected to a secure HTTPS captive portal. Once authentication is done, the client can be redirected back to the original destination over HTTP.
673205	In *Dashboard* > *Users and Devices*, administrators can use the *FortiSwitch NAC VLANs* widget to see which devices have been added to which VLANs by the NAC policy. A donut chart overview summarizes the number of devices in each VLAN.
673371	Support ICMP type 13 at local interface.
673590	Policy hit counters are now seven-day rolling counters. Instead of storing a single number for the hit count and byte count collected since the inception of each policy, seven numbers for the last seven days plus an active counter for the current day are stored. The past seven-day hit count is displayed on the policy list and policy dialog page. A seven-day bar chart for additional visualization of the statistics has been added. These changes help put the policy hit count comparison on the same footing.
674507	Using the ARM64_KVM image, users can deploy the FortiGate VM on KVM hypervisors running ARM64 processors.
674653	In order to support packet duplication on dial-up IPsec tunnels between sites, each spoke must configure a location ID. On the dial-up VPN hub, packet duplication can be performed on tunnels in the IPsec aggregate with the same location ID. `config system settings` `  set location-id <IPv4 address>` `end`
674724	Once an incoming webhook connector is created in Microsoft Teams, this webhook URL can be used in an automation stitch under the action Microsoft Teams connector. `config system automation-action` `  edit <action name>` `  set action-type microsoft-teams-notification` `  next` `end`
675049	Add support for PRP (Parallel Redundancy Protocol) in NAT mode for a virtual wire pair. This preserves the PRP RCT (redundancy control trailer) while the packet is processed by the FortiGate.
675200	Improve SOCKS/SSH proxy to support `internet-service`.
675401	Provide options for controlling concurrent TCP/UDP connections by introducing a connection quota in the per-IP shaper and a port quota in the fixed port range type IP pool.

Bug ID	Description
675958	A DNS health check monitor can be configured for server load balancing. The monitor uses TCP or UDP DNS as the probes. The request domain is matched against the configured IP address to verify the response. `config firewall ldb-monitor` `edit <name>` `set type dns` `set port <string>` `set dns-protocol {udp | tcp}` `set dns-request-domain <string>` `set dns-match-ip <class_ip>` `next` `end`
676063	Add support for OCI IMDSv2 that offers increased security for accessing instance metadata compared to IMDSv1. IMDSv2 is used in OCI SDN connectors and during instance deployments with bootstrap metadata.
676260	FortiGates with a premium subscription (AFAC contract) for cloud-based central logging and analytics are able to send traffic logs to FortiAnalyzer Cloud, in addition to UTM logs and event logs. FortiGates with a standard FortiAnalyzer Cloud subscription (FAZC contract) can send UTM and event logs only.
676484	When configuring the generic DDNS service provider as a DDNS server, the server type and address type can be set to IPv6. This allows the FortiGate to connect to an IPv6 DDNS server and provide the FortiGate's IPv6 interface address for updates. `config system ddns` `edit <name>` `set ddns-server genericDDNS` `set server-type {ipv4 | ipv6}` `set ddns-server-addr <address>` `set addr-type ipv6 {ipv4 | ipv6}` `set monitor-interface <port>` `next` `end`
676549	The past seven-day hit count is displayed on the policy list page and the policy dialog page for IPv4 and IPv6 multicast policies. A seven-day bar chart for additional visualization of the statistics has been added.
676577	Introduce FortiGuard updates for OUI files used to identify device vendors by MAC address. This database is used in WiFi and device detection.
677334	Add support for MacOS Big Sur 11.1 in SSL VPN OS check.
677672	Support running both BYOL and on-demand type FGT-VMs on ARM-based Graviton2 EC2 instances on AWS.

Bug ID	Description
677750	The *Local Out Routing* page consolidates features where a source IP and an outgoing interface attribute can be configured to route local out traffic. The outgoing interface has a choice of *Auto*, *SD-WAN*, or *Specify* to allow granular control over the interface in which to route the local out traffic. *Local Out Routing* must be enabled from *System > Feature Visibility*, and it supports multi-VDOM mode.
677784	Add commands to debug traffic statistics for traffic monitor interfaces (`interface`), interface traffic in real-time data (`peek`), and to dump interface traffic history data (`history`): `# diagnose debug traffic {interface | peek | history}`
678783	Add option for users to set a non-default SD-WAN member zone for OCVPN IPsec interfaces. The `sdwan-zone` option is only available if SD-WAN is enabled. `sdwan-zone` references the entries in the SD-WAN configuration, and the default is `virtual-wan-link`. `config vpn ocvpn` `...` `set sdwan enable` `set sdwan-zone {virtual-wan-link | <zone> | ...}` `...` `end`
679175	Add `interface-select` option for `email-server`. `config system email-server` `set interface-select-method {auto | sdwan | specify}` `set interface <interface>` `end`
680599	Increase the ICMP rate limit to allow more ICMP error message to be sent by the FortiGate per second. The ICMP rate limit has changed from 1 second (100 jiffies) to 10 milliseconds (1 jiffy).
681600	Add support for syslog RFC 5424 format, which can be enabled when the syslog mode is UDP or reliable. `config log syslogd setting` `set format {default | csv | cef | RFC5424}` `end`
682106	If a FortiCloud account has a FortiManager Cloud account level subscription (ALCI), a FortiGate registered to the FortiCloud account can recognize it and enable FortiManager Cloud central management.
682480	Flow-based SIP inspection is now done by the IPS engine. Proxy ALG features that are supported in flow mode include blocking scenarios, rate limitation, and malformed header detection. Inspection mode is selected at the firewall policy level.
683791	From the CLI, users are allowed to enable malware threat feeds and outbreak prevention without performing an AV scan. In the GUI and CLI, users can choose to use all malware thread feeds, or specify the ones they want to use. New replacement message for external block lists have been added.

Bug ID	Description
	config antivirus profile edit <name> config http set av-scan {disable | block | monitor} set outbreak-prevention {disable | block | monitor} set external-blocklist {disable | block | monitor} set quarantine {enable | disable} end set outbreak-prevention-archive-scan {enable | disable} set external-blocklist-archive-scan {enable | disable} set external-blocklist-enable-all {enable | disable} set external-blocklist <source> next end Note that the external-blocklist <source> option is hidden if external-blocklist-enable-all is enabled.
684133	Support site-to-site IPsec VPN in an asymmetric routing scenario with a loopback interface as a VPN bound interface. config vpn ipsec phase1-interface edit <name> set interface "loopback" set loopback-asymroute {enable | disable} next end
687282	When FortiGuard DDNS is configured as a DDNS server, the server type and address type can be set to IPv6. This allows the FortiGate to connect to FortiGuard over IPv6 and provide the FortiGate's IPv6 interface address for updates.
689140	FortiAI can be added to the Security Fabric so it appears in the topology views and the dashboard widgets.
689150	When the detect server becomes unavailable in a link monitoring configuration, instead of removing all routes associated with the gateway and interface defined in the link monitor, only remove specific routes. These subnets can be specified in the link-monitor configuration. config system link-monitor edit <id> set srcintf <interface> set server <server IP> set gateway-ip <gateway IP> **set route <subnet 1> ... <subnet n>** next end

Bug ID	Description
689174	Adds support for Layer 3 unicast `standalone config sync`. This allows peers to be synchronized in cloud environments that do not support Layer 2 networking, which expands support for auto-scale scenarios. Configuring a unicast gateway allows peers to be in different subnets altogether (this is an optional setting). `config system ha` `  set unicast-status enable` `  set unicast-gateway <address>` `  config unicast-peers` `  edit 1` `  set peer-ip <address>` `  next` `  ...` `  end` `end`
690179	The SD-WAN REST API for health-check and sla-log now exposes ADVPN shortcut information in its result. The `child_intfs` attribute returns the statistics for the corresponding shortcuts. The following command displays real-time SLA information for ADVPN shortcuts: `# diagnose sys sdwan sla-log <health check name> <sequence number> <child name>`
690688	Add UX enhancements: • When selecting objects, the omni-select menu displays recently used items. • Support nested object tooltips.
690691	The radio transmit power can now be configured in dBm or as a percentage in FortiAP profiles and override settings.
690801	FortiDeceptor can be added to the Security Fabric so it appears in the topology views and the dashboard widgets.
691340	DHCP address enforcement ensures that clients who connect must complete the DHCP process to obtain an IP address; otherwise, they are disconnected from the SSID. This prevents users with static addresses that may conflict with the DHCP address scheme, or users that fail to obtain a DHCP IP assignment to connect to the SSID.
691411	Ensure EMS logs are recorded for dynamic address related events under *Log & Report* > *Events* > *SDN Connector Events* logs: • Add EMS tag • Update EMS tag • Remove EMS tag
691676	Wireless controller now supports NAC profiles to onboard wireless clients into default VLANs. It can also apply NAC policies to match clients based on device properties, user groups or EMS tags, and assign clients to specific VLANs. VLAN sub-interfaces based on the VAP interfaces are used for the VLAN assignment.

