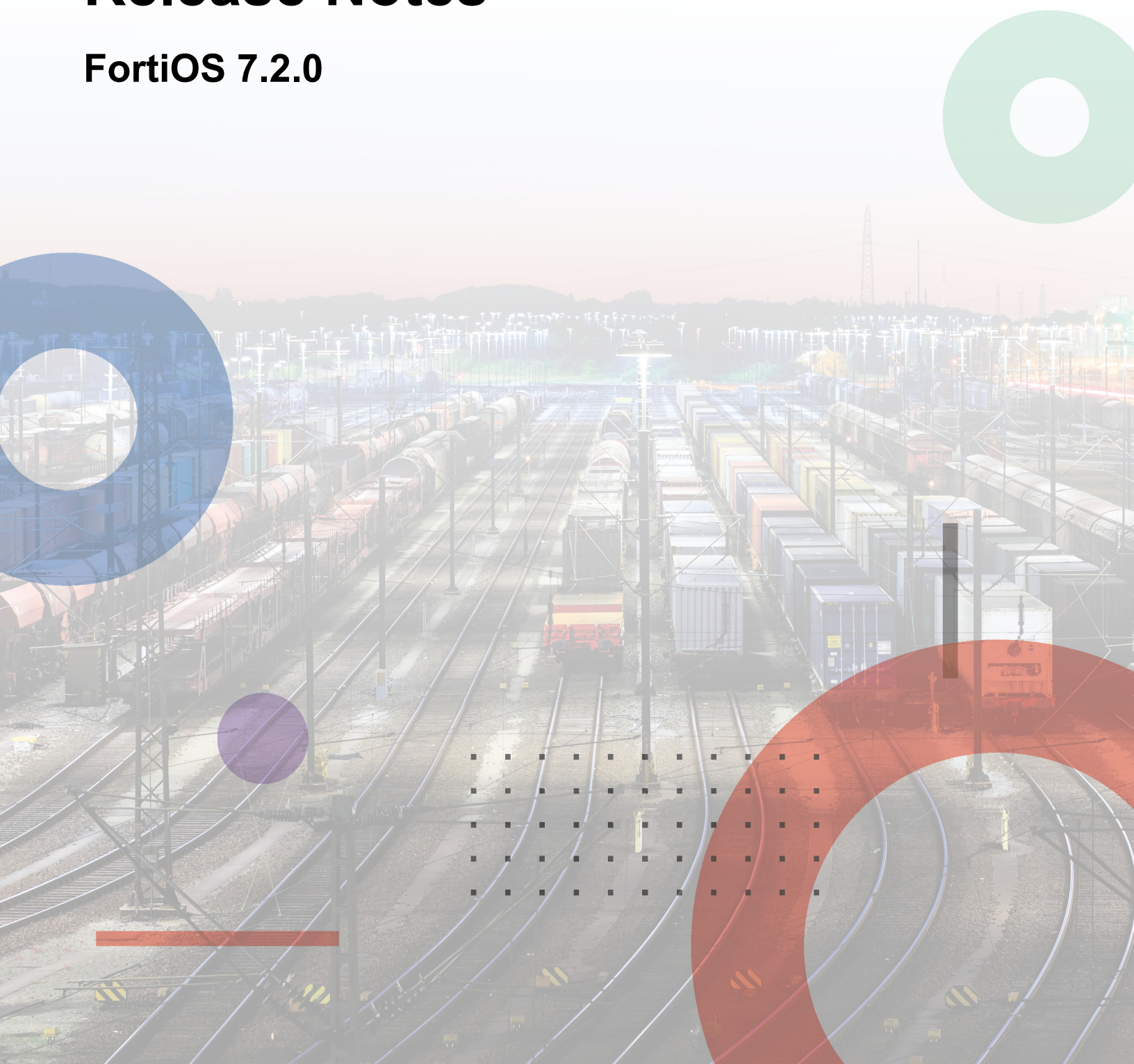
FORTINET

Release Notes

FortiOS 7.2.0



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/training-certification

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 31, 2022
FortiOS 7.2.0 Release Notes
01-720-768157-20220331

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-03-31	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.2.0 build 1157.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.2.0 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-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1500D, FG-1500DT, FG-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-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, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-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

Changes in CLI

Bug ID	Description
735470	The following settings under `config firewall vip/vip6` are hidden when NAT46/NAT64 is enabled: • `http-redirect` • `http-multiplex` • `max-embryonic-connections` • `http-host` • `http-host` option for `ldb-method`
738151	Previously, SSL certificate options for VIP access proxy configurations contained an option for CA certificates. A configuration using a CA certificate would cause a *ERR_SSL_KEY_USAGE_INCOMPATIBLE* error because it is not a server certificate. Now, the CLI will filter out certificates that do not exist, are a CA certificate, or are not valid. Previous configurations in which SSL certificate options get filtered are upgraded to use default the FORTINET_SSL certificate.
743309	Change `config vrf-leak/config vrf-leak` to `config vrf/config vrf6` and `config target` to `config leak-target` in BGP settings. `config router bgp` `  config vrf` `  edit <vrf>` `  config leak-target` `  edit <id>` `  set route-map <string>` `  set interface <string>` `  next` `  end` `  next` `  end` `end`
749250	Add setting for IPv4 reachable time (previously only IPv6 was supported). `config system interface` `  edit <name>` `  set reachable-time <integer>` `  next` `end` The IPv4 reachable time is measured in milliseconds (30000 - 3600000, default = 30000).
751346	Allow IPv6 DNS server override to be set when DHCPv6 prefix delegation is enabled. `config system interface` `  edit <name>`

Bug ID	Description
	`` config ipv6 set ip6-mode static set dhcp6-prefix-delegation enable set ip6-dns-server-override enable end next end ```
753631	Add option to configure H323/RAS direct model traffic. ``` config system settings set h323-direct-model {enable | disable} end ``` The setting is disabled by default (the wide open pinhole will be closed); however when upgrading from an older version, the setting will be enabled to preserve the previous behavior.
756881	The following options in the one-arm sniffer policy configuration are removed. ``` config firewall sniffer edit <id> set host <string> set port <string> set protocol <string> set vlan <string> set ipv6 {enable | disable} set non-ip {enable | disable} set max-packet-count <integer> set free-style {enable | disable} set free-style-filter <string> next end ```
774154	Add `auth-timeout` setting in `config wireless-controller timers` to configure the waiting time after which a wireless client is considered to fail RADIUS authentication and times out (in seconds, 5 - 30, default = 5). ``` config wireless-controller timers set auth-timeout <integer> end ```

Changes in GUI behavior

Bug ID	Description
718291	The *Log & Report* > *Events* page is renamed to *System Events*. Improvements include: • A *Summary* tab that displays the top five events in each event log type, and a line chart to show aggregated events by each level • A *Details* tab that drills down to a detailed log view by event type • Clicking an event in the *Summary* tab will automatically bring users to the *Details* tab with appropriate filters applied
739172	The *System* > *Firmware* page in the main menu has been removed. The *System* > *Firmware* shortcut from the top-right dropdown menu has also been removed, and was replaced with a shortcut to the *Fabric Management* page.
739180	The *Log & Report* UTM log subtypes are combined into a *Security Events* log page. Improvements include: • A *Summary* tab that displays the top five events in each security event log type • A *Details* tab that drills down to a detailed log view by UTM type • Clicking an event in the *Summary* tab will automatically bring users to the *Details* tab with appropriate filters applied
754542	The new *Log & Report* > *FortiAnalyzer Reports* page displays FortiAnalyzer reports in the FortiOS GUI. Administrators can generate, delete, and edit report schedules, and view and download generated reports.
756881	Remove the previous *Network* > *Packet Capture* menu and replace it with the *Network* > *Diagnostics* menu. The new *Packet Capture* page streams the capture in real-time. It also allows users to select a packet and view its header and payload information in real-time. Once completed, packets can be filtered by various fields or filtered through the search bar. It can be saved as a PCAP file for further analysis.
758638	Debug flows can now be executed from GUI on the *Network* > *Diagnostics* > *Debug Flow* page. Debug flow output is displayed in real-time until it is stopped. The completed output can be filtered by time, message, or function. It can be exported as a CSV file.

Changes in default behavior

Bug ID	Description
718290	When using FortiGuard servers for DNS, FortiOS will default to using DNS over TLS (DoT) to secure the DNS traffic. New FortiGuard DNS servers are added as primary and secondary servers.
738438	Split-task VDOM mode is removed. When a VDOM is set to `multi-vdom` mode, individual VDOMs can be configured as an `admin` type. • When the `vdom-type` is set to `admin`, the VDOM is used for local traffic only. Administrative users can log in to the FortiGate using SSH, HTTPS, and so on. • When the `vdom-type` is set to `traffic`, the VDOM can pass traffic just like regular VDOMs previously. Upon upgrade, if a FortiGate is in `split-vdom` mode, then it will be converted to `multi-vdom` mode. The FG-traffic VDOM will become a traffic type VDOM. The root VDOM will become an admin VDOM.
743583	AV and IPS packages are now signed by the Fortinet CA to ensure authenticity of the packages. The FortiGate will execute the following checks based on the method used to perform updates: • During automatic updates, only signed and validated packages are accepted. • During manual package updates, signed and validated packages will be accepted. If a package is not signed, the following applies: • Level-0: accept the new package even if it is unsigned. • Level-1: display a warning and request a user confirmation to accept. • Level-2: display an error and reject the image. • If no level is configured, apply Level-1. • For HA and configuration synchronization, the secondary device will synchronize signature files from the primary in the presence of a saved signed package. FDN will maintain signed and unsigned packages for 7.2 and pre-7.2 compatibility. FortiManagers used for package distribution will also download signed and unsigned packages for backwards compatibility.

