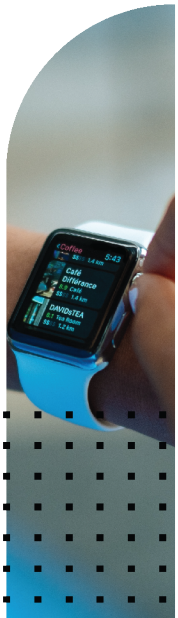
Release Notes

FortiOS 7.0.2



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

October 22, 2021
FortiOS 7.0.2 Release Notes
01-702-745052-20211022

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-10-20	Initial release.
2021-10-22	Updated Special notices on page 7.

Introduction and supported models

This guide provides release information for FortiOS 7.0.2 build 0234.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.2 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-201E, 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-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-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

Special notices

Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

GCP-On-Demand image

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

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

ALI-On-Demand image

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

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

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

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

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

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

FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
    edit <id>
        set fec enable
    next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

Changes in CLI

Bug ID	Description

713694	Configuring individual ciphers to be used in SSH administrative access can now be done from the CLI. Administrators can select the ciphers and algorithms used for SSH encryption, key exchange, and MAC using the following settings:
	`config system global`
	`set ssh-enc-algo <algo 1> [<algo 2> ... <algo n>]`
	`set ssh-kex-algo <algo 1> [<algo 2> ... <algo n>]`
	`set ssh-mac-algo <algo 1> [<algo 2> ... <algo n>]`
	`end`
	Previous configurations for enabling or disabling certain ciphers and algorithms have been deprecated.

719315	Add a new `block-sevrfail` option for `block-action` attribute in `dnsfilter profile`. Returns `SERVFAIL` for blocked domains.

721747	Add authd SSL control options for maximum protocol version SSL/TLS connections and signature algorithms for HTTPS authentication (affects TLS versions 1.2 and lower):
	`config user setting`
	`set auth-ssl-max-proto-version [default | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2]`
	`set auth-ssl-sigalgs [no-rsa-pss | all]`
	`end`
	The `auth-ssl-max-proto-version` default setting is no limit (`default`). The `auth-ssl-sigalgs` default setting is `all`.

725877	Change auto-scale `master-ip` to `primary-ip`.
	`config system auto-scale`
	`set primary-ip <IP address>`
	`end`

732007	The `virtual-host-only` attribute under `config vpn ssl web realm` is now hidden unless a virtual host is defined. Add `virtual-host-server-cert` attribute:
	`config vpn ssl web realm`
	`edit <url-path>`
	`set virtual-host-only {enable | disable}`
	`set virtual-host-server-cert <certificate>`
	`next`
	`end`

732645	Allow Security Fabric upstream to be specified as IP or FQDN, and change the setting from `upstream-ip` to `upstream`.

Bug ID	Description
	config system csf set upstream <IP or FQDN> end

Changes in GUI behavior

Bug ID	Description
727501	Several ZTNA features are now configurable from the GUI on the *ZTNA Servers* tab: • When configuring *Service/Server Mapping*, a new toggle enables load balancing and a dropdown to select different load balancing methods. • When configuring *Service/Server Mapping*, *TCP Forwarding* can be selected under the *Service* option, which can be configured in the new slide-in pane by setting the TCP forwarding server and using a toggle to enable additional SSH options. • SAML can be enabled and configured on a ZTNA server. Additionally: • *Log & Report* has a menu item for *ZTNA* logs. • Some settings under `config authentication setting` can be configured under *User & Authentication* > *Authentication Settings*.
728746	Users are now able to export the current view of the *Policy & Objects* > *Firewall Policy* page to CSV and JSON format.

Changes in default behavior

Bug ID	Description
537354	Interface egress shaping offload to NPU when `shaping-offload` is enabled.
728234	ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration. Changes: • Firewall policies no longer have the *ZTNA* toggle for switching between *Full ZTNA* and *IP/MAC filtering*. • To perform IP/MAC filtering with ZTNA tags, assign tags under *IP/MAC Based Access Control* in a firewall policy. • ZTNA rules must include a source interface. Upgrading: • If an `access-proxy` type `proxy-policy` does not have a `srcintf`, then after upgrading it will be set to `any`. • All full ZTNA firewall policy will be automatically removed.
729879	When FIPS-CC mode is enabled, `subject-match` can now be configured. The default value is no longer `superset`, so it keeps the current setting.