Bug ID	Description
691902	Support pulling malware threat feeds from FortiClient EMS, which in turn receives malware hashes detected by FortiClients. The malware hash can be used in an antivirus profile when AV is enabled with block or monitor actions.
693799	Add the following enhancements for `voice-enterprise` SSID: • Support 802.11k neighbor report dual band. • Enhance 802.11v BSS transition management by adding `bstm-disassociation-imminent` option, disassociation timer for low RSSI, and disassociation timer for AP load-balancing.
694148	Support file filter profile in a one-arm sniffer policy in the GUI and CLI.
695259	Adds support for DNS over TLS (DoT) and DNS over HTTPS (DoH) in DNS inspection. Prior to 7.0, DoT and DoH traffic silently passes through DNS proxy. In 7.0, WAD is able to handle DoT and DoH, and redirect DNS queries to the DNS proxy for further inspection. `config firewall ssl-ssh-profile` `edit "dot-deep"` `config dot` `set status deep-inspection` `set client-certificate bypass` `set unsupported-ssl-cipher allow` `set unsupported-ssl-negotiation allow` `set expired-server-cert block` `set revoked-server-cert block` `set untrusted-server-cert allow` `set cert-validation-timeout allow` `set cert-validation-failure block` `end` `next` `end`
695855	In the wireless controller settings, add options to specify the delimiter used for various RADIUS attributes for RADIUS MAC authentication and accounting. The options are hyphen, single-hyphen, colon, or none. `config wireless-controller vap` `edit <name>` `set mac-username-delimiter {hyphen | single-hyphen | colon | none}` `set mac-password-delimiter {hyphen | single-hyphen | colon | none}` `set mac-calling-station-delimiter {hyphen | single-hyphen | colon | none}` `set mac-called-station-delimiter {hyphen | single-hyphen | colon | none}` `set mac-case MAC {uppercase | lowercase}` `next` `end`

Bug ID	Description
695983	In a scenario where a tunnel mode SSID or a VLAN sub-interface of an SSID is bridged with other interfaces via a software switch, support is added to allow captive portal authentication on the SSID or VLAN sub-interface. This requires that `intra-switch-policy` is set to `explicit` from the CLI when the switch interface is created. Users accessing the SSID will be redirected to the captive portal for authentication.
698462	Add the ability to perform SD-WAN passive WAN health measurement, which reduces the amount of configuration required and decreases the traffic that is produced by health check monitor probes doing active measurements. The passive and prefer-passive detection modes rely on session information captured in firewall policies with `passive-wan-health-measurement` enabled. `config system sdwan` `  config health-check` `  edit <name>` `  set detect-mode {active | passive | prefer-passive}` `  next` `  end` `end` `config firewall policy` `  edit <id>` `  set passive-wan-health-measurement {enable | disable}` `  next` `end`
699161	Allows service assurance management (SAM) mode to be configured from the CLI, where a radio is designated to operate as a client and perform tests against another AP. Ping and iPerf tests can run on an interval and the results are captured in the Wi-Fi event logs. This allows the FortiGate to verify and assure an existing Wi-Fi network can provide acceptable services.
701185	Support DoT and DoH in explicit mode, where FortiGate acts as an explicit DNS server listening for DoT and DoH requests. Add support for local-out DNS traffic over TLS and HTTPS.
705248	The new GUI retro theme showcases a style of FortiOS giving homage to FortiOS 3.0. To enable it, go to *System* > *Settings*. Under *View Settings*, for *Theme*, select *FortiOS v3 Retro*.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.0.0 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 7.0.0
- FortiManager 7.0.0
- FortiClient EMS 6.4.3 build 1600 or later
- FortiClient 6.4.3 build 1608 or later
- FortiAP 6.4.4 build 0456 or later
- FortiSwitch 6.4.5 build 0461 or later

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

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS

13. FortiWLC
14. FortiNAC
15. FortiVoice
16. FortiDeceptor
17. FortiAI

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.0. When Security Fabric is enabled in FortiOS 7.0.0, all FortiGate devices must be running FortiOS 7.0.0.

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 select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Strong cryptographic ciphers

FortiOS 7.0.0 has reinforced strong cryptographic ciphers. As a result, legacy FortiAP models using weak ciphers are blocked from connecting with FortiGates running FortiOS 7.0.0.

To workaround this issue, enter the following in FortiOS:

```
config system global
    set ssl-static-key-ciphers enable
    set strong-crypto disable
end
```

How VoIP ALG mode settings determine the firewall policy inspection mode

The `default-voip-alg-mode` setting will determine which inspection mode each firewall policy uses after upgrading.

Scenario 1

```
config system settings
    set default-voip-alg-mode proxy-based
end
```

This is the default setting. All firewall policies will be converted to proxy-based inspection.

Scenario 2

```
config system settings
    set default-voip-alg-mode kernel-helper-based
end
```

All firewall policies with a selected VoIP profile will be converted to proxy-based inspection. Policies without a configured VoIP profile will remain in the same inspection mode after upgrading.

Recommendation

If the scenario 1 outcome is not desired, do the following:

1. Before upgrading, set `default-voip-alg-mode` to `kernel-helper-based`.
2. Perform the upgrade.

3. After upgrading, set `default-voip-alg-mode` to `proxy-based`.
   The upgraded policies will remain in the same inspection mode if they do not contain a VoIP profile.

Product integration and support

The following table lists FortiOS 7.0.0 product integration and support information:

Web Browsers	• Microsoft Edge 89 • Mozilla Firefox version 87 • Google Chrome version 89 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 29. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 7.0.0 must work with FortiManager 6.4.1 or later. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 29. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiClient EMS	• 6.4.0
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later
FortiSwitch OS (FortiLink support)	• 3.6.9 and later

FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0295 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
FortiExtender	• 3.2.1
AV Engine	• 6.00258
IPS Engine	• 7.00018
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

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 87 Google Chrome version 89
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 87 Google Chrome version 89
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 87 Google Chrome version 89
macOS Big Sur 11.2	Apple Safari version 14 Mozilla Firefox version 87 Google Chrome version 89
iOS	Apple Safari

Operating System	Web Browser
	Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

Resolved issues

The following issues have been fixed in version 7.0.0. For inquires about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
650160	When using email filter profile, emails are being queued due to IMAP proxy being in stuck state.

Anti Virus

Bug ID	Description
524571	Quarantined files cannot be fetched in the AV log page if the file was already quarantined under another protocol.
560044	Secondary device blades occasionally report critical log event `Scanunit initiated a virus engine/definitions update`. Affected models: FG-5K, 6K, and 7K series.
683835	Files fail to open in some CIFS setups where FortiOS cannot generate a signature.

Application Control

Bug ID	Description
576727	*Unknown Applications* category is not present in NGFW policy-based mode.

Data Leak Prevention

Bug ID	Description
616918	DLP cannot detect attached ZIP and PDF files when receiving emails via MAPI over HTTPS.

DNS Filter

Bug ID	Description
649985	Random SDNS rating timeout events on 6K/7K SLBC with FGSP.
653581	Cannot pass DNS traffic through FortiGate or DNS traffic originated from FortiGate when external blocklist (threat feed) is updated.
674302	Do not send FortiGate generated DNS response if no server response was received and redirect DNS queries time out.
682060	DNS proxy is holding 60% memory caused by retransmitted DNS messages sent from DNS clients, which causes the FortiGate to enter conserve mode.
693551	DNS filter is not working on active VDOM in second HA unit in virtual cluster environment.

Endpoint Control

Bug ID	Description
664654	EMS host tags are not synced with the FortiGate when the user connects to a tunnel mode SSID.

Explicit Proxy

Bug ID	Description
607230	Percent encoding is not converted in FTP over HTTP explicit proxy.
639092	Web proxy forward server allows empty string for monitor option when health check is enabled.
642196	Web proxy forwarding server health check does not send user name and password.
654455	Proxy policy destination address set to none allows all traffic.
662931	Browsers change default `SameSite` cookie settings to `Lax`, and Kerberos authentication does not work in transparent proxy.
664380	When configuring explicit proxy with forward server, if `ssl-ssh-profile` is enabled in `proxy-policy`, WAD is unable to correctly learn the destination type correctly, so the destination port is set to 0, but the squid proxy server does not accept the request and returns an error.
664548	When the FortiGate is configured as an explicit proxy and AV is enabled on the proxy policy, users cannot access certain FTP sites.
681054	Web proxy users are disconnected due to external resource update flushing the user even if they do not have an authentication rule using the related proxy address or IP list.

Bug ID	Description
681969	FSSO explicit proxy authentication appears as basic instead of FSSO.
689002	Proxy traffic failed after modifying resource setting in external connector.
697836	Performance issue when transferring data over FortiGate explicit proxy using fast match feature.
707832	WAD crashes each time when setting the access proxy VIP to the destination address of the explicit web proxy.

File Filter

Bug ID	Description
676485	File filter rule set with the `msc` file type was removed after upgrading.

Firewall

Bug ID	Description
230997	Do not allow `match-vip` in firewall policies when the action is set to accept.
586995	Cluster VDOM policy statistics data is not correct when VFID is different for same VDOM on primary/secondary.
612371	The `captive-portal-exempt` policy option does nit work for IPv6 traffic in a new firewall policy.
635074	Firewall policy `dstaddr` does not show virtual server available based on virtual WAN link member.
650867	Firewall does not track UDP sessions on the same port.
653828	When web filter and application control are configured, blocked sessions to play.google.com remain in the session table for 3600 seconds.
659142	TNS connection request limited to 500 per second when client is trying to reach database server through the firewall.
659650	DSCP marking on `traffic-shaper/per-ip-shaper` failed to mark corresponding IPv6 packets.
660461	Configuration changes take a long time, and ipsmonitor and cmdbsrv processes go up to 100% of CPU in a large, complex configuration.
661014	FortiCarrier has GTP drop packet log after configuring GTP allow list.
661777	Source NAT port reuses ports too quickly, and GCP/API fails to establish due to endpoint independence conflict.

Bug ID	Description
663062	Sessions are marked dirty when IPsec dialup client connects/disconnects and policy routes are used.
665739	HTTP host virtual server does not work well when real server has the same IP but a different port.
665964	In NAT64 scenario, ICMPv6 `Packet too big` message translated to ICMPv4 does not set the MTU/DF bit correctly.
666612	Get internet service name configuration error on version 7.01011 when FortiGate reboots or upgrades.
667277	Support using a zone as an external interface of a VIP.
667696	Reputation settings in policies are not working when `reputation-minimum` is set and no source/destination address is set.
667772	When NGFW mode is policy-based and the security policy is configured, the quard daemon should start when one of the following profiles is enabled: anti virus, web filter, application control, IPS, or DLP.
669665	All ISDB groups are lost when upgrading from 6.2.5 to 6.4.2.
675353	Security policy (NGFW mode) flow-based UTM logs are still generated when policy traffic log is disabled.
675821	In firewall policies, the configuration order of NAT commands is not correct.
676503	The central SNAT map does not work in policy-based NGFW mode.
678813	Cannot change the order of IPv4 access control list entries from FortiOS after upgrading from 6.4.1. to 6.4.3.
682956	ISDB is empty/crashes after upgrading from 6.2.4/6.2.5 to 6.2.6.
683426	No hit counts on policy for DHCP broadcast packets in transparent mode.
683604	When changing a policy and creating a firewall sniffer concurrently, there is traffic that is unrelated to the policy that is being changed and matching the implicit deny policy. Some IPv4 firewall policies were missing after the change.
683669	Firewall schedule settings are not following daylight saving time.
694284	In transparent mode when HA is enabled, if the packet passes through the FortiGate more than once time, the MAC address could be different from main session.
699785	The performance will drop heavily when there are more than 3000 VIPs.