Changes in table size

Bug ID	Description
778197	Increase SDN connector table size to 256 on high-end FortiGates (FG-1xxx and higher, 2U).
784755	Increase number of managed FortiSwitches from 16 to 24 for 60F and 80F series FortiGates.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
491991	Support Websense Integrated Services Protocol (WISP) server in flow mode, which allows the FortiGate to send traffic to the third-party web filtering service for rating. This feature was previously only supported in proxy-based security profiles.
535099	Update MAC address filter under VAP configuration to directly use a firewall address group containing MAC addresses. `config wireless-controller vap` `edit <name>` `set address-group <firewall_address_group>` `set address-group-policy {allow | deny}` `next` `end` Previous `wireless-controller address` and `wireless-controller addrgrp` commands have been removed.
655389	Add IPv6 options for SSH client in the CLI. `# execute ssh6-options {interface <outgoing_interface> | reset | source6 <source_IPv6_interface> | view-settings}`
665383	Switch controller supports dynamic discovery in FortiLink over L3 mode for new FortiSwitch platforms and FortiSwitches with split ports (`phy-mode`).
678544	Add option to configure MAC authentication bypass (MAB) re-authentication from the switch controller globally or as a local override.
684236	In NGFW policy mode, a security policy can be configured in *Learn Mode* to monitor traffic that passes through the source and destination interfaces. These traffic and UTM logs use a special prefix in the `policymode` and `profile` fields so that FortiAnalyzer and the FortiManager Policy Analyzer can identify these logs for policy analysis.
684516	Add support for configuring flap guard settings on FortiSwitch through switch controller. When the configured number of changed events (`flap-rate`) is reached within a certain period of time (`flap-duration`), the flap guard is triggered and FortiSwitch will shut down the switch port. The protection is disabled after the timeout (`flap-timeout`) expires.
691337	Allow a GCP SDN connector to have multiple projects attached to it. Previously, GCP SDN connectors could only be associated with one project, a limit of 256 SDN connectors, and users could only add a maximum 256 projects to the FortiGate. A single GCP SDN connection can now have thousands of projects attached to it. Add support for dynamic address filters based on project name and zones: `config system sdn-connector`

Bug ID	Description
	`` edit <name> set type gcp config gcp-project-list edit <name> set gcp-zone-list <name_1> <name_2> ... <name_n> next end next end ``` GUI changes: • Add buttons to switch between *Simple* and *Advanced* project configurations. The simple configuration displays a single text field to add one project to the GCP SDN connector. • The advanced configuration displays a mutable table for users to add multiple projects to the GCP SDN connectors. Adding projects displays a slide-out pane to specify the project name and zones. • A confirmation slide-out pane appears when switching from advanced to simple to warn about projects being deleted from the GCP SDN connector. • A tooltip on the GCP SDN connector card shows the list of projects, and the filter list of GCP dynamic addresses shows the project and zones.
696871	Allow SSL VPN web portals to be defined in the ZTNA access proxy settings. The ZTNA access proxy handles the user and device authentication, posture check, and establishes the HTTPS connection between the end user and the access proxy. Then it forwards the user to the web portal where they can use pre-defined bookmarks to access internal and external resources.
705455	Improve FortiAnalyzer log caching in reliable mode to prevent lost logs sent when the FortiAnalyzer connection is down. Logs are first cached in memory, and once sent, they are moved to a confirm queue. The FortiGate periodically queries the FortiAnalyzer for the latest `seq_no` of the last log received and clears the logs from the confirm queue up to that `seq_no`. If the connection is down, the logs in the confirm queue will be re-sent when the connection is re-established.
714788	Add HA uninterruptible upgrade option, which allows users to configure a timeout value in minutes (1 - 30, default = 30) where the primary HA unit waits before the secondary HA unit is considered upgraded. ``` config system ha set uninterruptible-primary-wait <integer> end ```
718224	On some FortiSwitch models, the PHY mode on some ports can be changed in order to enable or disable split ports. When this configuration changes, it reboots the FortiSwitch and subsequently requires the FortiGate to re-discover and re-authorize the device. In this enhancement, the FortiGate is able to automatically update the port list and avoids re-discovering and re-authorizing the FortiSwitch after PHY mode changes and the device reboots.
718299	Support manual licensing for FortiGates running in air-gapped environments, such as industrial environments, where devices have no internet connections. The license can be uploaded from the *System* > *FortiGuard* page or CLI.

Bug ID	Description
	`# execute restore manual-license {ftp | tftp} <license_file> <server> [args]`
718332	In previous DARRP implementation, channel bandwidth was not considered. Now, DARRP will also consider the radio bandwidth in its channel selection, adding support for 40, 80, and 160 MHz channel bandwidth.
718406	On a software switch interface that is dedicated to FortiSwitch (FortiLink enabled), it is now possible to add an aggregate interface as an interface member. This allows FortiSwitches to be managed on a software switch that has aggregate interfaces as a member.
720631	Add fields for `source-ip` and `source-ip6` to set the source address used to connect to the ACME server. `config system acme` `  set source-ip <class_ip>` `  set source-ip6 <IPv6_address>` `end`
720687	Add VLAN switch support on FG-20xF.
722647	Add IPsec fast path in VPN/DPDK for FG-VM (ESXi, KVM, Hyper-V, AWS, and Azure). Only GCM128 and GCM256 cyphers supported. IPv6 tunnels, anti-replay, and transport mode are not supported. `config dpdk global` `  set ipsec-offload {enable | disable}` `end`
726701	Add option to set the application default port as service port in NGFW mode. This allows applications to match the policy and be blocked immediately the first time that traffic hits the firewall. When this option is enabled, the NGFW policy aggregates the ports used by the applications in the policy and does a pre-match on the traffic. This is changed from previous behavior where traffic must first be identified by IPS, and then policy matching occurs based on the matched port. `config system settings` `  set default-app-port-as-service {enable | disable}` `end` New installations have this setting enabled by default. Upgrades will have this setting disabled to maintain previous `post-application-match` default port enforcement behavior.
727416	Support captive portal addresses and authentication certificates at the VAP level and on physical interfaces. `config wireless-controller vap` `  edit <name>` `  set security captive-portal` `  set auth-cert <HTTPS_server_certificate>` `  set auth-portal-addr <portal_address>` `  next` `end`

Bug ID	Description
	config system interface edit <name> set security-mode captive-portal set auth-cert <HTTPS_server_certificate> set auth-portal-addr <portal_address> next end
727514	Enhance the *System* > *Fabric Management* to include the ability to authorize and register Fabric devices, and display the FortiCare registration status and device type.
727890	Improve communication between FortiOS and FortiClient EMS with more efficient queries that request incremental updates. Retrieved device information can be written into the FortiGate's FortiClient NAC daemon cache. This increases ZTNA scalability to support up to 50 thousand concurrent endpoints. This feature requires FortiClient EMS 7.0.3 or later that has the `common-tags-api` capability.
728408	Add handling for expect sessions created by session helpers in NGFW policy mode. For protocols that are only supported by IPS but not session helpers (IPv6 SIP), IPS falls back on using its own handling of these sessions, which is similar to profile mode.
730310	User information and TLS sessions are synchronized between HA members. When a failover occurs, the new primary unit will continue allowing sessions from the logged in users without asking for the client certificate and re-authentication again.
730337	Add the following ZTNA enhancements to FortiView and the log view: • Add *FortiView ZTNA Servers* monitor, which includes options to drill down by *Sources*, *Rules*, *Real Servers*, and *Sessions*. • Add context menu shortcuts on the *ZTNA Rules* and *ZTNA Servers* tabs to redirect to the FortiView and log view pages. • Replace *Log & Report* > *ZTNA* page with *Log & Report* > *ZTNA Traffic* page. ZTNA logs now have a traffic type and ZTNA subtype. • Add fields to ZTNA traffic logs.
731779	Add `restart-on-topology-change` option to control if OSPF/OSPFv3 should continue with a graceful restart when detecting topology changes. config router ospf6 set restart-mode {none | graceful-restart} set restart-period <1 - 3600> set restart-on-topology-change {enable | disable} end config router ospf set restart-on-topology-change {enable | disable} end

Bug ID	Description
732241	FortiOS supports FortiSandbox inline scanning in proxy inspection mode. When inline scanning is enabled, the client's file is held while it is sent to FortiSandbox for inspection. Once a verdict is returned, the appropriate action (allow or block) is performed on the held file. If there is an error or timeout on the FortiSandbox, the FortiGate's configuration determines what to do with the held file. Inline scanning requires a FortiSandbox appliance running version 4.2 or later. This feature is not supported on FortiSandbox Cloud or FortiGate Cloud Sandbox. `config system fortisandbox` `  set inline-scan {enable | disable}` `end` In the antivirus profile, the `ftgd-analytics` option is renamed to `fortisandbox-mode`. There are new options to set FortiSandbox inline scan error and timeout actions. `config antivirus profile` `  edit <name>` `  set fortisandbox-mode {inline | analytics-suspicious | analytics-everything}` `  set fortisandbox-error-action {ignore | log-only | block}` `  set fortisandbox-timeout-action {ignore | log-only | block}` `  set fortisandbox-max-upload <integer>` `  config {http | ftp | imap | pop3 | smtp | mapi | cifs | ssh}` `  set av-scan {disable | block | monitor}` `  set fortisandbox {disable | block | monitor}` `  end` `  next` `end`
736275	Mark endpoint records and host tags as out of synchronization when failure timeout occurs for the EMS APIs, `report/fct/sysinfo` and `report/fct/host_tags`. The `out-of-sync` threshold (in seconds, 10 - 3600) can be configured from the CLI. `config endpoint fctems` `  edit <name>` `  set out-of-sync-threshold <integer>` `  next` `end`
736841	Add two new options, policy change summary and policy expiry, to workflow management. The policy change summary enforces an audit trail for changes to firewall policies. The policy expiry allows administrators to set a date for the policy to be disabled.
737778	Support phase 2 selectors for injecting IKE routes on shortcut tunnels in IPsec `mode-cfg` mode, thereby eliminating the requirement of reflecting BGP routes between spokes in SD-WAN and ADVPN configurations. `config vpn ipsec phase1-interface` `  edit <phase1-interface_name>` `  set mode-cfg-allow-client-selector {enable | disable}` `  next` `end`

Bug ID	Description
738450	Add six new automation triggers based on event log categories: • IPS logs • Anomaly logs • Virus logs • SSH logs • Traffic violations • Web filter violations When multi-VDOM mode is enabled, individual VDOMs can be specified so that the trigger is only applied to the specified VDOMs.
738863	For dynamic addresses in IKE, the first item under `config list` that can be successfully converted into an IP address can be used when `mode-cfg` is enabled and `split-include` is used.
739145	Federated upgrade for managed FortiSwitches allows a newly authorized FortiSwitch to be upgraded to the latest supported version automatically. The latest compatible FortiSwitch firmware is downloaded from FortiGuard without needing user intervention. `config switch-controller managed-switch` `edit <id>` `set fsw-wan1-peer <interface>` `set fsw-wan1-admin enable` `set firmware-provision-latest {once | disable}` `next` `end` `config switch-controller global` `set firmware-provision-on-authorization {enable | disable}` `end` If `firmware-provision-on-authorization` is set to `enable`, `firmware-provision-latest` will be set to `once` automatically when the FortiSwitch administrative status (`fsw-wan1-admin`) is enabled. When the FortiSwitch connection status becomes authorized or up, a one-time upgrade to the latest compatible firmware version starts if `firmware-provision-latest` is set to `once`. A FortiSwitch can connect to multiple VDOMs, and it will be upgraded through any VDOM that it is authorized in.
739167	L3 roaming between different VLANs and subnets on the same or different wireless controller is supported. A client connected to the SSID on one FortiAP can roam to the same SSID on another FortiAP managed by the same or different FortiGate wireless controller and continue to use the same IP. When the client idles longer than the `client-idle-rehome-timeout`, the client will rehome and receive an address on the new subnet from the new FortiAP. `config wireless-controller timers` `set client-idle-rehome-timeout <integer>` `end` `config wireless-controller vap` `edit <name>`