Changes in default values

Bug ID	Description
729516	Change `ft-over-ds` default setting from enable to disable.
736842	The following default values have changed under `config wireless-controller wids-profile`: • `ap-bgscan-intv` has changed from 1 second to 3 seconds • `ap-bgscan-duration` has changed from 20 milliseconds to 30 milliseconds • `p-bgscan-idle` has changed from 0 milliseconds to 20 milliseconds

Changes in table size

Bug ID	Description
729990	Increase `firewall.address` global table size limit to 500,000 for 3600E models and higher.
733978	Increase per-VDOM table size for DNS server (`system.dns-database`) to 4096 for all models.
736452	Removed global and per VDOM limits to number of monitors.
749024	Increase maximum explicit proxy user limit. The new limits are as follows: • Desktop models = 1,000 • 1U models = 12,000 • 1K models = 32,000 • 2K models = 64,000 • 3K, 4K, and 6K models = 128,000

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description

566452	Support hardware switch on FG-400E and FG-1100E models. The following commands have been removed:
	`config system virtual-switch`
	`edit <name>`
	`config port`
	`edit <name>`
	`set speed <option>`
	`set status {up | down}`
	`next`
	`end`
	`next`
	`end`
	`config system physical-switch`
	`edit <name>`
	`config port`
	`edit <name>`
	`set speed <option>`
	`set status {up | down}`
	`next`
	`end`
	`next`
	`end`

575686	When configuring an SSID in bridge mode, users can select individual security profiles instead of a security profile group. This applies to models in the FAP-U series that can perform UTM on the FortiAP itself.
603012	When defining the FortiPresence server for location based services, allow the server address entry to be configured as an FQDN.

641524	Add interface selection for IPS TLS protocol active probing.
	`config ips global`
	`config tls-active-probe`
	`set interface-selection-method {auto | sdwan | specify}`
	`set interface <interface>`
	`set vdom <VDOM>`
	`set source-ip <IPv4 address>`
	`set source-ip6 <IPv6 address>`
	`end`
	`end`

Bug ID	Description
685663	FortiOS Carrier now has the ability to set up, monitor, and filter messages, as well as manipulate a GTP tunnel on an S10 interface based on mobility management messages defined in 3GPP TS 29.274 section 7.3. It adds the capability for carrier customers to manipulate GTP tunnels and perform message filtering when deployed in inter-LTE/MME handover scenario.
685910	Add SoC4 driver support for the IEEE 802.1ad, which is also known as QinQ. When the OID is used up, it is forbidden to create a new QinQ interface.
687074	Add support for IGMP snooping proxy to be configurable per VLAN. For each VLAN with IGMP snooping proxy enabled, an IGMP snooping querier can also be configured per VLAN for a selected managed switch.
688237	Add support for a FortiGate to manage a Procend 180-T DSL transceiver (FN-TRAN-DSL) that is plugged in to an SFP port. The management of the DSL transceiver includes the ability to program the physical layer attributes on the DSL module, retrieve the status and statistics from the module, support firmware upgrades of the module, and reset the module. Supported VDSL profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a. Supported platforms: FG-80F, FG-81F, FG-80F-BP, FGR-60F, and FGR-60F-3G4G.
690690	The new *Asset Identity Center* page unifies information from detected addresses, devices, and users into a single page, while building a data structure to store the user and device information in the backend. *Asset* view groups information by *Device*, while *Identity* view groups information by *User*. When hovering over a device or a user in the GUI, it is possible to perform different actions relevant to the object, such as adding a firewall device address, adding an IP address, banning the IP, quarantining the host, and more.