FortiView

Bug ID	Description
628225	FortiView *Compromised Hosts* dashboard cannot show data if FortiAnalyzer is configured using the FQDN address in the log setting. FortiAnalyzer configured with an IP address does not have this issue.
643198	*Threats* drilldown for *Sources*, *Destinations*, and *Country/Region* (1 hour, 24 hours, 7 days) gives the error, *Failed to retrieve FortiView data*.
673225	FortiView *Top Traffic Shaping* widget does not show data for outbound traffic if the source interface's role is WAN. Data is displayed if the source interface's role is LAN, DMZ, or undefined.
683413	Some FortiView pages/widgets fail to query data from FortiAnalyzer Cloud if the local FortiAnalyzer is not enabled. Affected pages/widgets: *Compromised Hosts*, *FortiView Cloud Applications*, *FortiView VPN*, *FortiView Web Categories*, *Top Admin Logins*, *Top Endpoint Vulnerabilities*, *Top Failed Authentication*, *Top System Events*, *Top Threats*, *Top Threats - WAN*, and *Top Vulnerable Endpoint Devices*.
683627	FortiView has no data when FortiAnalyzer Cloud is the data source.

GUI

Bug ID	Description
446427	Using the GUI to update a VDOM license fails when the new license has a lower VDOM count than the current license.
490396	Account profile permission override and RADIUS VDOM override features do not work with two-factor authentication for remote admin login via GUI. The feature still works when the admin login is via SSH.
547123	The help message for `gui-dynamic-profile-display` is not correct.
561420	On *Traffic Shaping Policy* list page, right-click option to show matching logs does not work.
561889	When creating a firewall with an invalid subnet mask, an error is not generated.
567996	Slow load times for the *Managed FortiSwitch* and *FortiSwitch Ports* pages when there is a large number of FortiSwitches.
588159	When disabling *Allow Endpoint Registration* on the *VPN Creation Wizard*, the action succeeds, but the error *Unable to setup VPN* is incorrectly displayed.
589749	Incorrect error message on log settings page, *Connectivity issue, 0 logs queued*, for FortiAnalyzer connection when the VDOM is in transparent mode with log setting override enabled.

Bug ID	Description
592854	An address created by the VPN wizard cannot save changes due to an incorrect validation check for parentheses, *()*, in the *Comments* field.
599815	Support inspecting username (email address) in case-insensitive format.
602102	Warning message is not displayed when a user configures an interface with a static IP address that is already in use.
606814	When creating a profile group with an SSL/SSH profile of *no-inspection*, the profile group correctly displays this, but when you edit the profile, *certificate-inspection* is displayed.
612066	GUI does not allow user to select SSL VPN tunnel when configuring *Multicast* routing.
634550	GARP is not sent when using the GUI to move a VDOM from one virtual cluster to another. GARP is sent when using the CLI.
636208	On *SD-WAN Rules* page, the GUI does not indicate which outgoing interface is active. This is due to auto-discovery VPN routing changes.
638752	FortiGates in an HA A-P configuration may lose GUI access to the HA secondary device after a period of 8 days of inactivity, when at least one static IPv6 address is configured on an interface.
645441	FortiAnalyzer Cloud card on the *Fabric Connectors* page shows a connected icon when it is not connected.
645606	GUI does not allow users to select SD-WAN as a destination interface in an SSL VPN policy while CLI does.
650307	GUI does not show the configured external FortiGuard category in the SSL-SSH profile's exempt list.
650708	When the client browser is in a different time zone from the FortiGate, the *Guest Management* page displays an incorrect expiry time for guest users. The CLI returns the correct expiry.
651711	Unable to select an address group when configuring *Source IP Pools* for an SSL VPN portal.
652522	When performed from the primary FortiGate, using the GUI to change a firewall policy action from accept to deny does not disable the IP pool setting, causing the HA cluster to be out of sync. Updating the policy via the CLI does not have this issue.
652975	Cannot access FortiGate GUI over IPv6 after configuring IPv6 for the first time.
653240	When refreshing the FortiGuard page, connectivity status for *Web Filtering* and *Anti-Spam* incorrectly changes from up to down.
653422	When VDOM is enabled, the GUI cannot be used to edit a remote user group from within the *Administrators* dialog.
654018	When there are more than 600 quarantined IP addresses, the *Quarantine Monitor* (GUI and CLI) will not properly display them.
654156	When editing CLI objects that have an mkey ending with an "/.", the page is either stuck loading, shows a JS error, or shows a notification that the entry does not exist.

Bug ID	Description
654186	The top charts of the *Device Inventory Monitor* dashboard are empty when the visualization is set to table view.
654250	Firewall users cannot change their password via web captive portal when password renewal is enforced by the firewall policy for remote users.
654626	Unable to change the action setting of *Freeware and Software Downloads* using the *FortiGuard Category Based Filter* of the DNS filter profile.
654705	Aggregated IPsec VPN interface shows as down when each member tunnel has phase 1 and phase 2 names that differ from each other.
655255	FortiGuard resource retrieval delay causes GUI pages to respond slowly. Affected pages include: *Firewall Policy*, *Settings* (log and system), *Explicit Proxy* (web and FTP), *System Global*, and *System CSF*.
655568	Users cannot deselect *Administrative Access* options for VLAN interfaces from the GUI; the CLI must be used.
655891	Web CLI console cannot load due to `Connection lost` if port 8080 is used (HTTP).
656139	When editing the *Interface* column from the *Multicast Policy* page, an empty column appears when the *any* entry is selected from *Select Entries* and applied. The same occurs from the NAT64 and NAT46 policy pages.
656429	Intermittent GUI process crash if a managed FortiSwitch returns a reset status.
656599	Automation CLI script should support setting an administrator profile context to restrict access.
656668	On the *System* > *HA* page, GUI tooltip for the reserved management interface incorrectly shows the connecting IP address instead of the configured IP address.
656974	`ip6-mode` was changed from `delegated` to `static` after the interface was edited from the GUI.
657322	For AV profiles, the outbreak-prevention setting on enabled protocols is not automatically configured when enabling *Use External Malware Block List*.
657545	Enabling the *Dynamic Gateway* toggle for a static route fails without warning when the configuration is incorrect.
659490	A remote certificate in VDOM mode that has no references cannot be deleted from the GUI. Removal is possible using the CLI.
661582	*Date/Time* filter does not work on FortiGate Cloud logs.
662705	REST API, `api/v2/monitor/firewall/internet-service-details` returns `start_ip` and `end_ip` in raw format instead of string format.
662873	Editing the LDAP server in the GUI removes the line `set server-identity-check disable` from the configuration.
663351	Connectivity test for RADIUS server using CHAP authentication always returns failure.
663737	Re-add the FortiView facets filtering bar to full screen or standalone mode.

Bug ID	Description
663818	When filtering log view entries by IP address range, entries higher than the upper limit of the range are shown.
663956	Unable to load web CLI console for LDAP admin with a login name that contains a space.
664007	GUI incorrectly displays the warning, *Botnet package update unavailable, AntiVirus subscription not found.*, when the antivirus entitlement is expiring within 30 days. The actual botnet package update still works within the active entitlement duration.
665111	There is no way to add a line break when using the GUI to edit the replacement message for *pre_admin-disclaimer-text*. One must use the CLI with the `Shift + Enter` keys to insert a line break.
665444	*Log Details* does not resize the log columns and covers existing log columns.
665712	When multiple favorite menus are configured, the new features video pops up after each GUI login, even though user previously selected *Don't show again*.
666857	LDAP connectivity issue in transparent mode VDOM.
666999	When editing the *Poll Active Directory Server* page, the configured LDAP server saved in FSSO polling is not displayed. Users must use the CLI to modify the setting.
668020	Disclaimer users are not shown in the user monitor; they must be displayed in the CLI with `diagnose firewall auth list`.
668470	FortiGuard DDNS setting incorrectly displays truncated unique location and empty server selection after saving changes.
672599	After performing a search on firewall *Addresses*, the matched count over total count displayed for each address type shows an incorrect total count number. The search functionality still works correctly.
672906	GUI does not redirect to the system reboot progress page after successfully restoring a configuration.
673478	FortiView shows no data due to backend filtering error.
673496	When editing phase 2 configurations, clicking *Complete Section* results in a red highlight around the phase 2 configuration GUI box, and users cannot click *OK* to save configuration changes.
680804	SD-WAN default implicit rule shows the destination address as *Route tag: undefined*.
680805	The list of firewall schedules displays time based on the browser time, even though the global time preference is set to use the FortiGate system time. The *Edit Schedule* page does not have this issue.
682008	On the *SSL-VPN Settings* page, the option to send an SSL VPN configuration to a user for FortiClient provisioning does not support showing domain name for VPN gateway.
682440	In the *Firewall Policy* list, the tooltip for *IP Pool* incorrectly shows *Port Block Allocation* as being exhausted if there are expiring PBAs available to be reallocated.