Bug ID	Description
	`` set l3-roaming {enable | disable} next end config wireless-controller inter-controller set l3-roaming {enable | disable} end ```
739172	When performing a Fabric or non-Fabric upgrade under *System* > *Fabric Management* while choosing a firmware that requires multiple builds in the upgrade path, the FortiGate can follow the upgrade path to complete the upgrade automatically. This can be performed immediately or during a scheduled time.
739173	This enhancement improves upon BGP conditional advertisement by accepting multiple conditions to be used together. The conditional route map entries are treated with an AND operator. When the `condition-type` is `exist`: • If the conditional route map matches, then advertised route map will apply. • If the conditional route map does not match, then the advertised route map will not apply. When the `condition-type` is `non-exist`: • If the conditional route map matches, then the advertised route map will not apply. • If the conditional route map not matches, then advertised route map will apply.
739193	Add *IP Address Lookup* to the *Internet Service Database* page that allows users to look up IP information on demand from the ISDB and GeoIP database. Returned information includes reverse IP/domain lookup, location, reputation, and other internet service information.
739195	Improve the channel selection for each of the 2.4 GHz and 5 GHz wireless radios. For 2.4 GHz, two default channel plans (*Three Channels* and *Four Channels*) can be selected to automatically configure non-overlapping channels. For 5 GHz, a new slide-in page (*Set Channels*) with improved visualization is added to help users select their desired channels.
739740	Add a map of FortiSwitch model prefixes to full model names, and update the GUI to use these full model names on the *Managed FortiSwitches* page. For example, in previous versions the *Model* displayed for a FortiSwitch would be *FS1D24*, and now it is displayed as *FortiSwitch 1024D*.
740155	Add GUI configuration and improvements to the NAC LAN segmentation feature introduced in FOS 7.0.1. Improvements include: • Display NAC segment and LAN segment VLANs as parent and child on the *Network* > *Interface* page. • Add a *VLAN segment* toggle to apply VLAN segmentation to a switch VLAN interface. • Add a *NAC Settings* dialog to the *NAC Policies* page to enable NAC VLANs and modify the primary, onboarding, and segment VLANs.
740774	Previously, users could be assigned to VLANs dynamically according to the RADIUS attribute `Tunnel-Private-Group-Id` returned from the Access-Accept message. The value can either match a particular VLAN ID or a VLAN interface name. A third option is now added to match based on a VLAN name table defined under the virtual AP.
741715	Add option to allow administrators to enable or disable FFDHE groups for VIP SSL key share.

Bug ID	Description
	config firewall vip edit "access-proxy" set type access-proxy set ssl-accept-ffdhe-groups {enable | disable} next edit "server-load-balance" set server-load-balance set ssl-accept-ffdhe-groups {enable | disable} next end
742087	Enhance `link-monitor` to measure the SLA information of dynamic VPN interfaces that assign IP addresses to their clients during tunnel establishment. This includes SSL VPN tunnels, IPsec remote access, and IPsec site-to-site tunnels. config system link-monitor edit <name> set server-type {static | dynamic} next end # diagnose sys link-monitor tunnel {name | all} <tunnel_name>
742089	Upon receiving direct FSSO logon REST API requests, the FortiGate now returns the HTTP response code instantaneously and offloads the LDAP group membership query to a backend API. This improves response times, and prevents delays and backlogs when many requests are sent in a short time period.
742162	License enforcement on downstream devices by: • Supporting the CSF REST API via a FortiGate Cloud (FGC) tunnel from the root to downstream devices and vice-versa. • Restricting create, edit, and delete permissions when accessing devices without a subscription from the FortiGate Cloud portal. • Adding the ability to re-run notifications when switching via the CSF FortiGate chooser dropdown. • Showing read-only access notifications when users switch to a downstream device without a paid subscription from the FortiGate Cloud portal.
742364	Add options to increase flexibility in controlling how the FortiGate's routing engine resolves the BGP route's next hops. config router bgp set tag-resolve-mode {disable | preferred | merge} end The `preferred` option uses a tag match if a BGP route resolution with another route containing the same tag is successful The `merge` option merges the tag match with best match if they are using different routes. The results excludes the next hops of tag matches whose interfaces have appeared in best match.

Bug ID	Description
742981	Add mean opinion score (MOS) calculation and logging for performance SLA health checks. The MOS is a method of measuring voice quality using a formula that takes latency, jitter, packet loss, and the codec into account to produce a score from zero to five (0 - 5). The G.711, G.729, and G.722 codecs can be selected in the health check configurations, and an MOS threshold can be entered to indicate the minimum MOS score for the SLA to pass. The maximum MOS score will depend on which codec is used, since each codec has a theoretical maximum limit. Currently, the MOS cannot be used as the `link-cost-factor` to steer traffic in an SD-WAN rule.
743309	Enhance the SD-WAN, VPN, and BGP configurations to support the segmentation over a single overlay scenario. In this scenario, a hub and spoke SD-WAN deployment requires that branch sites, or spokes, are able to accommodate multiple companies or departments. Each company's subnet is separated by a different VRF. A subnet on one VRF cannot communicate with a subnet on another VRF between different branches, but can communicate with the same VRF.
743804	Add a RADIUS option to allow the FortiGate to set the RADIUS accounting message group delimiter to a comma (,) instead of a plus sign (+) when using RSSO. The default delimiter is still a plus sign.
744195	Add maximum output size (megabytes) and timeout (seconds) limit to the CLI script automation action settings. The script will stop if the either one of the limits is reached. `config system automation-action` `edit <name>` `set output-size <integer>` `set timeout <integer>` `next` `end` Add maximum concurrent stitch setting in `config automation setting` that limits how many stitches can run at same time. `config automation setting` `set max-concurrent-stitches <integer>` `end`
744652	Exchange the SD-WAN member's local cost on an ADVPN shortcut tunnel to give spokes the capability of using remote cost as a tie-breaker to select the preferred shortcut.
745158	When creating a software switch from *Network* > *Interfaces*, it is possible to add multiple FortiSwitch FortiLink VLANs as *Interface members*.
745169	Depending on which region a customer chooses to deploy their FortiSandbox Cloud instance, the FortiGate will automatically connect to fortisandboxcloud.com and discover the specific region and server to connect to.
745240	Add maximal field for each resource in `get system performance status` and improve average value accuracy by rolling over samples immediately when queried. Extend `api/v2/monitor/system/resource/usage` to include new maximum, minimum, and average fields for each resource.
746496	Optimize broadcast and multicast suppression over SSID tunnel mode across the FortiAP network.

Bug ID	Description
747602	Allow customization of RDP display size (width and height settings) for SSL VPN web mode when creating a new connection or bookmark. Administrators can also specify the display size when pre-configuring bookmarks.
749981	Allow the AWS SDN connector to use the AWS security token service (STS) API to connect to multiple AWS accounts concurrently. This allows a single AWS SDN connector to retrieve dynamic objects from multiple accounts, instead of needing to create an SDN connector for each account. `config system sdn-connector` `edit "aws1"` `config external-account-list` `edit "arn:aws:iam::6*******5494:role/CrossAccountSTS"` `set region-list "us-west-1" "us-west-2"` `next` `edit "arn:aws:iam::9*******1167:role/CrossAccountSTS"` `set region-list "us-west-1" "us-west-2"` `next` `end` `next` `end`
749982	Support activation of Flex-VMs when connecting to the internet using a web proxy. `# execute vm-license <token> http://user:pass@proxyip:proxyport`
750038	When configuring security policies in NGFW policy-based mode, it is possible to select and apply web filter URL categories and URL category groups. `config firewall security-policy` `edit <id>` `set url-category {g<group_value> <category_value>}` `next` `end`
750224	To enhance BFD support, FortiOS can now support neighbors connected over multiple hops. When BFD is down, BGP sessions will be reset and try to re-establish neighbor connection immediately.
750275	An application category can be selected as an SD-WAN service rule destination criterion. Previously, only application groups or individual applications could be selected. `config system sdwan` `config service` `edit <id>` `set internet-service enable` `set internet-service-app-ctrl-category <id_1> <id_2> ... <id_n>` `next` `end` `end`

Bug ID	Description
750309	The new Netflow fields, ipClassOfService and postIpClassOfService, for identifying class of service in traffic flows are supported in FortiOS. The FortiGate reads the TOS(IPv4)/Traffic Class(IPv6) fields from the first packet of incoming traffic flow for the ipClassOfService value, and the first packet of outgoing traffic flow for postIpClassOfService value. These fields were added to NetFlow template ID 262.
750310	Indicator of compromise (IoC) detection for local out traffic helps detect any FortiGate locally generated traffic that is destined for a known compromised location. The FortiGate will generate an event log to warn administrators of IoC detection.
750318	Support tracking of authenticated LDAP users by logging the users' group memberships and logon/logout timestamps into local files on the log disk over a rolling four-week period. The historical records can be queried from CLI. This feature is only enabled on FortiGate models with a log disk.
750319	Support UTM scanning and deep inspection for mail protocols SMTP, IMAP, and POP3 in ZTNA TCP forwarding access proxy.
750321	Enable TLS sessions to use an abbreviated TLS handshake instead of a full TLS handshake upon failover from a primary HA unit to a secondary HA unit in A-A or A-P mode. Instead of using the `admin-server-cert` to generate the key that is used in a TLS session ticket, FortiOS uses the web proxy global `ssl-ca-cert` that can be synchronized to the secondary HA member. When a TLS session reconnects after HA failover using the same session ticket as the first session, the new primary unit is able to generate the same key matching that session ticket and allow an abbreviated handshake.
750557	Enhance the *FortiSwitch Ports* page in port and trunk mode by adding a *Statistics* button and slide-in pane to view traffic statistics and issues. Enhance the *Diagnostics and Tools* slide-in pane by adding the fan and PSU status to the general health status, and a *Clients* tab to view clients for the specific FortiSwitch.
750702	Add support for FQDN and ZTNA TCP forwarding. A wildcard domain name can be in the TCP forwarding access proxy with the `domain` option under the real server settings. When a domain name request arrives, it matches the domain in the request with the configured domain. If there is a match, a DNS request is made and the destination of the request is the DNSed IP. If there is no match, a DNS request is made and the DNSed IP is matched with the configured real server's IP.
750902	Introduce real-time FortiView monitors for *Proxy Sources*, *Proxy Destinations*, and all *Proxy Sessions*. Proxy policy sessions are no longer show in *FortiView Policies* and *FortiView Applications*.
751525	Allow `flow-tracking` to be configurable for multiple NetFlow collectors. FortiSwitch 7.0.0 or later is required to support the multiple collectors configuration; otherwise, only the first collector will be supported.
751595	Add `email-to` and `subject` types in email filter `block-allow-list`. The `email` type has been renamed to `email-from`. `config emailfilter block-allow-list` `edit 1`