695223	Add options to enable caching infected scan results and cleaning scan results in AV stream-based scans to help detect malware in oversized archives when downloads are interrupted. Cached traffic is released after five minutes.
	`config antivirus settings`
	`set cache-infection-result {enable | disable}`
	`set cache-clean-result {enable | disable}`
	`end`

697060	The MTU of an IPv6 tunnel interface will be calculated from the MTU of its parent interface minus headers.

700073	Add a default-action into `youtube-channel-filter` configuration to apply a default action to all channels when there is no match.
	`config videofilter youtube-channel-filter`
	`edit <id>`
	`set default-action {block | monitor | allow}`
	`set log {enable | disable}`
	`next`
	`end`
	The default settings are `monitor` for `default-action`, and `disable` for `log`.

Bug ID	Description
701125	LAN extension is a new configuration mode on the FortiGate that allows FortiExtender to provide remote thin edge connectivity back to the FortiGate over a backhaul connection. A FortiExtender deployed at a remote location will discover the FortiGate access controller (AC) and form an IPsec tunnel (or multiple tunnels when multiple links exists on the FortiExtender) back to the FortiGate. A VXLAN is established over the IPsec tunnels to create an L2 network between the FortiGate and the network behind the remote FortiExtender.
701632	Add `switch-recommendations` command to check the firmware used in the managed switches in order to make a recommendation on which tunnel mode to use: `execute switch-controller switch-recommendations tunnel-mode-settings <FortiLink interface>`
707682	Add support for a FortiGate to manage a Procend 180-T DSL transceiver (FN-TRAN-DSL) that is plugged in to a FortiSwitch port being managed through FortiLink. The management of the DSL transceiver and the FortiSwitch port includes the ability to program the physical layer attributes on the DSL module, retrieve the status and statistics from the module, support firmware upgrades of the module, and reset the module. A FortiSwitch running in standalone mode does not support programmability of the DSL module. Supported platforms: FG-60F and FG-40F-3G4G.
708971	Allow customers to send Fortinet system log entries to external TACACS+ accounting servers. Up to three external TACACS+ servers can be configured, each with different filters for log events. These filters include TACACS+ accounting for login events, configuration change events, and CLI command audits.
710098	Support FQDN address type in ZTNA access proxy real servers configurations.
711577	Add warnings to inform users when an installed firmware is not signed by Fortinet. The warning message appears in the CLI when the uploaded firmware fails signature validation, and when logging in to the FortiGate from the GUI. Additional messages are added in various places once a user is logged in to the GUI to remind them of the unsigned firmware.

711932	IPAM (IP address management) is now available locally on the FortiGate. A standalone FortiGate or a Fabric root in the Security Fabric can act as the IPAM server. Interfaces configured to be auto-managed by IPAM will receive an address from the IPAM server's address/subnet pool. *DHCP Server* is automatically enabled in the GUI, with the address range also populated by IPAM. Users can customize the address pool subnet and the size of a subnet that an interface can request.
	The following setting for FortiIPAM has been moved:
	`config system global`
	`  set fortiipam-integration {enable | disable}`
	`end`
	To:
	`config system ipam`
	`  set status enable`
	`  set server-type cloud`
	`end`

Bug ID	Description
713690	Add user count per LDAP group in an Active Directory. When LDAP users log on through firewall authentication, the active users per LDAP group is counted and displayed in the *Firewall Users* view and in the CLI.

714788	Add HA uninterruptible upgrade option that allows users to configure a timeout value in minutes (1 - 300, 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`

715498	Add option to enable NAT64 and NAT46 for security policy in NGFW policy mode.
717336	The dedicated management CPU feature ensures that CPU 0 is only used for management traffic. This feature, which was previously available for 2U models and higher, is extended to 1U models.
717963	Support subscription-based VDOM licensing for FG-VM S-series using the new stackable subscription-based SKU.
718001	Add support for the recently released Wi-Fi Alliance Hotspot 2.0 Release 3 specifications. The release version can now be configured in the wireless controller hotspot profile.
718071	Support for RFC 7606 extends BGP error handling for malformed attributes in UPDATE messages. Instead of only using the session reset approach from the base BGP specifications, the FortiGate will also use the treat-as-withdraw approach and the attribute discard approach specified in RFC 7606.
718293	The dstuser field added to UTM logs records the username of a destination device when that user has been authenticated on the FortiGate.