Bug ID	Description
684076	Erroneous duplication error displayed when creating a phase 2 with *Named IPv6 Address* set to *all* if there is already a phase 2 entry defined with *Named IPv4 Address* set to *all*. The CLI must be used for this configuration.
684904	When a FortiGate with VDOM and explicit proxy enabled has an access profile with packet capture set to none, administrators with this access profile are not able to create an explicit proxy policy.
687303	Unable to edit Fabric Connector on FortiGate in HA.
688076	The *Firewall Address* and *Service* pages cannot load on a downstream FortiGate if *Fabric Synchronization* is enabled, but the downstream FortiGate cannot reach the root FortiGate.
688567	Under *Policy & Objects* > *Addresses*, users are unable to save changes when enabling or disabling *Fabric Sync* for SSLVPN_TUNNEL_ADDR1.
688994	The *Edit Web Filter Profile* page incorrectly shows that a URL filter is configured (even though it is not) if the URL filter entry has the same name as the web filter profile in the CLI.
689605	On some browser versions, the GUI displays a blank dialog when creating custom application or IPS signatures. Affected browsers: Firefox 85.0, Microsoft Edge 88.0, and Chrome 88.0.
693624	Certificate details in the GUI no longer have values for validity (*Valid From*, *Valid To*).
697667	When the FortiGate is managed by FortiManager, an administrator that selects *Login Read-Only* is incorrectly allowed to select *Update firmware* in *System* > *Firmware*, browse for an image, and install it.
704638	Allow customers choose which format is used for the *Date/Time* column in the log viewer.

HA

Bug ID	Description
421335	Get one-time hasync crash when running HA scripts for FIPS-CC.
540600	The HA `hello-holddown` value is divided by 10 in the hatalk daemon, which makes the `hello-holddown` time 10 times less than the configuration.
615001	LAG does not come up after link failed signal is triggered.
643958	Inconsistent data from FFDB caused several confsyncd crashes.
650624	HA GARP sending was delayed due to lots of transceiver reading.
653095	Inband management IP connection breaks when failover occurs (only in virtual cluster setup).
654341	The new join-in secondary chassis failed to sync, while primary chassis has 6K policies in one VDOM.
656988	In an HA cluster, when a backup configuration file uses an automation stitch, the primary and secondary devices use the same file name in the script. This causes the secondary device's configuration file to overwrite the primary device's configuration file.

Bug ID	Description
657376	VLAN interfaces are created on a different virtual cluster primary instead of the root primary do not sync.
658839	Cloning a policy from the CLI causes the HA cluster to get out of sync.
662893	HA cluster goes out of sync if SAML SSO admin logs in to the device.
670331	Management access not working in transparent mode cluster after upgrade.
671288	FortiGate in standalone mode has a virtual MAC address.
675781	HA cluster goes out of sync with new custom DDNS entry, and changes with respect to the `ddns-key` value.
677246	Unable to contact TACACS+ server when using HA dedicated management interface in 6.4.3.
677552	After two quick failovers, VPN does not work until rekey.
678309	Cluster is out of sync because of `config vpn certificate ca` after upgrade.
680753	`admin-restrict-local` feature does not work on management interface in HA cluster.
682150	Virtual MAC on interface does not change when VDOM is moved back from secondary vCluster to primary vCluster.
690248	Malicious certificate database is not getting updated on the secondary unit.
692212	The interfaces on NP6 platforms are down when doing a configuration revert in HA mode.
693178	Sessions timeout after traffic failover goes back and forth on a transparent FGSP cluster.
693223	hasync crashes with signal 11 in `ha_same_fosver_with_manage_master`.

Intrusion Prevention

Bug ID	Description
638341	In some cases, IPS fails to get interface ID information that would result in IPS incorrectly dropping the session during static matching.
647568	Got `exec child 210 does not reply, skip it.` output after adding application control and antivirus profiles in an IPS policy.
660111	SSL VPN web mode IPS detection with HTTP does not work, even though it works with HTTPS.
668631	IPS is constantly crashing, and ipshelper has high CPU when IPS extended database has too many rules (more than 256) sharing the same pattern. Affected models: SoC3-based FortiGates.
671322	IPS engine reloads, or FortiGate reboots and displays CMDB `__bsearch_index()` duplicate value insertion errors.
678166	TFTP upload not working when application control and ASIC offload are enabled.
686301	ipshelper CPU spikes when configuration changes are made.

Bug ID	Description
688888	BZIP2 file including EICAR is detected in the original direction of the flow mode firewall policy even though `scan-bzip2` is disabled.
689259	Flow-Based AV scanning does not send specific extension files to FortiSandbox.
691395	Signature false positives causing outage after IPS database update.
694777	Application, IPS, and AV databases and engines are not updated by scheduled updates if a security policy is used.

IPsec VPN

Bug ID	Description
566076	IKED process signal 11 crash in an ADVPN and BGP scenario.
592361	Cannot pass traffic over ADVPN if: `tunnel-search` is set to `nexthop`, `net-device disable`, `mode-cfg enable`, and `add-route disable`.
638352	In extreme situations when thousands of tunnels are negotiating simultaneously (IKEv2), iked process gets exhausted and stuck.
639806	User name log empty when IPsec dialup IKEv2 has client RSA certificate with empty subject.
642543	IPsec did not rekey when keylife expired after back-to-back HA failover.
646012	DHCP over IPsec randomly works when `net-device` is disabled.
647285	IKE HA sync IPsec SA fails on receiver when ESP null crypto algorithm is used.
652774	OCVPN spoke-to-spoke communication intermittently fails with mixed topology where spokes have one or two ISPs, but the hubs have two.
655739	`local-gw` is replaced with primary IP on a secondary device when the secondary IP is used as a `local-gw`.
658215	When the SA is about to expire, before it is removed it is not offloaded so the traffic may not go through.
659442	NP6Lite platforms may enter conserve mode because the `get`/`put` reference count for `pinfo` is not reasonable. When there is an inbound SA update, the old `pinfo` is not freed.
659535	Setting same `phase1-interface` in SD-WAN member and SD-WAN zone causes iked watchdog timeout.
660472	Could not locate phase 1 configuration for IPv6 dialup IPsec VPN.
663648	BGP over dynamic IPsec VPN tunnel with `net-device enable` not passing through traffic after rebooting.
666693	If NAT-T IP changes, the dynamic IPsec spoke add route entry is stuck on hub.
667129	In ADVPN with SLA mode, traffic does not switch back to the lowest cost link after its recovery.

Bug ID	Description
668554	Upon upgrading to FortiOS 7.0.0, a device with IPsec configured may experience IKE process crashes when any configuration change is made or an address change occur on a dynamic interface.
670025	IKEv2 `fragmentation-mtu` option not respected when EAP is used for authentication.
672925	Traffic cannot pass through IPsec tunnel after being offload to NPU.
673049	FortiGate not sending its external interface IP in the IKE negotiation (Google Cloud Platform).
673258	FortiGate to Cisco IKEv2 tunnel randomly disconnects after rekey.
675276	Kernel panic occurs after OCVPN role changes.
675838	iked ignores phase1 configuration changes until the process restarts.
684133	Site-to-site IPsec VPN cannot establish in asymmetric routing scenario where the IPsec VPN bound interface is a loopback interface.
690903	ADVPN shortcut is flapping when spokes are behind one-to-one NAT.
691178	Exchanging IPs does not work with multiple dynamic tunnels.
691878	Creating or updating a user with two-factor authentication causes dialup VPN traffic to stop.
694992	Issue establishing IPsec and L2TP tunnel with Chromebook behind NAT.
699834	ESP errors are logged with incorrect SPI value.

Log & Report

Bug ID	Description
570152	Remove redundant `override-setting.override` attribute for logging.
587916	Logs for local-out DNS query timeout should not be in the DNS filter UTM log category.
645914	Move `eventtime` field to the beginning of the log to save performance on Splunk or other logging systems.
647741	On FG-60F, logging and FortiCloud reporting incorrect IPv6 bandwidth usage for sessions with NPU offload.
650325	miglogd crashes with signal 11.
650886	No log entry is generated for SSL VPN login attempts where two factor authentication challenge times out.
654363	Traffic log shows *Policy violation* for traffic hitting the allow policy in NGFW policy mode.
658665	Cannot retrieve logs from FortiAnalyzer on non-root VDOM.
661040	Cyrillic characters not displayed properly in local reports.

Bug ID	Description
667274	FortiGate does not have log disk auto scan failure status log.
667950	IPS UTM log is missing `msg=` and `attackcontext=` TLV fields because the TLV buffer is full and not sent to miglogd.
670741	Unable to configure syslog filter data size more then 512 characters.
675347	In local log search, results returned immediately when there are checked logs.
677540	First TCP connection to syslog server is not stable.
682374	Traffic logs are not forwarded correctly to syslog server in CEF format.
691728	Traffic log missed for some UTM DLP logs.
692237	FortiOS is truncating the group field to 35 characters in traffic logs.
696825	In rare cases, reportd crashes when the number of items can be zero, but the pie chart is still generated successfully.
702859	*Outdated report files deleted* system event log keeps being generated.

Proxy

Bug ID	Description
550350	Should not be able to set `inspection-mode proxy` with IPS-enabled only policy.
579902	Proxy deep inspection fails if server chooses to sign with ECDSA-SHA1.
619707	When Kerberos (negotiate without NTLM) authentication method is used for web proxy user authentication, there may be a rare memory leak issue. This memory leak issue may eventually cause the FortiGate to go into conserve mode once it occurs after many users are authenticated by Kerberos repeatedly over time.
632085	When CIFS profile is loaded, using MacOS (Mojave 10.14) to access Windows 2016 SMB Share causes WAD to crash.
633303	SSO guest user group does not work in proxy policy to authenticate users.
640488, 669736, 675480	When URLs for block/allow/external resource are processed, the system might enter conserve mode when external resources are very big.
648831	WAD memory leak caused by Kerberos proxy authentication.
653099	Wildcard URL filter in proxy mode with `?` and `*` not always handled properly.
655356, 660857	Proxy deep inspection fails if server uses TLS 1.3 cookies or record padding.
656830	FortiGate should be in SSL bypass mode for TLS 1.2 certificate inspection with client certificate request.