Bug ID	Description
	`` set name "bal list" config entries edit 1 set type email-to set pattern "test@fortinet.com" next edit 2 set type subject set pattern "Spam!" next end next end ``` The *Email Regular Expression* and *Email Wildcard* types have been replaced with *Sender Address*, *Recipient Address*, and *Subject*. Add *Pattern Type* selector with two values, *Wildcard* and *Regular Expression* for each type.
753108	Enhance DLP with backend updates and CLI changes. The following configuration commands are added: ``` config dlp data-type edit <name> set pattern <regex_pattern> set verify <regex_pattern> set look-back <integer> set look-ahead <integer> set transform <string> set verify-transformed-pattern {enable | disable} set comment <string> next end ``` ``` config dlp dictionary edit <name> set match-type {match-all | match-any} set comment <string> config entries edit <id> set type {credit-card | hex | keyword | regex | ssn-us} set pattern <string> set ignore-case {enable | disable} set repeat {enable | disable} set status {enable | disable} set comment <string> next end next end ```

Bug ID	Description
	config dlp sensor edit <name> set match-type {match-all | match-any | match-eval} set eval <string> set comment <string> config entries edit <id> set dictionary <dlp_dictionary> set count <integer> set status {enable | disable} next end next end config dlp profile edit <name> set feature-set proxy config rule edit <id> set proto <protocol> <protocol> ... set sensor <dlp_sensor> set action {allow | log-only | block | quarantine-ip} next end next end In config firewall policy and config firewall proxy-policy, the dlp-sensor option is renamed to dlp-profile.
753749	Remove support for Security Fabric loose pairing. Affected devices include: FortiADC, FortiDDoS, and FortiWLC.
754784	Implement support for NAT46 and NAT64 for SIP ALG, allowing customers that have mix of IPv4 and IPv6 networks to use SIP ALG for proper call handling.
754785	When authenticating with RADIUS in a wired or wireless scenario, the FortiGate can support proper handling of the Termination-Action AVP. In the wired scenario, a hardware switch configured with 802.1X security authentication can read the Termination-Action attribute value from the RADIUS Access-Accept response. If the Termination-Action is 1, the FortiGate will initiate re-authentication when the session time has expired. During re-authentication, the port stays authorized. If the Termination-Action is 0, the session will be terminated.
755141	The following existing options can be used to control explicit DoT handshakes. config system global set ssl-min-proto-version {SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2 | TLSv1-3} set ssl-static-key-ciphers {enable | disable} set strong-crypto {enable | disable}

Bug ID	Description
	`end`
756180	Allow both primary and secondary HA members to be registered to FortiCare at the same time from the primary unit. The secondary unit will register through the HA proxy. Display a new FortiCare *Register* option in the GUI on various Fabric related pages and widgets.
756538	Add Windows 11 and macOS 12 to the SSL VPN OS check. The following options are available for `config os-check-list <name>`: `macos-bigsur-11`, `macos-catalina-10.15`, `macos-mojave-10.14`, `macos-monterey-12`, `windows-7`, `windows-8.1`, `windows-10`, and `windows-11`. Operating systems no longer supported by FortiClient were removed.
756639	Update the OVF package so it reflects newer VMware ESXi and hardware versions.
757878	Allow pre-authorization of a FortiAP on the FortiGate wireless controller by specifying a wildcard serial number that represents the model of FortiAP being pre-authorized. For example, a wildcard serial number of FP231F****000001 will allow the first FortiAP-231F that registers to the wireless controller to be authorized automatically and adopt the profile configurations.
758133	Allow pre-authorization of a FortiSwitch on the FortiGate switch controller by specifying a wildcard serial number that represents the model of FortiSwitch being pre-authorized. For example, a wildcard serial number of S248EP****000001 will allow the first FortiSwitch-248E-POE that registers to the switch controller to be authorized automatically and adopt the profile configurations.
758552	Automatically detect and display the SSL VPN portal login page based on the user's browser language.
758560	Add macOS 12 and Windows 11 to SSL VPN host check. Windows 8 and macOS 10.9 to 10.13 are removed from the SSL VPN host check.
758588	A client certificate is configured on an LDAP server configuration when an LDAP server expects the LDAP client to use the client certificate to authenticate itself in order to access to the LDAP server. `config user ldap` `  set client-cert-auth {enable | disable}` `  set client-cert <source>` `end` The client certificate source comes from `config vpn certificate local`, and is filtered by client authentication key usage.
759873	On supported FortiSwitch models, it is possible to establish a VXLAN tunnel with the FortiGate over a layer 3 network, and use the VXLAN interface for the FortiLink connection. This allows for a layer 2 overlay over layer 3 routed network.
760210	Users have more options to filter IPS signatures when configuring IPS sensor profiles. Signatures can be selected by these additional attributes: default status, default action, vulnerability type, and last update date. `config ips sensor` `  edit <name>` `  config entries`

Bug ID	Description
	edit <id> set last-modified {before <date> | after <date> | between <start-date> <end-date>} set vuln-type <id_1> ... <id_n> set default-action {all | pass | drop} set default-status {all | enable | disable} next end next end
761397	Add *Process Monitor* page for displaying running processes with their CPU and memory usage levels. Administrators can view a list of running processes, sort and filter them, and select a process to terminate it. Enhancements have been made to the FortiGate Support Tool Chrome extension, including: backend capture support, CSF support, more daemon logging, pre-process CPU and memory charts, crash log support, REST API profiling, organized node logging, and WebSocket messages.
761507	In the *Top FortiSandbox Files* FortiView monitor, users can select a submitted file and drill down to view its static and dynamic file analysis. The full FortiSandbox report can be downloaded in PDF format. This feature works with FortiGate Cloud Sandbox, FortiSandbox Cloud, and FortiSandbox appliance. FortiSandbox must be running version 3.2.1 and later.
762238	Display a warning in the GUI and CLI when upgrading a device in an HA cluster that is out of synchronization.
763021	Allow dedicated scan to be disabled on FortiAP F-series profiles, which then allows background scanning using the WIDS profile to be enabled on radios 1 and 2.
763275	In dynamic port policies, it is now possible to use the hardware vendor as a filter for the device patterns.
763381	Support multiple members per SD-WAN neighbor configuration and the new `minimum-sla-meet-members` option to configure the minimum number of members that must be in an SLA for preferable route map to be used. For a current SD-WAN neighbor plus `route-map-out-preferable` design, only one member can be defined in the SD-WAN neighbor configuration for one BGP neighbor. If the member is in SLA, the preferable route map will be applied on the BGP neighbor; otherwise, the default route map will be applied. In the case of one BGP neighbor over multiple SD-WAN members, the current SD-WAN neighbor plus `route-map-out-preferable` mechanism is enhanced to allow defining multiple members in the SD-WAN neighbor configuration for one BGP neighbor. The new `minimum-sla-meet-members` option can flexibly trigger a route map change based on a minimum threshold of in-SLA members.
763832	DNS servers learned through DHCP may not support the default FortiOS configured DoT protocol. The `dns-server-protocol` setting under config `system interface > edit <name>` is introduced to offer the ability to chose the protocol for DNS servers learned through DHCP under any interface.

Bug ID	Description
764679	When sending a response to an SNMP request for ipAddressTable, append the IP address type (type 1 for IPv4, type 2 for IPv6) and number of octets (four for IPv4, 16 for IPv6) in the format `1.3.6.1.2.1.4.34.1.3.<type>.<octet>`.
765018	In multi VDOM mode, users can choose which VDOM is used by FortiGuard services to initiate updates, instead of being locked to the management VDOM. This allows deployment scenarios where the management VDOM is a closed network. `config global` `  config system fortiguard` `  set vdom <vdom>` `  end` `end`
765301	Add `advpnsc` log field to the VPN event log to indicate that a VPN event is based on an ADVPN shortcut. A value of 1 indicates the tunnel is an ADVPN shortcut, and 0 indicates that it is not.
765315	When authenticating with RADIUS in a wireless scenario, the FortiGate can support proper handling of the Termination-Action AVP. In the wireless scenario, when a virtual AP is configured with WPA2-Enterprise security with RADIUS and has CoA enabled, it processes the RADIUS CoA request immediately upon receiving it and re-authenticates when the Termination-Action is 1.
765322	To improve GUI performance, an option is added to enable loading static GUI artifacts cached in CDN (content delivery network) servers closer to the user rather than from the FortiGate. On failure, the files can fall back to loading from the FortiGate. `config system global` `  set gui-cdn-usage {enable | disable}` `end`
765708	Support access control for SNMP based on MIB view and VDOM. Administrators can provide access control to SNMP based on restricting an MIB view to specific OID subtrees or by VDOM. This allows multi-tenant FortiGate deployments to give restricted access per VDOM.
766171	When the `admin-restrict-local` setting is enabled under `config system global`, local administrators cannot be used until all remote authentication servers are down. In this enhancement, the FortiGate only checks all remote authentication servers that are applied in `config system admin` are down, instead of all remote servers configured on the FortiGate, before allowing local administrators to log in.
766182	On the *WiFi & Switch Controller* > *FortiSwitch Clients* page, client devices connected to the managed FortiSwitches are displayed. Clicking a client entry shows more information about the port and policies associated with the client device.
766236	Add option to perform SD-WAN on-demand packet duplication only when SLAs in the configured service is matched. When the `sla-match-service` option is enabled, only the SLA health checks and targets used in the service rule are used to trigger the packet duplication. Prior to this, when using an SD-WAN on-demand duplication rule that is configured to match a service rule, the duplication will only be triggered when all SLA health checks miss their thresholds. This is the same behavior as when `sla-match-service` is disabled.