718295	Add the ability to specify EU servers as the location to send FortiGuard updates and queries. This option can be toggled from the GUI under *System* > *FortiGuard* > *FortiGuard Updates*, or from the CLI:
	`config system fortiguard`
	`  set update-server-location {automatic | us | eu }`
	`end`

718296	Support configuration save (workspace) mode in the GUI. When in workspace mode, setting changes are saved to the memory and take effect right away as normal. However, setting changes are not saved to the flash until committed. If the device is rebooted, uncommitted configuration changes will be reverted. The *Revert upon timeout* setting can be enabled, which automatically reboots the device after the configured timeout and reverts configuration changes back to the previous save point.
718298	Three new web filter categories have been added to the FortiOS and FortiGuard servers: URL shortening (97), crypto mining (98), and potentially unwanted program (99).
718306	Location based services (LBS) information of associated and unassociated wireless stations can be retrieved through the REST API.

Bug ID	Description
718664	Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant to the ZTNA policy. The FortiGate monitors changes to endpoint tags that are updated by EMS through the fcnacd process. When a change is detected, active ZTNA sessions for the endpoint must match the ZTNA policy again before data can pass.
719764	As of 7.0.1, IPv6 can be configured in ZTNA in the following scenarios: • IPv6 client with IPv6 server • IPv6 client with IPv4 server • IPv4 client with IPv6 server Configuration changes: • Add `access-proxy` type in `config firewall vip6` • Add `config firewall access-proxy6` • Add `config firewall access-proxy(6) > config api-gateway6` • Add `access-proxy6` in `config firewall proxy-policy` As of 7.0.2, IPv6 can be configured in GUI in the *ZTNA Server* settings: • The server IP *Type* can be selected when creating a new server. • When IPv6 is enabled, the ZTNA server table will have multiple sections for IPv4 and IPv6 servers. • Server service mappings can now be selected as either IPv4 or IPv6. • TCP forwarding now contains IPv6 addresses.
719798	GTP sessions state synchronization for FortiOS Carrier is now extended to FGSP over FGCP clusters. This allows session synchronization for FGCP clusters across different sites in the same FGSP peer group, enhancing customer network's local redundancy and geo redundancy.
719799	When specifying ZTNA tags in a ZTNA rule, it is now possible to use the logical AND for tag matching. When *Match ZTNA tags* is configured to *All*, the client must match all the tags. When *Match ZTNA tags* is configured to *Any*, the client can match any of the tags.
720371	New ciphers have been added in FIPS ciphers mode on FortiGate VMs so that cloud instances running this mode can form IPsec tunnels with hardware models running FIPS-CC mode. Added to IPsec phase 1: • aes128-sha256 • aes128-sha384 • aes128-sha512 • aes256-sha256 • aes256-sha384 • aes256-sha512 Added to IPsec phase 2: • aes128-sha256 • aes128-sha384 • aes128-sha512 • aes256-sha256 • aes256-sha384 • aes256-sha512

Bug ID	Description

721828	User fields in logs can be anonymized by generating a hash based on the user name and salt value with the `set anonymization-hash` option.
	`config log setting`
	`  set user-anonymize enable`
	`  set anonymization-hash <string>`
	`end`