Bug ID	Description
657905	Firewall policy with UTM in proxy mode breaks SSL connections in active-active cluster.
658654	Cannot access specific website using proxy-based UTM with certification inspection due to delays from the server in replying to ClientHello message when a second connection from the same IP is also waiting for ClientHello.
661063	If a client sends an RST to a WAD proxy, the proxy can close the connection to the server. In this case, the relatively long session expiration (which is usually 120 seconds by default) could lead to session number spikes in some tests.
664737	WAD crash with signal 11 (`/bin/wad => wad_ui_diag_session_get`).
666522, 666686	Proxy mode is blocking web browsing for some websites due to certificate inspection.
675343	WAD crashes with transparent web proxy when connecting to a forward server.
680651	Memory leak when retrieving the thumbnailPhoto information from the LDAP server.
681134	Proxy-based SSL certification inspection session hangs if the outbound probe connection has no routes.
682002	An incorrect teardown logic on the WAD SSL port causes memory leak.
682980	Proxy deep inspection workaround needed for sites that require psk_key_exchange_modes.
684168	WAD process consumes memory and crashes because of memory leak when calling FortiAP API from WAD.
691468	WAD IPS crashes because task is scheduled after closing.
693951	Cannot access Java-based application in proxy mode.
696541	Mirroring decrypted SSL traffic is not designed to work on a virtual interface, so this configuration should not be allowed.

REST API

Bug ID	Description
597707	REST API `/api/v2/monitor/firewall/security-policy` adds UUID data for security policy statistics.
658206	New REST API `POST /api/v2/monitor/vpn/ike/clear?mkey=<gateway_name>` will bring down IKE SAs tunnel the same way as `diagnose vpn ike gateway clear`.
663441	REST API unable to change status of interface when VDOMs are enabled.
686351	Remove blocking call to AWS meta out of `/api/v2/monitor/web-ui/state`.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
579884	VRF configuration in WWAN interface has no effect after reboot.
585816	SD-WAN route selection does not use the most specific route in the routing table when selecting the egress path.
613716	Local-out TCP traffic changes output interface when irrelevant interface is flapping and causes disconnections.
628896	DHCP relay does not match the SD-WAN policy route.
641050	Need support for SSL VPN web mode traffic to follow SD-WAN rules/policy route.
654032	SD-WAN IPv6 route tag command is not available in the SD-WAN services.
655447	BGP prefix lifetime resets every 60 seconds when scanning BGP RIB.
659409	FortiGate blocks IPv6 but allows IPv4 for traffic that looks asymmetric with `asymroute` is disabled.
660285	Editing an existing route map rule to add `set-weight 0` results in `unset set-weight` behavior.
660300	Application vwl signal 11 (segmentation fault) received when HA receives 0 bytes of data.
660311	Application vwl signal 6 (aborted) received due to wrong memory allocation for SD-WAN service when creating an ADVPN shortcut.
661769	SD-WAN rule disappears when an SD-WAN member experiences a dynamic change, such as during a dynamic PPPoE interface update.
662655	The OSPF neighborship cannot be established; get MD5 authentication error when the wrong MD5 key is deleted after modifying the key.
662696	If a session is initiated from the server side, SD-WAN application control does not work as expected.
662845	HA secondary also sends SD-WAN `sla-fail-log-period` to FortiAnalyzer.
663396	SD-WAN route changes and packet drops during HTTP communication, even though `preserve-session-route` is enabled.
666829	The bfdd application crashes.
667469	SD-WAN members and OIFs keep reordering despite the health check status being stable in an HA setup.
668218	SD-WAN HTTP health check does not work for URLs longer than 35 characters.
668592	Incorrect default timers for BFD parameters, `bfd-desired-min-tx` and `bfd-required-min-rx`.
668982	Possible memory leak when BGP table version increases.

Bug ID	Description
670017	FortiGate as first hop router sometimes does not send register messages to the RP.
672061	In IPsec topology with hub and ~1000 spokes, hundreds of spoke tunnels are flapping, causing BGP instability for other spokes.
673603	Only the interface IP in the management VDOM can be specified as the health check source IP.
675442	Weight-based load-balance algorithm causes local-in reply traffic egress from wrong interface.
676685	VRRP does not consider VRF when looking up destination in routing table.
677201	Route maps show unset attributes after upgrading from 6.4.2.
677928	SD-WAN with `sit-tunnel` as a member creates an unwanted default route.
678819	The `preserve-route` is kept in session states if the route is deleted and the egress interface changes.
679175	Email server local-out traffic should be controlled by SD-WAN services.
680365	BGP is choosing local route that should have been removed from the BGP network table.
681433	GRE local-out traffic is not following SD-WAN rules.
684378	Traffic is forwarded out to the wrong interface if an LTE interface is an SD-WAN member. The LTE interface may lose its SD-WAN flag during modem initialization.
685871	OSPFv3 routes are missing from routing table when unsetting or setting the ASBR table.
688774	The traffic is sent out from an interface in the default route table when using `diagnose trafficTest run`.
691660	`set match` in community string not accepting four-byte AS.
692241	BGP daemon consumes high CPU in ADVPN setup when disconnecting after socket writing error.
693238	OSPF neighbor cannot form with spoke in ADVPN setup if the interface has a parent link and it is a tunnel.
693496	SD-WAN rules not working for FortiAnalyzer settings.
696079	`config aggregate-address6` is not summarizing the aggregate route.
697658	FortiCloud activation does not honor the `set interface-select-method` command under `config system fortiguard`.
698360	OSPF area range routes lost during HA failover.
698665	Get `iprope_in_check () check failed on policy 0, drop` error on debug flow for CAPWAP/Nmap on port 5246 connecting to VRRP.
700384	Incorrect IP address is chosen as forward address by the FortiGate while generating an OSPF type 7 LSA.

Security Fabric

Bug ID	Description
649344	When viewing CSF child *Dashboard* > *WiFi* from parent FortiGate, GUI reports, *Cannot read property 'spectrum_analysis' of undefined*.
650724	Invalid license data supplied by FortiGuard/FortiCare causes invalid warning in the *Security Rating* report.
652737	FortiGate does not send interface configuration to FortiIPAM.
653368	Root FortiGate fails to load Fabric topology if HA downstream device has a trusted device in both primary and secondary FortiGates.
660250	The ipamd process is causing high memory usage after a few days as the JSON was not freed.
660624	FortiAnalyzer Cloud should be taken into consideration when doing CLI check for CSF setting.
662128	*Security Rating Summary* trigger is not available in multi-VDOM mode.
666242	Automation stitch CLI scripts fail with greater than 255 characters; up to 1023 characters should be supported.
669436	Filter lookup for Azure connector in *Subnet* and *Virtual Network* sections only shows results for VMSS instance.
673560	Compromised host automation stitch with IP ban action in multi-VDOM setup always bans the IP in the root VDOM.
686420	Dynamic address resolution is lost when SDN connector sends `sync.callback` command to the FortiGate.
690812	FortiGate firewall dynamic address resolution lost when SDN connector updates its cache.

SSL VPN

Bug ID	Description
548599	SSL VPN crashes on parsing some special URLs.
586035	The policy `script-src 'self'` will block the SSL VPN proxy URL.
598614	When a group and a `user-peer` is specified in an SSL VPN authentication rule, and the same group appears in multiple rules, each group and `user-peer` combination can be matched independently.
610995	SSL VPN web mode gets error when accessing internal website at https://st***.st***.ca/.
613733	Access problem for website.
615453	WebSocket using Socket.IO could not be established through SSL VPN web mode.

Bug ID	Description
623379	Memory corruption in some DNS callback cases causes SSL VPN crash.
630068	When sslvpn SSH times-out, a crash is observed when the SSH client is empty.
630771	SSL VPN rewrites the URL inside the emails sent in Outlook (webmail).
637217	Internal webpage, di***, is not loading in web mode.
641379	Internal SharePoint 2019 website cannot be accessed in SSL VPN web portal.
642838	Redirected URLs do not work in web mode for am***.com.
645973	Content from internal Microsoft Dynamics CRM cr***.local portal is not loading properly in SSL VPN web mode.
646339	SSL-SSH inspection profile changes to `no-inspection` after device reboots.
648433	Internal website loading issue in SSL VPN web portal for ca***.fr.
649130	SSL VPN log entries display users from other VDOMs.
652070	BMC Remedy Mid Tier 8.1 web application elements are not displayed properly in SSL VPN web mode.
652880	SSL VPN crashes in a scenario where a large number of groups is sent to fnbam for authentication.
653349	SSL VPN web mode not working for Ec***re website.
655374	SSL VPN web portal bookmark not loading internal web page after login credentials are entered.
656208	Users with explicit web proxy authentication lose their proxy authentication group.
656557	The map on the http://www.op***.org website could not be shown in SSL VPN web mode.
657689	The system allows enabling split tunnel when the SSL VPN policy is configured with destination `all`. It is not consistent with 5.6.x and 6.0.x.
657890	Internal website, https://*.da***.cz, is not working correctly in SSL VPN web mode due to source link error.
658036	When adding an FTP link to download FortiClient and accessing it through the portal, the colon is dropped from the string.
659234	FortiGate keeps replying to an ARP request for an IP address that was once assigned to an SSL VPN user, who has already disconnected and been deleted.
659312	Unable to load HTTPS bookmark in Safari (`TypeError: 'text/html'`).
659322	SSL VPN disconnects all connections after adding new address to IP pool.
659481	Internal websites not displayed successfully in SSL VPN web portal.
661290	https://mo***.be site is non-accessible in SSL VPN web mode.
661372	SSL VPN incorrectly rewrites the script URL.
661835	ASUS ASMB9-iKVM application shows blank page in SSL VPN web mode.

Bug ID	Description
662042	The https://outlook.office365.com and https://login.microsoft.com websites cannot be accessed in the SSL VPN web portal.
662871	SSL VPN web mode has problem accessing some pages on FortiAnalyzer 6.2.
663298	The internal website is not working properly using SSL VPN.
663433	SSL VPN web mode cannot open DFS shared subdirectories, get *Invalid HTTP request* error as sslvpnd adds `NT`.
663723	SSL VPN with user certificate and credential verification allows a user to connect with a certificate signed by a trusted CA that does not match the certificate chain of the configured CA in the user peer configuration.
664121	SCM VPN disconnects when performing an SVN checkout.
664276	SSL VPN host check validation not working for SAML user.
664804	User cannot use column header for data sorting (bookmark issue).
665330	SDT application can no longer load secondary menu elements in SSL VPN web mode.
665408	Occasionally, 2FA SSL VPN users are unable to log in when two remote authentication servers with the same IP are used.
665879	When sslvpn processes the HTTP/HTTPS response with content disposition, it will change the response body since the content type is HTML.
666194	WALLIX Manager GUI interface is not loading through SSL VPN web mode.
666513	An internal web site via SSL VPN web mode, https://***.46.19.****:10443, is unable to open.
666855	FortiOS supports verifying client certificates with RSA-PSS series of signature algorithms, which causes problems with certain clients.
667780	Policy check cache should include user or group information.
667828	SSL VPN web mode authentication problem when accessing li***.com.
668574	Unable to load a video in SSL VPN web mode.
669144	HTTPS access to ERP Sage X3 through web mode fails.
669497	Cannot view TIFF files in SSL VPN web mode.
669506	SSL VPN web mode cannot load web page https://jira.ca.ob***.com properly based on Jira application.
669685	Split tunneling is not adding FQDN addresses to the routes.
669707	The jstor.org webpage is not loading via SSL VPN bookmark.
669900	SSL VPN crash when updating the existing connection at the authentication stage.
670042	Internal website, http://si***.ar, does not load a report over SSL VPN web portal.