Bug ID	Description
	config system sdwan config duplication edit <id> set service-id <rule_id> set packet-duplication on-demand set sla-match-service {enable | disable} next end end
766237	Add Fortinet objects to the built-in Internet Service Database (ISDB) in the FortiOS image to assist in scenarios where firewall rules or policy routes use the ISDB to access FortiGuard servers after booting up.
767347	Allow the FortiGate to act as an 802.1X supplicant. The new configurations can be enabled from the network interface in the CLI. The EAP authentication method can be either PEAP or TLS using a user certificate. config system interface edit <interface> set eap-supplicant {enable | disable} set eap-method {peap | tls} set eap-identity <identity> set eap-password <password> set eap-ca-cert <CA_cert> set eap-user-cert <user_cert> next end
767991	Add and update the following log fields for HTTP transaction related logs to improve log analysis coverage: • Add field for HTTP method (`httpmethod`). • Change URL rating method field (`method`) to `ratemethod`. • Extend user agent field (`agent`) to save the whole `User-Agent` header. • Remove referrer from `rawdata` field and insert it into the `referralurl` field.
768820	Remove overlap check for VIPs so there are no constraints when configuring multiple VIPs with the same external interface and IP. Instead, a new security rating report will alert users of any VIP overlaps.
769154	Allow empty address groups with no members in the GUI, CLI and through the API.
769807	Add option to configure console port login on a managed FortiSwitch. config switch-controller switch-profile edit "default" set login {enable | disable} next end
771742	Multicast traffic shaping is supported under the following conditions:

Bug ID	Description
	• In `config router multicast`, `multicast-routing` is enabled (and multicast routing is properly configured). • In `config firewall shaper traffic-shaper`, `per-policy` is disabled (default setting). Per-policy enabled shapers are not supported. • In `config firewall multicast-policy`, `auto-asic-offload` is disabled. `config firewall multicast-policy` `edit <id>` `set traffic-shaper <string>` `next` `end` Running `diagnose sys mcast-session list` displays traffic shaper information for each path.
773126	Add support for Apple French keyboard layout for RDP in SSL web portal, user bookmark, and user group bookmark settings (`set keyboard-layout fr-apple`).
773530	Allow a two-hour grace period for Flex-VMs to begin passing traffic upon retrieving a license from FortiCare without VM entitlement verification from FortiGuard.
773558	Allow VRRP to be configured on an EMAC-VLAN interface.
773615	Support IPv4 over IPv6 DS-Lite service in virtual network enabler (VNE) tunnels. In addition, the VNE tunnel fixed IP mode supports username and password authentication.
777675	By default, the connection from the ZTNA access proxy to the backend servers uses the IP of the outgoing interface as the source. This enhancement enables customers to use an IP pool as the source IP, or use the client's original IP as the source IP. This allows ZTNA to support more sessions without source port conflict. `config firewall proxy-policy` `edit <id>` `set type access-proxy` `set poolname <ip_pool>` `set transparent {enable | disable}` `next` `end`
779304	Support backing up and restoring configuration files in YAML format. `# execute backup yaml-config {ftp | tftp} <filename> <server> [username] [password]` `# execute restore yaml-config {ftp | tftp} <filename> <server> [username] [password]`
780869	When the Security Fabric is not enabled on a FortiGate, it will still run a lightweight mode to display managed FortiSwitches and FortiAPs in topology view and tree view. It also supports federated upgrades between the FortiGate and the managed FortiSwitches and FortiAPs.

Bug ID	Description
782594	Allow the `route-map` to apply priority on BGP routes, which enables the hub to mark the preferred path learned from branches with higher priority instead of utilizing numerous SD-WAN service rules on the hub. `config router route-map` `edit <name>` `config rule` `edit <id>` `set set-priority <integer>` `next` `end` `next` `end`

Upgrade information

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

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.2.0 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.2
FortiManager	• 7.0.2
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 33
FortiClient* EMS	• 7.0.3 build 0229 or later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 or later
FortiClient* Mac OS X	• 7.0.3 build 0131 or later
FortiClient* Linux	• 7.0.3 build 0137 or later
FortiClient* iOS	• 7.0.2 build 0036 or later
FortiClient* Android	• 7.0.2 build 0031 or later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 4.2.0 and later for post-transfer and inline scanning

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

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

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.0. When Security Fabric is enabled in FortiOS 7.2.0, all FortiGate devices must be running FortiOS 7.2.0.

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*.

Strong cryptographic cipher requirements for FortiAP

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

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

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

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

Product integration and support

The following table lists FortiOS 7.2.0 product integration and support information:

Web browsers	• Microsoft Edge • Mozilla Firefox version 98 • Google Chrome version 99 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.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	• 5.0 build 0306 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
AV Engine	• 6.00273
IPS Engine	• 7.00212

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESX	• Versions 4.0 and 4.1
VMware ESXi	• Versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

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

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

Resolved issues

The following issues have been fixed in version 7.2.0. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
701658	High CPU utilization because of scanunitd process spike and crash.
769563	Archive bomb detection made more lenient to prevent false positives.

Data Leak Prevention

Bug ID	Description
763687	If a filter configured with `set archive enable` matches a HTTP post, the file is not submitted for archiving (unless `full-archive proto` is enabled).

DNS Filter

Bug ID	Description
692482	DNS filter forwards the DNS status code 1 `FormErr` as status code 2 `ServFail` in cases where the redirect server responses have no question section.
748227	DNS proxy generated local out rating (FortiGuard category) queries can time out if they are triggered for the same DNS domains with the same source DNS ID.

Endpoint Control

Bug ID	Description
777294	Fabric connection failure between EMS and FortiOS.

Explicit Proxy

Bug ID	Description
754191	Websites are not accessible if the `certificate-inspection` SSL-SSH profile is set in a proxy policy.
754259	When an explicit proxy policy has a category address as destination address, the FortiGate needs to check if the address is a Google Translate URL for extra rating. This will trigger a keyword match. However, if a web filter profile is not set yet, WAD will crash. The fix will delay the keyword match until a web filter profile is present.
755298	SNI `ssl-exempt` result conflicts with CN `ssl-exempt` result when SNI is an IP.
765761	Firewall with forward proxy and UTM enabled is sending TLS probe with forward proxy IP instead of real server IP.
766127	PAC file download fails with `incorrect service` error after upgrading to 7.0.2.
771152	GUI does not display *Source Address* field when using a proxy address group in authentication rules.
780211	`diagnose wad stats policy list` output displays information for only 20 proxy policies, so not all policies are included.
783946	Explicit proxy policy does not deny request for ClearPass object if it is used as a source.
785342	FortiGate explicit proxy does not work with SOCKS4a.

Firewall

Bug ID	Description
644638	Policy with a Tor exit node as the source is not blocking traffic coming from Tor.
724145	Expiration timer of expectation session may show a negative number.
744888	FortiGate drops SERVER HELLO when accessing some TLS 1.3 websites using a flow-based policy with SSL deep inspection.
747190	When `auto-asic-offload` is enabled in policy, IP-in-IP sessions show as expired while tunnel traffic goes through the FortiGate.
752784	Packet is dropped due to the wrong UDP header length. The NP6XLite driver and kernel drop the packet because of the transport header check.
761494	HTTP persistence not working for HTTP cookie and SSL session ID for round-robin load balancer.
761646	FQDN address and FQDN custom service do not work as expected in security policy.
767226	When a policy denies traffic for a VIP and `send-deny-packet` is enabled, the `mappedip` is used for the RST packet's source IP instead of the external IP.

Bug ID	Description
767294	The `match-vip` option is only useful for deny policies; however, its flag is not cleared after changing the policy action from deny to accept. When a policy uses a mapped FQDN VIP, the destination field of the `iprope` policy accepts the full IP range.
770668	The packet dropped counter is not incremented for `per-ip-shaper` with `max-concurrent-session` as the only criterion and offload disabled on the firewall policy.
773035	Custom services name is not displayed correctly in logs with a port range of more than 3000 ports.
775783	Get httpsd signal 11 crash when inline editing custom service from policy list page with FortiGate support tool running.
778513	Forward traffic logs do not show MAC address object name in *Device* column.
779902	FortiGate policy lookup does not work as expected (in the GUI and CLI) when the destination interface is a loopback interface.
780721	Some firewall policies do not work on FG-2500E after upgrading.
784939	*Dashboard* > *Load Balance Monitor* is not loading in 7.0.4 and 7.0.5.

FortiView

Bug ID	Description
546312	Application filter does not work when the source is ISDB or unscanned.
765993	*Dashboard* > *FortiView Sources - WAN* monitor does not show data for VLAN interface.

GUI

Bug ID	Description
473841	Newly created deny policy incorrectly has logging disabled and can not be enabled when the CSF is enabled.
535099	The SSID dialog page does not have support for the new MAC address filter.
535794	Policy page should show new name/content for firewall objects after editing them from the tooltip.
630216	A user can browse HA secondary logs in the GUI, but when a user downloads these logs, it is the primary FortiGate logs instead.
663558	*Log Details* under *Log & Report* > *Events* displays the wrong IP address when an administrative user logs in to the web console.

Bug ID	Description
713529	When a FortiGate is managed by FortiManager with FortiWLM configured, the HTTPS daemon may crash while processing some FortiWLM API requests. There is no apparent impact on the GUI operation.
720192	GUI logs out when accessing FortiView monitor page if the VDOM administrator only has `ftviewgrp` permission.
729324	*Managed FortiAPs* and *Managed FortiSwitches* pages keep loading when VDOM administrator has `netgrp` and `wifi` read/write permissions.
730533	On the *Policy & Objects* > *Firewall Policy* page, an unclear error message appears when a user creates a new SSL VPN policy with a web mode portal and a VIP or VIP group is used as the destination address.
746239	On the *Policy & Objects* > *Virtual IP* page the GUI does not allow the user to configure two virtual IPs with different service for the same external/mapped IP and external interface.
746953	On the *Network* > *Interfaces* page, users cannot modify the TFTP server setting. A warning with the message *This option may not function correctly. It is already configured using the CLI attribute: tftp-server.* appears beside the *DHCP Options* entry.
750490	Firewall policy changes made in the GUI remove the replacement message group in that policy.
751219	*Last Login* in *SSL-VPN* widget is shown as *NaN* on macOS Safari.
751482	cmbdsvr signal 11 crash occurs when a wildcard FQDN is created with a duplicate ID.
753398	httpsd crashes after NGFW policy is deleted.
754539	On the *Policy & Objects* > *Addresses* page, filters applied on the *Details* column do not work.
755625	Application control profile cannot be renamed from the GUI.
755893	Dashboard menus are not translated for non-English languages.
756420	On the *Security Fabric* > *Fabric Connectors* page, the connection to FortiManager is shown as down even if the connection is up.
757130	After upgrading, the new ACME certificates configured in the GUI are using the staging environment.
757606	*Dashboard* > *Users & Devices* > *Firewall Users* widget cannot load if there is a client authenticated by the WiFi captive portal.
758820	The GUI cannot restore a CLI-encrypted configuration file saved on a TFTP server. There is no issue for unencrypted configuration files or if the file is encrypted in the GUI.
760863	PPPoE interface is not selectable if interface type is *SSL-VPN Tunnel*.
761615	Unable to see details of Apache.Struts.MPV.Input.Validation.Bypass log.
761658	*Failed to retrieve information* warning appears on secondary node faceplate.
761933	FSSO user login is not sorted correctly by duration on *Firewall Users* widget.
762683	The feature to send an email under *User & Authentication* > *Guest Management* is grayed out.

Bug ID	Description
763724	After the current session is disconnected, pressing the `Enter` key does not restart a new session on the GUI CLI console.
764744	On the *Network* > *Explicit Proxy* page, the GUI does not support configuring multiple outgoing IP addresses.
768261	After two-factor authentication times out, the next login always fails with `logincheck_handler -- Invalid username`.
770948	When using NGFW policy-based mode, the *VPN* > *Overlay Controller VPN* option is removed.
772311	On the LDAP server page, when clicking *Browse* beside *Distinguished Name* and then clicking *OK* after viewing the query results, the LDAP server page is missing fields containing the server settings.
776969	Unable to select and copy serial number from *System Information* dashboard widget.
777145	*Managed FortiSwitches* page incorrectly shows a warning about an unregistered FortiSwitch even though it is registered. This only impacts transferred or RMAed FortiSwitches. This is only a display issue with no impact on the FortiSwitch's operation.
778258	Unable to set IP address for IPsec tunnel in the GUI.
778542	Local domain name disappears from the GUI after clicking *API Preview*.
778932	MAC address name is not displayed in the *Device* column in the *Asset Identity Center*.
779181	Security rating *Optimization* card shows failure for system uptime due to low uptime for FortiAP (less than 24 hours).
783152	Filtering by *Status* in the *SD-WAN* widget is not working.
787007	httpsd is crashing without any interaction on the GUI at `api_cleanup_cache in api_cmdb_v2_handler`.
788935	GUI is slow to load when CDN is enabled and accessed on a closed network.

HA

Bug ID	Description
664929	The hatalk process crashed when creating a disabled VLAN interface in an A-P cluster.
683584	The hasync process crashed because the write buffer offset is not validated before using it.
683628	The hasync process crashes often with signal 11 in cases when a CMDB mind map file is deleted and some processes still mind map the old file.
701367	In an HA environment with multiple virtual clusters, *System* > *HA* will display statistics for *Uptime*, *Sessions*, and *Throughput* under virtual cluster 1. These statistics are for the entire device. Statistics are not displayed for any other virtual clusters.

Bug ID	Description
714788	Uninterruptible upgrade might be broken in large-scale environments.
738728	The secondary unit tries to contact the forward server for sending the health check packets when the `healthcheck` under `web-proxy forward-server` is enabled.
744349	Unable to connect to FortiSandbox Cloud through proxy from secondary node in an HA cluster.
750004	The secondary FortiGate shows a DHCP IP was removed due to conflict, but it is not removed on the primary FortiGate.
750829	In large customer configurations, some functions may time out, which causes an unexpected failover and keeps high cmdbsvr usage for a long time.
751072	HA secondary is consistently unable to synchronize any sessions from the HA primary when the original HA primary returns.
752892	PPPoE connection gets disconnected during HA failover.
752928	fnbamd uses `ha-mgmt-interface` for certificate related DNS queries when `ha-direct` is enabled.
752942	When the secondary is being synchronized, the GARP is sent out from the secondary device with the physical MAC address.
753295	Configuration pushed from FortiManager does not respect `standalone-config-sync` and is pushed to all cluster members.
754599	SCTP sessions are not fully synchronized between nodes in FGSP.
757494	A member might not be able to be added to an aggregate interface that is down in an HA cluster.
760562	hasync crashes when the size of hasync statistics packets is invalid.
761581	`Tunnel to Fortimanager is down` log message is generated on the secondary FortiGate unit (without HA management interface).
764873	FGSP cluster with UTM does not forward UDP or ICMP packets to the session owner.
765619	HA desynchronizes after user from a read-only administrator group logs in.
766842	Long wait and timeout when upgrading FG- 3000D HA cluster due to vluster2 being enabled.
771389	SNMP community name with one extra character at the end stills matches when HA is enabled.
771391	HA uptime remains the same after `mondev` failure.
773901	The dnsproxy daemon is not updating HA management VDOM DNS after it is configured. The secondary also does not update.
775724	Static routes not installed after HA failover.
776258	FortiGate needs time to complete reconnecting PPPoE network if it part of an HA cluster.
778011	The hasync daemon crashes on FG-80E.
779512	If the interface name is a number, an error occurs when that number is used as an `hbdev` priority.

Bug ID	Description
782769	Unable to form HA pair when HA encryption is enabled.
783483	On the *System* > *HA* page, *Sessions* are shown as *0* after upgrading from 7.0.3 to 7.0.4.
785514	In some cases, the fgfmd daemon is blocked by a query to the HA secondary checksum, and it will cause the tunnel between FortiManager and the FortiGate to go down.

Intrusion Prevention

Bug ID	Description
715360	Each time an AV database update occurs (scheduled or manually triggered), the IPS engine restarts on the SLBC secondary blade.
751027	FortiGate can only collect up to 128 packets when detected by a signature.
755859	The IPS sessions count is higher than system sessions, which causes the FortiGate to enter conserve mode.
775696	Each time an AV database update occurs (scheduled or manual), the IPS engine restarts on the SLBC secondary blade. This stops UTM analysis for sessions affected by that blade.

IPsec VPN

Bug ID	Description
735412	IKE HA resynchronizes the synchronized connection without an established IKE SA.
738863	For dynamic addresses in IKE, the first item under `config list` that can be successfully converted into an IP address can be used when `mode-cfg` is enabled and `split-include` is used.
749509	IPsec traffic dropped due to anti-replay after HA failover.
766750	FortiGate does not accept secondary tunnel IP address in the same subnet as the primary tunnel.
767765	Tooltip in *Dashboard* > *Network* > *IPsec*widget for phase 2 shows a *Timeout* year of 1970 in Firefox, Chrome, and Edge.
767945	In a setup with IPsec VPN IKEv2 tunnel on the FortiGate to a Cisco device, the tunnel randomly disconnects after updating to 7.0.2 when there is a CMDB version change (configuration or interface).
768638	Invalid IP address while creating a VPN IPsec tunnel.
770354	L2TP over IPsec stopped encrypting traffic after upgrading from 6.4 to 7.0.2.

Bug ID	Description
770437	Referenced IPsec phase 1 and phase 2 interfaces can be deleted.
771302	Spoke cannot register to OCVPN when FortiGate is in policy-based NGFW mode.
773313	FG-40F-3G4G with WWAN DHCP interface set as L2TP client shows drops in WWAN connections and does not get the WWAN IP.
777398	Calling-Station-ID is not present in the RADIUS packet.
780850	IPsec hub fails to delete selector routes when NAT IP changed and IKE crashed.
781917	`Session clash` messages appear in event logs for new sessions from VPN towards VIP.
783597	Framed IP is not assigned to IPsec clients configured with `set assign-ip-from usrgrp`.
786409	Tunnel had one-way traffic after iked crashed.
789705	IKE crash disconnected all users at the same time.

Log & Report

Bug ID	Description
621329	Mixed traffic and UTM logs are in the event log file because the current `category` in the log packet header is not big enough.
705455	FortiAnalyzer logs are not cached between actual and detected loss of connection.
745689	Unknown interface is shown in flow-based UTM logs.
753904	The reportd process consumes a high amount of CPU.
757703	Report suddenly cannot be generated due to no response from reportd.
764478	Logs are missing on FortiGate Cloud from the FortiGate.
774767	The expected reboot log is missing.
777008	The syslogd daemon encounters a memory leak.
783145	Cyrillic alphabet is not displayed correctly in file filter and DLP logs.

Proxy

Bug ID	Description
650348	FortiGate refuses incoming TCP connection to FTP proxy port after explicit proxy related configurations are changed.

Bug ID	Description
712584	WAD memory leak causes device to go into conserve mode.
738151	Browser has *ERR_SSL_KEY_USAGE_INCOMPATIBLE* error when both ZTNA and web proxy are enabled.
739627	`diagnose wad stats policy list` does not show statistics correctly when enabling certificate inspection and HTTP policy redirect.
747915	Deep inspection of SMTPS and POP3S starts to fail after restoring the configuration file of another device with the same model.
751674	Load balancer based on HTTP host is DNATing traffic to the wrong real server when the correct real server is disabled.
752744	Proxy-based certificate with deep inspection fails upon receipt of a large handshake message.
754969	Explicit FTP proxy chooses random destination port when the FTP client initiates an FTP session without using the default port.
755294	Firefox gives `SEC_ERROR_REUSED_ISSUER_AND_SERIAL` error when ECDSA CA is configured for deep inspection.
756603	WAD memory spike when downloading a file larger than 4 GB.
756616	High CPU usage in proxy-based policy with deep inspection and IPS sensor.
758122	WAD memory usage may spike and cause the FortiGate to enter conserve mode when downloading a large file fails.
758496	WAD crash due to LDAP group looping.
758532	WAD memory usage may spike and cause the FortiGate to enter conserve mode.
760585	Captive portal fails to open requested web page on first try if WAD user is expired.
764193	The three-way handshake packet that was marked as `TCP port number reused` cannot pass through the FortiGate, and the FortiGate replies with a `FIN, ACK` to the client.
765349	Once AV is enabled in proxy mode, traffic will be blocked in proxy mode.
768358	Failure to access certain AWS pages with proxy SSL deep inspection.
772041	WAD crash at signal 11.
774859	WAD signal 11 Segmentation fault crash occurs at `wad_h2_port_read_sync`.
775193	Frequent WAD crashes are causing the FortiGate to go down.
775966	Changes to address group used for full SSL exemptions are not being activated.
776989	In some cases, WAD daemon `signal 6 (Aborted) received` occurs when adding a VDOM.
778659	Proxy inspection fails due to `ipsapp session open failed: all providers busy`.
782426	WAD crash with signal 11 and signal 6 occurs when performing SAML authentication if the URL size is larger than 3 KB.

Bug ID	Description
783112	FortiGate goes into conserve caused due to high memory usage of WAD `user-info` process.
783438	When diagnosing WAD memory with a significant number of open HTTP sessions, the function pointer may still be called and will cause a segmentation fault.
792505	Memory leak identified for WAD worker `dnsproxy_conn` causing conserve mode.

REST API

Bug ID	Description
743169	Update various REST API endpoints to prevent information in other VDOMs from being leaked.
768056	HTTPS daemon is not responsive when successive API calls are made to create an interface.

Routing

Bug ID	Description
710606	Some static routes disappear from RIB/FIB after modifying/installing static routes from the GUI script.
717086	External resource local out traffic does not follow the SD-WAN rule and specified egress interface when the `interface-select-method` configuration in `system external-resource` is changed.
724541	One IPv6 BGP neighbor is allowed to be configured with one IPv6 address format and shows a different IPv6 address format.
728058	A typo in `set dst` when configuring a static route with a valid `set device` will result in a default static route.
744589	LDAP external connector/FSSO polling traffic is not following the SD-WAN rules.
745856	The default SD-WAN route for the LTE wwan interface is not created.
748508	IKE might add two connected static routes to the same destination. If they are using same interface, deleting one of the routes will make the connected address stored on that interface get deleted.
759711	OSPF E2 routes learned by Cisco routers are randomly removed from the routing table when the OSPF/OSPFv3 neighbor flaps.
759752	FortiGate is sending malformed packets causing a BGP IPv6 peering flap when there is a large amount of IPv6 routes, and they cannot fit in one packet.
762258	When policy-based routing uses a PPPoE interface, the policy route order changes after rebooting and when the link is up/down.