Bug ID	Description
670731	Internal application server/website bookmark (https://***.***.***.***.****/nexgen/) not working in SSL VPN web mode.
670803	Internal website, http://gd***.local/share/page?pt=login, log in page does not load in SSL VPN web mode.
672743	sslvpnd segmentation fault crash due to old DNS entries in cache that cannot be released if the same results were added into the cache but in a different order.
673320	Pop-up window does not load correctly when accessing internal application at https://re***.wo***.nl using SSL VPN web mode.
674279	Customer cannot access SAP web GUI with SSL VPN bookmark.
675196	RTA login webpage is not displaying in SSL VPN web mode.
675204	JSON parse error returned SSL VPN web mode for website https://bi***.u***.cat/az.php.
675878	When matching multiple SSL VPN firewall policies, SSL VPN checks the group list from bottom to top, and the user is mapped to the incorrect portal.
675901	Internal website https://po***.we***.ac.uk is not loading correctly with SSL VPN bookmark.
676345	SSL VPN web mode is unable to open some webpages on the internal site, https://vi***.se, portal.
676391	`set banned-cipher` command does not work for TLS 1.3.
676673	Ciphers with ARIA, AESCCM, and CHACHA cannot be banned for SSL VPN.
677167	SSL VPN web mode has problem accessing Sapepronto server.
677256	Custom languages do not work in SSL VPN web portals.
677548	In SSL VPN web mode, options pages are not shown after clicking the option tag on the left side of the webpage on an OWA server.
677550	GUI issues on the internal Atlassian Jira web portal in SSL VPN web mode.
678130	Customer internal website, https://va***.do***.com:21108/mne, cannot be displayed correctly in SSL VPN web mode.
678132	SSL VPN web portal SSO credentials for alternative option are not working.
678450	Unable to view the management GUI of PaloAlto running on 8.1.16 in SSL VPN web mode.
678996	Customized replacement messages for SSL VPN login page sometimes cannot be parsed correctly, causing the FortiToken authentication page to not appear.
679141	Website https://we***.p*.cz is not working in SSL VPN web mode.
680711	Unable to access OWA web server on mobile device in SSL VPN web mode.
680744	Internal SolarWinds Orion platform's webpages have issue in SSL VPN web mode.
681424	Unable to access sc***.com in SSL VPN web mode.
681626	Internal Gridbees portal does not display in SSL VPN web mode.

Bug ID	Description
681865	Bookmark to web server http://hc***.hi***.st***.es/ is redirected to a direct URL and web socket fails to establish in SSL VPN web mode.
683823	Internal ADB Epicentro portal has issue in SSL VPN web mode.
683963	SSL VPN bookmark fails to authenticate user through single sign-on for internal website login.
684012	SSL VPN crashed with signal 11 (segmentation fault) `uri_search` because of rules set for a special case.
684866	Specific content in portal.ag***.com cannot be shown in SSL VPN web mode.
685269	SSL VPN web mode is not working properly for aw***.co***.com website.
685854	After SSL VPN proxy rewrite, some Salto JS files could not run.
686425	When accessing an application in SSL VPN web mode (Sage HR), images fail to load for http://S-***.ro***.de/mp***/.
688023	SSL VPN bookmarked website shows empty page after logging in to SSL VPN gateway https://vd***.vi***.com.
688988	An internal web site, http://ar***.ar***.be***.it/, is unable to load PDF document in SSL VPN web mode.
689616	When a client is connected to SSL VPN and has an internet outage for more then 15 seconds, the client fails to reconnect.
689901	SharePoint links (su***.com) not working properly on webpage launched by SSL VPN web portal.
690217	Unable to display the data in SSL VPN web mode on innovaphone PBX link.
690282	Access through web portal to an Opengear Lighthouse server does not load the login page properly.
690507	SSO login for the bookmark to access FortiAnalyzer GUI does not work.
690686	Certificate authentication does not check PKI users in the expected order.
692107	Unable to load webpage, https://ax.***.on***.sp***.com/namespaces/, in SSLVPN web mode.
692326	Get `Entry not found` error when editing address object members that contain `interface-subnet` address objects.
693691	VPN logs do not show any bandwidth utilization in SSL web tunnel statistics when only using RDP.
694346	Report section of internal web server (https://lm***.lm***.au***.vw***/ar***/) is not accessible via the SSL VPN web portal.
694671	PDF files on internal web server, https://co***.ag***.em***.vw***:8443, are not opening in SSL VPN web portal.
695386	SAML login failure when a user belongs to multiple groups associated with multiple VPN realms.
695844	In SSL VPN web mode, redirection inside bookmark re***.ce***.fi***br keeps loading.
696009	Tunnel IP pool leak when DTLS tunnel user session is deleted due to timeout (idle or authentication).

Bug ID	Description
697142	SharePoint server (de***.sc***.gov.sa) is not working on web-based VPN.
697336	SSL VPN web mode cannot access https://em***.login.***.oraclecloud.com/.
699619	SSL VPN web mode fails to access to https://www.we***.org.
700572	SSL VPN web mode has problem accessing iDRAC9 server.
700673	Unexpected group to portal matching priority with SAML authentication.
702493	CMS URLs incorrectly rewritten by SSL VPN proxy in web mode.
705695	OS check for SSL VPN tunnel is not working on macOS Big Sur; the connection is rejected when the action is set to allow.
706067	PatientFocus has style issues in SSL VPN web mode.
706232	An internal web portal http://sr***/li***/ does not load properly in SSL VPN web mode.

Switch Controller

Bug ID	Description
649913	HA cluster not synchronizing when configuring an active LACP with MCLAG via FortiManager.
671135	flcfg crashes while configuring FortiSwitches through FortiLink.
686031	LLDP updates from FortiSwitch can cause flcfgd to leak memory.
686325	High rate of LLDP traffic can cause flcfgd to get stuck in Z state and halt FortiSwitch configuration synchronization.
690904	Unable to de-autorize FortiSwitch, or assign VLAN on FortiSwitch port on a tenant VDOM.
691985	L3 managed FortiSwitch configuration synchronization error due to the empty string parameter in `ptp-policy` on managed port configuration.
696405	`disable-discovery` of a FortiSwitch on one VDOM should not make the FortiSwitch disconnect from another VDOM.
700310	When managed switch PTP policy and settings configuration was pushed as part of initial FortiLink configuration, the FortiLink connection is in an error state.
700842	FortiSwitch MAC delete logs are not being generated.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
495532	EHP drop improvement for units with no NP service module.
521213	Read-only administrators should be able to run `diagnose sniffer packet` command.
572038	VPN throughput dropped from 1 Gbps to 40 Mbps when FEC is enabled.
578241	3DES and SHA1 should not be included in strong crypto list.
582536	Link monitor behavior is different between FGCP and SLBC clusters.
585882	Error in log, `msg="Interface 12345678001-ext:64 not found in the list!"`, while creating a long name VDOM in FG-SVM.
598464	Rebooting FG-1500D in 5.6.x during upgrade causes an L2 loop on the heartbeat interface and VLAN is disabled on the switch side.
606360	HQIP loopback test failed with configured software switch.
616576	DoS log counters are inaccurate (policy counters, event log entries, packet counts).
623775	newcli daemon crash due to FortiToken Mobile user token activation email processing.
627236	TCP traffic disruption when traffic shaper takes effect with NP offloading enabled.
628642	Issue when packets from the same session are forwarded to each LACP member when NPx offloading is enabled.
630861	Support FortiManager when `private-data-encryption` is enabled in FortiOS.
631132	Symantec connector does not work if management VDOM is not root vdom and root VDOM has no network connection.
631689	FG-100F cannot forward fragmented packets between hardware switch ports.
633827	Errors during fuzzy tests on FG-1500D.
634202	STP does not work in transparent mode.
634929	NP6 SSE drops after a couple of hours in a stability test.
636999	LTE does not connect after upgrading from 6.2.3 on FG-30E-3G4G models.
642005	FortiGate does not send `service-account-id` to FortiManager via fgfm tunnel when FortiCloud is activated directly on the FortiGate.
643033	`get system interface transceiver port1` should return RX power and TX power for all Ch0[1-4] with a 0 value or N/A when the admin port is down on one side and the link status is down.
644380	FG-40F/60F kernel panic if upgrading from 6.4.0 due to configuration file having a name conflict of `fortilink` as both aggregate interface and virtual switch name.

Bug ID	Description
645241	LACP failed to process traffic after adding new QSFP interfaces as LACP members even when the LACP status is up.
648014, 661784	FortiDDNS is unable to update the renewed public IP address to FortiGuard server in some error conditions.
648083	cmdbsvr may crash with signal 11 (segmentation fault) when frequently changing firewall policies.
648085	Link status on peer device is not down when admin port is set to down.
648406	Flow-based inspection with virtual wire pair causes MAC to flap.
649937	The `diagnose geoip geoip-query` command fails when `fortiguard-anycast` is disabled.
650411	SSL local certificate can not be imported via CMDB API (`api/v2/cmdb/vpn.certificate/local`) due to certificate data handling in CMF plugin (`vpn.certificate/local`).
651103	FG-101F crashed and rebooted when adding `vlan-protocol 8021ad` VLAN.
651420	Add support for `interface-shaping-offload` under `system npu` on SoC3 and SoC4 models.
652478	Get application cmdbsvr signal 11 crash log several times.
654131	No statistics for TX and RX counters for VLAN interfaces.
654159	NP6Xlite traffic not sent over the tunnel when NPU is enabled.
654424	FortiGate sends incorrect static route updates to FortiManager when using dedicated management interface.
655555	Unable to sniff LLDP frames on management and TFTP ports.
656690	Curaçao is not listed in the database when registering the FortiGate via the dashboard.
656983	MIB OID fgSysLowMemUsage returns value for devices where it is not applicable.
657629	ARM-based platforms do not have sensor readings included in SNMP MIBs.
657632	IPv6 passes though the DNS filter with application control enabled.
659539	FortiGate running 7.0.0 cannot validate license via FortiManager due to FortiManager hardware missing Fortinet_CA2 and Fortinet_SUBCA2001.
660441	When a PPPoE interface is enabled, it overwrites the LAN address object that was created.
660709	The sflowd process has high CPU usage when application control is enabled.
661450	Another application VWL `signal 6 (Aborted) received` appears.
662239	FGR-60F-3G4G hardware switch span does not work.
662681	Policy package push from FortiManager fails the first time, and succeeds the second time if it is blank or has no changes.

Bug ID	Description
662687	Asynchronous SDK call may take a long time and cause HA A-P to have `Kernel panic - not syncing` error.
663083	Offloaded traffic from IPsec crossing the NPU VDOM link is dropped.
663815	Low IPS HTTP throughput on SoC4 platforms.
663826	Fortinet Factory certificate key integrity check failed in `diagnose hardware certificate` command.
664268	No `filename` setting on BOOTP response when option 67 is set on the DHCP server.
664279	snmpd crashes when sorting a list-based ARP table if it has about 50,000 or more entries.
664478	Kernel crash caused race condition on `vlif` accessing.
665000	HA LED off issue on FG-1100E/1101E models.
665332	When VDOM has large number of VIPs and policies, any firewall policy change causes cmdbsvr to be too busy and consume high CPU.
665550	Fragmented UDP traffic does not assemble on the FortiGate and does not forward out.
666030	Empty firewall objects after pushing several policy deletes.
666205	High CPU on L2TP process caused by loop.
666210	`diagnose sys csum` command shows wrong hash on SOC4 appliances (FG- 60F, FG-61F, FG-100F and FG-101F).
666700	In FIPS mode, `ssh-cbc-cipher` is disabled, but the FortiGate still responds with CBC cipher.
666852	FortiGate local-out system DNS traffic for host names lookup continuously generates timeout DNS log if the primary server cannot resolve them.
667722	VLAN interface created on top of a 10 GB interface is not showing the actual TX/RX counters.
667962	httpsd crashed and `*** signal 6 (Aborted) received ***` appears when loading configurations through REST API with interactions.
668410	NP6lite SoC3 adapter drops packets after handed from kernel.
668856	Offloaded traffic passing through two VDOMs connected with EMAC-VLANs is sometimes dropped.
669914	No statistics for TX and RX counters for VLAN interfaces.
669951	confsyncd may crash when there is an error parsing through the internet service database, but no error is returned.
670838	It takes a long time to set the member of a firewall address group when the member size is large. In the GUI, cmdbsvr memory usage goes to 100%. In the CLI, newcli memory usage goes to 100%.
670962	Packet loss occurs when traffic flow between VLAN interfaces is created under 10G LACP link.
671643	NTurbo does not work when enabled in IPsec tunnel or with session helper.

Bug ID	Description
671972	If `cfg-save` is set to `manual` (under `config system global`), it causes problems with the queries made when parsing the internet service database.
672003	Link status on peer device is not down when the admin port is down on the FortiGate.
673263	High memory issue is caused by heavy traffic on the VDOM link.
673609	The auto-join FortiCloud re-try timer 600 second value is too large.
673918	Read-only administrator with packet capture read-write permission cannot run `diagnose sniffer` command.
675171	L2TP with status set to enable should be configured before EIP and SIP.
675418	FortiManager CLI script for 2FA FortiToken mobile push does not trigger activation code email.
675842	Get `Failed on update FortiGuardDDNS` error for fortiddns when secondary device becomes primary device in an HA cluster.
677263	When changing the interface speed, some checking is skipped if it is set from FortiManager.
677568	Failed to parse `execute restore config` properly when the command is from a FortiManager script.
677784	Add `diagnose debug traffic {interface | peek | history}` command to debug interface bandwidth traffic.
678469	Configuration attribute field in system event logs has length limitation.
678734	GeoIP6 address causes policy to not install properly in the kernel.
679114	DHCP discover request is wrongly forwarded to all IPsec VPN interfaces when tunnel flipping occurs.
680881	Rebooting device causes interface mode to change from static to DHCP.
681478	After reboot, get `global.system.interface.npu0_vlink0 config` error when VDOM is in transparent mode.
683284	Configuration backup is possible via SCP with expired administrator password.
686539	Egress interface-based traffic shaping is not applied if the session is processed by NTurbo.
687457	dnsproxy process crashes with signal 11.
687519	Bulk changes through the CLI are very slow with 24000 existing policies.
688316	After upgrading from 6.4.2 to 6.4.4, some configurations moved to another VDOM.
689873	Sometimes a VWL service adds a child without a parent, leading to a `signal 6 (Aborted)` crash received at `cmf_query_ses_update_child`.
690762	Application lted signal 11 crash on FWF-40F-3G4G.
691858	The newcli process crashes or shows an error when creating a VIP with the same external interface IP but a different source address filter.

Bug ID	Description
692490	When an <entry name> is on the same line as `config <setting> <setting> <entry name>`, it is not handled properly to send to FortiManager.
692534	`allow-subnet-overlap` setting not honored in NAT64 prefix configuration.
694754	Cloning a firewall policy may cause cmdbsvr to crash.
696517	NPU6 is not able to support WCCP traffic offloading. NTurbo driver received packet, which included additional IPv4 header and WCCP header. NTurbo is unable to process this kind of packets so it dropped.
696836	The OID structure was changed in 6.2.5; however, the MIB definitions for `fgVpnTunEntry` did not change and is causing errors.
697303	SNMP NULL hit counter for implicit deny policy (policy ID 0) is not sent.
698014	When running `execute speed-test` command, it shows all VLAN and SSL interfaces from other VDOMs.
698204	SNMP query for firewall policy statistics in non-root VDOM returns a `0`.
700513	802.1x wiredap does not correctly process the TagID in the Tunnel-Private-Group-ID attribute.
702932	FG-1500D reboots suddenly after COMLog reported kernel panic and voipd is tainted.

Upgrade

Bug ID	Description
656869	FG-100F/101F may continuously boot upon upgrading from FortiOS 6.4.0.

User & Authentication

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW mode.
633435	FortiGate local FSSO agent replaces user login with same username and IP, which causes traffic sessions to be removed.
643583	`radius-vdom-override` and `accprofile-override` do not work when administrator has 2FA enabled.
658228	The authd and foauthd processes may crash due to crypto functions being set twice.
658794	FortiGate sent CSR certificate instead of signed certificate to FortiManager when retrieve is performed.
659456	REST API authentication fails for API user with PKI group enabled due to fnbamd crash.

Bug ID	Description
662391	Persistent sessions for de-authenticated FSSO users.
662404	Wildcard LDAP users created on FortiToken Cloud have the first character of the username removed.
663399	`interface-select-method` not working for RADIUS configuration.
663685	The authd process truncates user names to a length of 35 characters (this breaks RADIUS accounting and logging for very long user names).
664123	Log enrichment for source and destination IP with RSSO user information in logs not properly working for IPv4 with framed route attribute in RADIUS accounting.
665391	The authd process gets stuck with high CPU due to slow route lookup when the routing table is big. FSSO stops processing new authentication events.
666268	The authd process may crash if the FSSO server connection is disconnected.
667025	FortiGate does not send LLDP PDU when it receives LLDP packets from VoIP phones.
672289	Group filter for `diagnose firewall auth` command does not work and displays other groups/users.
675226	The `ssl-ocsp-source-ip` setting not configurable in non-management VDOMs.
675539	FSSO collector status is down, despite that it is reported as connected by authd in a multi-VDOM environment.
677535	The radiusd process has a `stale` state after cluster members reboot.
682139	When multiple authentication methods are used in SSL VPN, authentication session terminates when RADIUS authentication enters error mode even when other methods like LDAP are queued.
682394	FortiGate is unable to verify the CA chain of the FSSO server if the chain is not directly root to FSSO endpoint.
682966	FortiGate is unable to parse IPv6 RADIUS accounting packet (`Parse error: IP6 Prefix`).
685727	FortiTokens get activated by secondary node, causing token to be in an error state and token user assignment to fail.
686437	Policy-based authentication fails when the destination URL contains query parameters.
688707	Remote RADIUS administrators are unable to login to HA units using the HA management interface IP address in a multi-VDOM environment.
688973	OCSP verification fails with `Can't convert OCSP rsp` error after upgrading.
690386	FortiToken mobile activation is controlled by SD-WAN services, instead of honoring `set interface-select-method` command under `config system fortiguard`.