Bug ID	Description
769321	After ADVPN HA failover, BGP is not established, and tunnels are up but not passing traffic between the hub and spokes.
770923	OSPF authentication error occurs with MD5 or text authentication.
771052	The `set next-hop-self-rr6 enable` parameter not effective.
771423	BGP route map community attribute cannot be changed from the GUI when there are two 16-byte concatenated versions.
772023	Deleted BGP summary routes are not removed from routing table and are still advertised to eBGP neighbors.
772400	IPv6 route is not created for SIT tunnel interface in SD-WAN.
778392	Kernel panic crash occurs after receiving new IPv6 prefix via BGP.
779113	When a link monitor fails, the routes indicated in the link monitor are not withdrawn from the routing database.
779320	Multicast PIM hello packet is rejected by the FortiGate.
780210	Changing the interface weight under SD-WAN takes longer to be applied from the GUI than the CLI.
781483	Incorrect BGP Originator_ID from route reflector seen on receiving spokes.
783168	IPv6 secondary network is removed from the routing table after reboot.
784950	The `ecmp-max-paths` are not behaving as expected.

Security Fabric

Bug ID	Description
758493	SDN connector on FG-Azure stays stuck if it is alphabetically the first subscription that is not in the permission scope.
764825	When the Security Fabric is enabled, logging is not enabled on deny policies.
765525	The deleted auto-scripts are not sent to FortiManager through the auto-update and cause devices go out of sync.
767976	Downstream FortiGate csfd process crashed randomly with signal 11.

SSL VPN

Bug ID	Description
741674	Customer internal website (https://cm***.msc****.com/x***) cannot be rendered in SSL VPN web mode.
748085	Authentication request of SSL VPN realm can now only be sent to user group, local user, and remote group that is mapped to that realm in the SSL VPN settings. The authentication request will not be applied to the user group and remote group of non-realm or other realms.
749857	Web mode and tunnel mode could not reflect the VRF setting, which causes the traffic to not pass through as expected.
751366	JS error in SSL VPN web mode when trying to retrieve a PDF from https://vpn.ca***.com/.
751717	SAML user configured in groups in the IdP server might match to the wrong group in SSL VPN user authentication if an external browser is used.
752055	VNC (protocol version 3.6/3.3) connection is not working in SSL VPN web mode.
752351	When SSL VPN interface is turned down and then manually turned up again, the SSL routes are not added back to the kernel router.
753590	Brickstream web interface is not loading properly when accessed using SSL VPN web mode.
755296	SSL VPN web mode has issues accessing https://te***.or***.kr.
756561	Outdated OS support for host check should be removed.
757450	SNAT is not working in SSL VPN web mode when accessing an SFTP server.
758525	Users can modify the URL in SSL VPN portal to show connection launcher even when the *Show Connection Launcher* option is disabled.
759664	Renaming the server entry configuration will break the connection between the IdP and FortiGate, which causes the SAML login for SSL VPN to not work as expected.
760407	Unable to add domain entry in `split-dns` if `set domains` contains an underscore character (_).
760875	SSL VPN PKI users fail to log in when a special character is included in the CN or subject matching field.
762479	Telnet connection gets disconnected after three to four minutes in SSL VPN web mode while the connection is idle.
762685	Punycode is not supported in SSL VPN DNS split tunneling.
763619	SAP Fiori webpage using JSON is not loading in SSL VPN web mode.
764853	SSL VPN bookmark of VNC is not using ZRLE compression and consumes more bandwidth to end clients.
765258	Endpoint event is not reported when FortiClient 7.0 connects to SSL VPN.
767230	Issues with user log out request with Okta as an identity provider for SAML authentication.
767818	SSL VPN bookmark issues with internal website.

Bug ID	Description
767869	SCADA portal will not fully load with SSL VPN web bookmark.
768362	Default resolution for RDP/VNC in SSL VPN web mode cannot be configured.
768994	SSL VPN crashed when closing web mode RDP after upgrading.
770024	Resource is not reachable using SSL quick connection.
770452	Clicking an SSL VPN web portal bookmark web link displays blank page.
770919	Internal website (*.blt.local) is not loading in SSL VPN web mode.
771145	SSL VPN web mode access problem occurs for web service security camera.
771162	Unable to access SSL VPN bookmark in web mode.
772191	Website is not loading in SSL VPN web mode.
773254	SSL VPN web mode access is causing issues with MiniCAU.
774661	Unable to load SSL VPN web portal internal webpage.
774831	Comma character (,) is acting as delimiter in authentication session decoding when CN format is `Surname, Name`.
776069	The sslvpn daemon crashes due to memory access after it has been freed.
781542	Unable to access internal SSL VPN bookmark in web mode.
781550	HTTPS link is not working in SSL VPN web mode.
782732	Webpages of back-end server behind https://vpn-***.sys***.pl/remote/ could not be displayed in SSL VPN web mode.
783508	After upgrading to 6.4.8, NLA security mode for SSL VPN web portal bookmark does not work.
784335	Unable to load internal website in SSL VPN web mode.
784426	SSL VPN web mode has problems accessing ComCenter websites.
784522	When trying to create a support ticket in Jira with SSL VPN proxy web mode, the dropdown field does not contain any values.
784887	A blank page appears after logging in to an SSL VPN bookmark.
786179	Cannot reach local application (dat***.btn.co.id) while using SSL VPN web mode.
788641	Internal site not loading in SSL VPN web mode.
789644	Internal site not loading completely using SSL VPN web mode bookmark.

Switch Controller

Bug ID	Description
766583	A bin/cu_acd crash is generated when `cfg-revert` is enabled and involves FortiSwitch.

Bug ID	Description
774848	Bulk MAC addresses deletions on FortiSwitch is randomly causing all wired clients to disconnect at the same time and reconnect.
776442	FortiSwitch VLANs cannot be created in the FortiGate GUI for a second FortiLink.

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.
679035	NP6 drops, and bandwidth is limited to under 10 Gbps in `npu-vlink` case.
679059	The ipmc_sensord process is killed multiple times when the CPU or memory usage is high.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
699152	Add support for QinQ (802.1ad) on FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, and FG-3600E platforms.
706543	FortiGuard DDNS does not update the IP address when the PPPoE reconnects.
708228	A DNS proxy crash occurs during `ssl_ctx_free`.
712156	FortiCloud central management does not work if the FortiGate has trusted host enabled for the `admin` account.
716341	SFP28 port flapping when the speed is set to 10G.
718307, 729078	Verizon LTE connection is not stable, and the connection may drop after a few hours.
720687	On FG-20xF, the RJ45 ports connected to Dell N1548 switch do not automatically have an up link for energy detect mode.
722781	MAC address flapping on the switch is caused by a connected FortiGate where IPS is enabled in transparent mode.
738423	Unable to create a hardware switch with no member.
743945	Inconsistency between GUI and CLI with respect to changing password for any super_admin accounts.
749250	Firewall does not seem to utilize its ARP cache and is ARPing for a client MAC addresses every 20-30 seconds.
749613	Unable to save configuration changes and get `failed: No space left on device` error.
750533	The cmdbsvr crashes when accessing an invalid `firewall vip` mapped IP that causes traffic to stop traversing the FortiGate.
751044	There is no sensor trap function and related logs on SoC4 platforms.

Bug ID	Description
751346	DNS server obtained via DHCPv6 prefix delegation is not used by DNS proxy.
751523	When changing mode from DHCP to static, the existing DHCP IP is kept so no CLI command is generated and sent to FortiManager.
751870	User should be disallowed from sending an alert email from a customized address if the email security compliance check fails.
754567	FortiGate receives `Firmware image without valid RSA signature loaded` error when loading the image from FortiCloud.
755268	When changing a `per-ip-shaper`, if there is ongoing traffic offloaded by NPU and it attaches that shaper, the new shaper's quota will not get updated.
755953	Direct CLI script from FortiManager fails due to additional `end` at the end of `diagnose debug crashlog read`.
756160	Unable to configure firewall access control lists on FG-20xF.
756445	Flow-based inspection on WCCP (L2 forwarding) enabled policy with VLAN interfaces causes traffic to drop if `asic-offload` is enabled.
756713	Packet Loss on the LAG interface (eight ports) in static mode. Affected models: FG-110xE, FG-220xE, and FG-330xE.
757478	Kernel panic results in reboot due the size of inner Ethernet header and IP header not being checked properly when the SKB is received by the VXLAN interface.
757689	When creating a new interface with MTU override enabled, PPPoE mode, and a set MTU value, the MTU value is overridden by the default value.
757748	WAD memory leak could cause system to halt and print `fork() failed` on the console.
758545	Memory leak cause by leaked JSON object.
758815	Connectivity issue on port26 because NP6 table configuration has an incorrect member list. Affected models: FG-110xE, FG-220xE, and FG-330xE.
759689	When updated related configurations change, the updated configurations may crash.
760661	DDNS interface update status can get stuck if changes to the interface are made rapidly.
760942	dnsproxy signal 11 crash at `libcrypto.so.1.1` on FWF-61F.
763185	High CPU usage on platforms with low free memory upon IPS engine initialization.
764954	FortiAnalyzer serial number automatically learned from miglogd does not send it to FortiManager through the automatic update.
764989	Include an entry in SNMP OID that lists the number of octets for the IP type.
765452	Slow memory leak in IPS engine 6.091, which persists in 6.107.
766834	forticron allocates over 700 MB of memory, causes the FortiGate to go into conserve mode, and causes kernel panic due to 100 MB of configured CRL.
767778	Kernel panic occurs while adding and deleting LAG members on FG-1101E.

Bug ID	Description
768979	On a FortiGate with many FortiSwitches and FortiAPs, the *Device Inventory* widget and `user-device-store list` are empty.
769384	Kernel goes into conserve mode due to high memory consumption of confsyncd process.
771267	Zone transfer with FortiGate as primary DNS server fails if the FortiGate has more than 241 DNS entries.
771442	Discrepancy between session count and number of active sessions; sessions number creeps high, causing high memory utilization.
773067	CLI help text for link monitor `failtime` and `recoverytime` range should be `(1 - 3600, default = 5).`
773702	FortiGate running startup configuration is not saved on flash drive.
774443	SCP restore TCP session does not gracefully close with FIN packet.
777044	On a FortiGate only managed by FortiManager, the FDNSetup Authlist has no FortiManager serial number.
777145	FortiCloud FDS/selective update response contains `PendingRegistration` when not pending.
778116	Restricted VDOM user is able to access the root VDOM.
778474	dhcpd is not processing discover messages if they contain a 0 length option, such as 80 (rapid commit). The warning, `length 0 overflows input buffer`, is displayed.
778629	Disabling NP6XLite offloading does not work with VLAN interface on LAG one-arm scenario.
779241	DCE-RPC expectation session expires and never times out (`timeout=never`).
781137	Firewall gives incorrect information related to `link_setting` when running `diagnose hardware device nic <port>`.
783545	Backing up to SFTP does not work when the username contains a period (.).
789203	High memory usage due to DoT leak.
793401	fcnacd keeps using 99% CPU.