VM

Bug ID	Description
587757	Unable to deploy FG-VM image on AWS with additional HDD(st1) disk type.
620654	Spoke dialup IPsec VPN does not initiate connection to hub after FG-VM HA failover in Azure.
641038	SSL VPN performance problem on OCI due to driver.
646161	FG-VM8 does not recognize all memory allocated in Hyper-V.
647800	Merge FIPS ciphers to 6.4.3 and 7.0 trunk (visible to AWS and Azure only).
656701	FG-VMX service manager enters conserve mode; cmdbsvr has high memory utilization.
657375	Add logging for successful AWS HA failover actions.
657785	On FG-AWS, changing health check protocol to `tcp-connect` causes kernel panic and reboot.
659333	Slow route change for HA failover in GCP cloud.
662969	Azure SDN connector filter count is not showing a stable value.
663276	After cloning the OCI instance, the OCID does not refresh to the new OCID.
663487	Should add router policy in `vdom-exception` list.
664312	Support vfNIC driving for Broadcom 100G NIC.
668131	EIP is not updating properly on FG-VM Azure.
669722	Unable to import more than 50 groups from NSX-T SDN connector.
669822	Hot adding multiple CPUs at once to Xen-flavored VMs can result in a kernel panic crash.
670166	FG-VM64-KVM configuration revisions lost after upgrading from 6.2.5.
671279	FG-VM64-AZURE-PAYG license/serial number get lost after downgrading to 6.2.6 from 6.4.3.
672312	Azure SDN connector does not offer all service tags.
672509	OCI HA unable to handle cross-compartment failover.
682420	Dialup IPsec tunnel from Azure may not be re-established after HA failover.
682561	`get system status` output can be stuck getting the instance ID.
682690	Random dvfilterd crashes with signal 6.
689239	Azure route table is not using the proper subscription ID during failover.
690863	EIP is not updating properly with `execute update-eip` command in Azure with standard SKU public IP in some Canadian regions, like CanadaCentral and CanadaEast.
695957	Azure SDN connector gets an empty IP list when the REST API call fails, which results in IPsec connection being interrupted until the next SDN connector update succeeds (one-minute interval).
698810	Bootstrap does not work with FG-VM on Azure Stack.
700381	FG-VM kernel panicked and reboot after sending through IPv6 traffic.

VoIP

Bug ID	Description
682983	SIP ALG does not DNAT all IP addresses in the SIP response messages (route field).

WAN Optimization

Bug ID	Description
686729	Transparent mode configuration was not learned properly in 6.4.

Web Application Firewall

Bug ID	Description
624452	`user-agent` setting under `config system external-resource` does not accept XSS characters.

Web Filter

Bug ID	Description
610553	User browser gets URL block page instead of warning page when using HTTPS IP URL.
654675	Unable to get complete output of `diagnose test application ipsufd 1`.
655972	Custom category action set to allow in web filter profile causes the URL to use the FortiGuard category rather than the custom category.
661713	Global web filter profile is not applied after changes to allowed/blocked categories.
675436	YouTube channel home page on blocklist is not blocked when directed from a YouTube search result.
676403	Replacement message pictures (FortiGuard web filter) are not displayed in Chrome.
678467	Safe search URL option is not working while the original query in Google Images has the same parameter name.

WiFi Controller

Bug ID	Description
560038	WiFi maps do not synchronize to HA FortiGate.
609549	In the CLI, the WTP profile for `radio-2` 802.11ac and 80 MHz channels does not match the syntax collection files.
611986	Bridge captive portal SSID has a new `portal-type` option, `external-macauth`, to support external Cisco ISE authentication.
620764	AP country and region settings are not updating as expected.
621346	Dynamic VLAN on SSID cannot pass traffic through FG-100F/101F and FG-60F/61F when offloading is enabled.
625630	FWF-60E hangs with looping kernel panic at WiFi driver.
643854	Client traffic was dropped by CAPWAP offloading when it connected from a mesh leaf Forti-AP managed by a FWF-61F local radio.
647703	HTTPS server certificate is not presented when WiFi controller feature is disabled in *Feature Visibility*.
656804	Spectrum analysis disable/enable command removed in CLI from `wtp-profile` and causing a bottleneck for APs, such as FAP-222C/223C at 100% CPU.
657391	FG-600E has cw_acd crash with `*** signal 8 (Floating point exception) received ***` in 6.2.4.
660991	FAP-U431F cannot view what channel is operating, and the override channel setting must be unset to change to a different channel.
662714	The `security-redirect-url` setting is missing when the `portal-type` is `auth-mac`.
665766	Client failed to connect SSID with WPA2-Enterprise and user group authentication.
672136	Log severity for wireless events in FortiWiFi and FortiAP should be reconsidered for CAPWAP teardown.
672920	CAPWAP tunnel traffic is dropped when offloading is enabled (with FAP managed by a VLAN interface).
673211	CAPWAP traffic drops on FG-300E when FortiAP is managed by VLAN interface.
674342	The cw_acd crashes after upgrading to 6.4.3 at cwAcLocal.
676640	cw_acd crash with `*** signal 8 (Floating point exception) received ***` after upgrading to 6.4.3.
680503	The current Fortinet_Wifi certificate will expire on 2021-02-11.
680527	Clients failing to authenticate to SSID due to MPSK client limit being reached when the actual connected clients are below the limit.
686631	Wireless country setting option needs to remove sanctioned countries and add missing countries.
690483	Wireless default WTP profile not synchronized between FWF-61E with HA A-A mode.

Known issues

The following issues have been identified in version 7.0.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
705591	When `av-scan` is enabled on the load end box, the FortiGate CPU hits 100% for over one minute. Such high CPU might cause WAD daemon signal 6 abort during that period.

Endpoint Control

Bug ID	Description
707388	When EMS has an offline status, most of time the FortiClient de-registers from EMS and the client certificate will be empty in web browser certificate store. **Workaround**: configure the FortiGate access proxy with `set empty-cert-action block` to block the SSL handshake if the client certificate is empty.
708545	The WAD daemon is triggered to fetch the FortiClient information based on a ZTNA EMS tag enabled for checking in a proxy policy. It is then possible to get a ZTNA EMS tag in the firewall dynamic address and get the expected traffic control.

Explicit Proxy

Bug ID	Description
708851	When visiting a website for the first time in Firefox, the disclaimer page is shown and the webpage loads normally. When visiting a website for a second time, Firefox may take a few minutes to show the disclaimer and then another few minutes to load the webpage. **Workaround**:use Chrome and Edge to visit websites.

Firewall

Bug ID	Description
654356	Traffic is not hitting the rule it should in policy-based NGFW mode.

FortiView

Bug ID	Description
683654	FortiView pages with FortiAnalyzer source incorrectly display a *Failed to retrieve data* error on all VDOM views when there is a newly created VDOM that is not registered to FortiAnalyzer yet. The error should only show on the new VDOM view.

GUI

Bug ID	Description
602397	Managed FortiSwitch and FortiSwitch Ports pages are slow to load when there are many managed FortiSwitches.
704618	When the login banner is enabled and the user is forced to log in again to the GUI (due to password change or enabling VDOMs), the user may see a *Bad Gateway* error. **Workaround**: refresh the browser.
707589	*System* > *Certificates* list sometimes shows incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Usesr should be able to delete the certificate after all references are removed.

IPsec VPN

Bug ID	Description
644780	Rectify the consequences if password renewal on FortiClient is canceled.
672925	Traffic cannot pass through IPsec tunnel after being offloaded to NPU.
691718	Traffic cannot pass through IPsec tunnel after FEC is enabled on server side if NAT is enabled between VPN peers.
708940	Old session traffic is blocked after an ADVPN shortcut is established when `link-down-failover` is enabled.

Proxy

Bug ID	Description
663088	Application control in Azure fails to detect and block SSH traffic with proxy inspection.
701513	WAD encounters segmentation fault crash at `wad_http_scan_engine__on_unblock`.

REST API

Bug ID	Description
597494	REST API incorrectly returns error code 401 (authentication error) instead of 403 (authorization error) for requests that pass the authentication check but are not permitted to access the resource.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
672218	Root FortiGate VDOM topology view page still shows CSF tree for all VDOMs if set to multi-VDOM mode.

SSL VPN

Bug ID	Description
550819	guacd is consuming too much memory and CPU resources during operation.

Switch Controller

Bug ID	Description
699533	In FortiOS 7.0.0, the default authentication protocol for a switch controller SNMP user is SHA256, as opposed to the default SHA1 in previous versions.

System

Bug ID	Description
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
666418	SFP interfaces on FG-330xE do not show link light.
678704	FortiGate cannot join FortiManager.

Upgrade

Bug ID	Description
708250	Console prints `__set_clr_flag:wwan ioctl failed, flag:0x0200 errno:19` when upgrading from 6.4.5 to 7.0.0.

VM

Bug ID	Description
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).

WAN Optimization

Bug ID	Description
702876	FortiGate web cache does not work in proxy mode.

WiFi Controller

Bug ID	Description
700356	CAPWAP daemon crashing due to IoT detection.
703685	VLAN-tagged CAPWAP traffic was dropped by NP6XLite FortiGate when FortiAP is connected through aggregate FortiLink FortiSwitch.

Built-in AV engine

Resolved engine issues

Bug ID	Description
530470	DLP blocking HTML file categorized as a BAT file.
601088	AV engine will empty attached PDF when doing CDR for it.
607099	Antivirus scanunit is crashing.
607432	Get 500 internal error for some PDFs with AV applied.
613213	Fixed DLP encrypted files control not working on small encrypted files.
614078	Fixed CDR not being able to open some PDF files.
621636	Fixed CDR not being able to remove macros from some XLSM attachments.
637845	AV falsely blocks some files as corrupted.
675519	Virus in custom RPM 3.0 file not detected by AV.
680593	Emails with some PDFs are not delivered when CDR is enabled.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW mode.
638341	In some cases, IPS fails to get interface ID information that would result in IPS incorrectly dropping the session during static matching.
645848	FortiOS is providing self-signed CA certificate intermittently with flow-based SSL certificate inspection.
646961	Explicit FTPS data channel cannot be established through policy with flow-based inspection mode and AV enabled
654363	Traffic logs shows `policy violation` for traffic hitting the allow policy in NGFW mode.
669138	IPS Engine 4.067 crashes (segmentation fault and alarm clock).
676705	Custom IEC-104 application control signatures skipped after signature database update.
683669	Firewall schedule settings are not following daylight saving time.
688888	BZIP2 file including EICAR is detected in the original direction of the flow mode firewall policy even though `scan-bzip2` is disabled.
691196	One-arm IPS URL filter unable to block HTTPS websites.
691395	Signature false positives causing outage after IPS database update.
695441	Not getting past block/override page or warning page when doing a web filter override in flow mode.
695774	Remote category flow and proxy mode wildcard matching difference
696753	Chassis has multiple IPS crashes and UTM web filter is impacted after enabling web filter content header.
696819	IPS archive timestamp is dated from 1970.

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