Upgrade

Bug ID	Description
754180	MAC address group is missing in the configuration after upgrading if it has members with other address groups that come behind the current one.
766472	After upgrading, the diagnostic command for redundant PSU is missing on FG-100F.
790823	VDOM links configuration is lost after upgrading.

User & Authentication

Bug ID	Description
679016	A fnbamd crash is caused when the LDAP server is unreachable.
747651	There is no LDAP-based authentication possible during the time WAD updates/reads group information from the AD LDAP server.
749488	On an HA standby device, certain certificates (such as Fortinet_CA_SSL) regenerate by themselves when trying to edit them in CLI. This also causes issues when backing up configurations on the standby device.
749694	A fnbamd crash is caused by an LDAP server being unreachable.
751763	When MAC-based authentication is enabled, multiple RADIUS authentication requests may be sent at the same time. This results in duplicate sessions for the same device.
755302	The fnbamd process spikes to 99% or crashes during RADIUS authentication.
756763	In the email collection captive portal, a user can click *Continue* without selecting the checkbox to accept the terms and disclaimer agreement.
757883	FortiGate blocks expired root CA, even if the cross-signed intermediate CA of the root CA is valid.
765136	Dynamic objects are cleared when there is no connection between the FortiGate and FortiManager with NSX-T.
767844	User ID/password shows as blank when sending the guest credentials via a custom SMS server in *Guest Management*.
777004	Local users named pop or map do not work as expected when trying to add then as sources in a firewall policy.
781992	fssod crashes with signal 11 on `logon_dns_callback`.

VM

Bug ID	Description
689047	ARM64-KVM has kernel panic.
691337	When upgrading from 6.4.7 to 7.0.2, GCP SDN connector entries that have a `gcp-project-list` configuration will be lost.
735441	Low performance when copping files from server behind FG-VM to another site via IPsec VPN.
750889	DHCP relay fails when VMs on different VLAN interfaces use the same transaction ID.
755016	In AWS, if the HA connection between active and passive nodes breaks for a few seconds and reconnects, sometimes the EIP will remain in the passive node.

Bug ID	Description
759300	gcpd has signal 11 crash at `gcpd_mime_part_end`.
764184	Inconsistent TXQ selection degrades mlx5 vfNIC. Azure FortiGate interface has high latency when the IPsec tunnel is up.
769352	Azure SDN connector is unable to pull service tag from China and Germany regions.
774404	The vmxnet3 driver is causing IPv6 neighbor solicitation packets to be ignored.
781879	Flex-VM license activation failed to be applied to FortiGate VM in HA. Standalone mode is OK.
785234	GCP HA failover for external IP does not work when using Standard Tier.
785353	Azure performance issue on MLX5 when an unrelated VPN is up.
789223	Azure China uses the wrong API endpoint to get meta data after secondary becomes the new primary.

VoIP

Bug ID	Description
757477	PRACK will cause voipd crashes when the following conditions are met: `block-unknown` is disabled in the SIP profile, the PRACK message contains SDP, and PRACK fails to find any related previous transactions (this is not a usual case).
770888	Progress OpenLogicalChannel is not translated.

Web Application Firewall

Bug ID	Description
785743	When a web application firewall profile has version constraint enabled, HTTP 2.0 requests will be blocked.

Web Filter

Bug ID	Description
728104	A webpage categorized as one of the blocked categories is not actually blocked because some sites may have subdomains or paths categorized in a block category that should be blocked, but instead the request is transformed into a format unrateable by FortiGuard.

Bug ID	Description
770941	Unable to block https://cle***.com/oauth/dis***-pic*** using URL filter; content from cle***.com is still shown.
779278	FortiGate is responding on TLS 1.0, TLS 1.1, and SSLv3 on TCP port 8015.
781515	The urlfilter daemon continuously crashes on the secondary unit.

WiFi Controller

Bug ID	Description
489759	Consistent error messages, `internal_add_timer`, appear on console when running an automation script.
630085	A cw_acd crash is observed on the FortiGate when the FortiAP is deleted from the managed AP list.
727301	Unable to quarantine hosts behind FortiAP and FortiSwitch.
734801	Some Apple devices cannot handle 303/307 messages, and may loop to load the external portal page and fail to pass authentication. Some android devices cannot process JavaScript redirect messages after users submit their username and password.
744687	Client should match the new NAC policy if it is reordered to the top one.
745044	Optimize memory usage of wpad daemon in WiFi controller for large-scale 802.11r fast BSS transition deployment.
745642	Consider not generating rogue AP logs once a certain AP has been marked as accepted.
748479	cw_acd is crashing with signal 11 and is causing APs to disconnect/rejoin.
750425	In RADIUS MAC authentication, the FortiGate NAS-IP-Address will revert to 0.0.0.0 after using the FortiGate address.
757189	A batch of APs in cluster are exhibiting control messages that the maximal retransmission limit reached, and the APs disconnect from the FortiGate.
761996	If `concurrent-client-limit-type` is set to `unlimited` it is limited by the `max-clients` value in the VAP profile.
766652	FortiAP firmware status is inconsistent on *System* > *Fabric Management* page and upgrade slide.
773027	*Client limit* description tooltip displayed in the GUI shows incorrect information.
773742	Two-factor authentication and WPA2-Enterprise WiFi conflict on `remoteauthtimeout` setting.
775157	A packet with the wrong IP header could not be processed by the CAPWAP driver, which randomly causes the FortiGate to reboot.
776576	FortiAP upgrade panel still prompts to upgrade to latest firmware, even when FortiAP is operating latest firmware.

Bug ID	Description
780732	Unable to import MPSK keys in the GUI (CSV file into an SSID). An *Invalid file content* error appears.
783209	The `arrp-profile` table can now be purged if no entry is in use.
790367	FWF-60F has kernel panic and reboots by itself every few hours.
792738	The cw_acd process uses high CPU, which causes issues for FortiAP connecting with CAPWAP.

ZTNA

Bug ID	Description
765813	ZTNA access is systematically denied for ZTNA rule using SD-WAN zone as an incoming interface.
770350	ZTNA tags do not follow the correct policy when bound in a single policy. They also do not work with groups.
770877	Traffic was blocked by mismatched ZTNA EMS tags in a forwarding firewall policy.
777669	The secondary IP address in the EMS dynamic address table does not match the expected policy.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
752450	FortiOS 7.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-44168

Known issues

The following issues have been identified in version 7.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
775742	Upgrade EMS tags to include classification and severity to guarantee uniqueness.

Firewall

Bug ID	Description
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic. **Workaround**: rename the custom section to unique name between IPv4 and IPv6 policies.
750081	Traffic can pass through EMAC VLAN interface but can not be offloaded.
777231	*FortiView Traffic Shaping* monitor should not show an entry with no shaper.
794648	Cannot set `src-vendor-mac` in policy. The `src-vendor-mac` policy setting is not lost after upgrading from 7.0.5 and is still in the iprope.

FortiView

Bug ID	Description
787886	The tooltip for the *Bandwidth* column in the *FortiView Traffic Shaping by Bandwidth* widget incorrectly displays the receiving bandwidth as *0 bps*.

GUI

Bug ID	Description
651648	Searching for address groups on the *Addresses* page and address dialog is slow due to recursive algorithm.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI *Forward Traffic* log page can take time to load if there is no specific filter for the time range. **Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs.
740508	Bandwidth widget shows incorrect traffic on FG-40F.
778844	*Dashboard* and *Managed FortiAPs* pages can take a long time to load when there are over 1000 FortiAPs configured.
781310	*Policy & Objects* > *DNAT & Virtual IPs* page can take more than 30 seconds to load if there are more than 25 thousand virtual IPs.

HA

Bug ID	Description
750087	Multicast convergence on HA failover.
781463	FortiGate does not respond to ARP request for `management-ip` on interface if the interface IP is changed.

IPsec VPN

Bug ID	Description
564920	IPsec VPN fails to connect if FortiGate has `ftm-push` configured.
699973	IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages.
769567	UDP/TCP failures on performance test with IPsec.
781403	IKE is consuming excessive memory.

Limitations

Bug ID	Description
617042	ACI dynamic address table size is limited to 1000 entries on FortiGate per EPG.

Log & Report

Bug ID	Description
770352	On the *Log & Report* > *Forward Traffic* page, filters applied to an interface name with a comma (,) do not show the correct filtered results for that interface.
788724	The secondary FortiGate did not send the logs to the syslog server (`sendmmsg failed to send data`).

Routing

Bug ID	Description
618684	Static route will still in routing table after HA failover, and the BFD is down on the new primary.
795213	Named static route addition on an SD-WAN zone is causing the creation of a default blackhole route.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
741084	Entry-level FortiGate with Security Fabric enabled for 30 or more downstream FortiGates can go into conserve mode when loading the physical or logical topology pages, or running security rating reports. **Workaround**: configure fewer downstream FortiGates in a Security Fabric configuration.
793474	FortiManager card has red color on *Security Fabric* > *Fabric Connectors* page.

SSL VPN

Bug ID	Description
486837	SSL VPN with external DHCP servers is not working.
795381	FortiClient Windows cannot be launched with SSL VPN web portal.

System

Bug ID	Description
540389	Remote administrator password renewal shows Remote Token instead of New password (CLI and GUI)
716250	Incorrect bandwidth utilization traffic widget for VLAN interface based on LACP interface.
725048	Performance improvements for `/api/v2/monitor/system/available-interfaces` (phase 2).
761546	The graphs for sessions on the *Dashboard* page may be incorrect for the 12 and 24 hour periods.
776646	Configuring a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server in the GUI fails with a CLI internal error.
790446	The vwl process is spiking CPU and memory, which triggers conserve mode.

User & Authentication

Bug ID	Description
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.

VM

Bug ID	Description
782073	IBM HA is unable to fail over route properly when route table has a delegate VPC route.

ZTNA

Bug ID	Description
792829	WAD re-challenges user authentication upon HA failover.

Built-in AV engine

Resolved engine issues

Bug ID	Description
558678,	Implemented AV timeout checks throughout MS Office CDRs and PDF parsers to prevent AV engine crash.
754519	Implemented AV timeout checks throughout MS Office CDRs and PDF parsers to prevent scanunitd crash.
769563	Make archive bomb detection more lenient to prevent false positives.
771674	Fixed malformed trailer and xref stream in PDF files caused by CDR reconstruction. CDR returning `NULL` value for reconstructed PDF file paths has been fixed.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
713508	Low download performance occurs when SSL deep Inspection is enabled on aggregate and VLAN interfaces when nTurbo is enabled.
754579	Application performance is ten times worse when IPS is applied in flow mode.
757314	IPS engine crashes after upgrading to 6.4.7 and is affecting traffic.
765859	Repeated IPS engine signal 11 and signal 7 crashes occur.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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

www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.