722651	Introduce an MSRP (Message Session Relay Protocol) decoder in the IPS engine to scan for IPS signatures against the application data. Malicious payload in the text message can be blocked. Both VoIP and IPS profiles must be configured in the firewall policy, and the inspection mode must be flow.
722849	Increase the number of HA group IDs to 1024, and extend the HA virtual MAC address range to support 1024 groups. Groups 0-255 will use the same VMACs as before, but groups 256-1023 will use VMAC addresses with the prefix e0:23:ff:fc.
724266	The FortiGate LAN extension controller can push out a bandwidth limit to the FortiExtender thin edge. The limit will be enforced on the FortiExtender side using traffic shaping.
725887	Support external browser-based SAML authentication for ZTNA policies. Add SAML redirect option to enable redirection after successful SAML authentication.
726268	Previously, `estimated-downstream-bandwidth` and `ingress-shaping-profile` needed to be configured to use the ingress traffic shaping feature work. Now, `estimated-downstream-bandwidth` changed to `inbandwidth`.
727502	Add WebSocket enhancements to allow users to subscribe to and listen to configuration table changes from the GUI. New alerts are added to notify users to reload the page when configuration changes occur on the page.
727512	When querying a FortiExtender or LTE-modem through the FortiGate REST API, GPS coordinates are now included in the response.
727947	Add `action-type cli-script` attribute to `config system automation-action` for CLI scripts to execute on all FortiGates in the Security Fabric.

728528	Add option to perform server identity check for FSSO SSL/TLS connection. The server FQDN or IP must match the SAN field in the collector agent certificate. If no SAN field is present, the IP must match the IP in the certificate's CN field.
	`config user fsso`
	`  edit <FSSO server>`
	`  set server <FQDN or valid IP>`
	`  set ssl-server-host-ip-check {enable | disable}`
	`  next`
	`end`

729664	Add commands to lock down ISL/ICL links between FortiSwitches so that they become static configurations: • `execute switch-controller switch-recommendations fabric-lockdown-check`

Bug ID	Description
	• `execute switch-controller switch-recommendations fabric-lockdown-disable` • `execute switch-controller switch-recommendations fabric-lockdown-enable` This adds stability during events such as cable disconnection or power outages.
731720	Add wireless controller syslog profile that enables APs to send logs to the syslog server configured in the profile.

732325	Extend passive health measurement to support passive detection per internet service/application. If internet services/applications are defined in an SD-WAN rule with a passive health check, the SLA information per internet service/application will be differentiated and collected. Then, the SLA metrics (latency, jitter, and packet loss) on each SD-WAN member in this rule will be calculated based on relevant internet services/applications SLA information.
	`config system sdwan`
	`  config service`
	`  edit <id>`
	`  set passive-measurement {enable | disable}`
	`  next`
	`  end`
	`end`
	This feature is disabled by default.

733597	Add the ability to authenticate wireless clients using MAC authentication and MPSK against a RADIUS server. Instead of statically storing the MPSK passphrases on the FortiGate, they can be passed from the RADIUS server dynamically when the client MAC is authenticated by the RADIUS server. The result passphrase will be cached on the FortiGate for future authentication, with a timeout configured per VAP.
	`config wireless-controller vap`
	`  edit <name>`
	`  set radius-mac-auth enable`
	`  set radius-mac-auth-server <server>`
	`  set mpsk-profile <profile>`
	`  set radius-mac-mpsk-auth enable`
	`  set radius-mac-mpsk-timeout <integer>`
	`  next`
	`end`

733970	Adaptive Forward Error Check (FEC) improves upon the previous FEC mechanism in many ways. While the previous FEC mechanism always sends out x number of redundant packets for every y number of base packets, adaptive FEC takes link conditions into consideration and adaptively adjusts the FEC packet ratio. FEC can be configured to apply to only certain streams that are sensitive to packet loss to reduce unnecessary bandwidth. Since FEC does not support NPU offloading, being able to specify streams and policies that do not require FEC allows that traffic to be offloaded.

Bug ID	Description
733976	ECDSA (Elliptic Curve Digital Signature Algorithm) is now supported in SSH administrative access. Administrative users can connect using an ECDSA key pair or ECDSA based-certificate.
735938	On the NAC Policy configuration page, specifying FortiSwitch groups is now supported. Previously, individual FortiSwitches had to be specified. The CLI command to specify individual switches is now updated to specify switch groups.
736574	In some unlikely scenarios where a FortiSwitch needs to upgrade its BIOS before the firmware upgrade, a new command has been added to perform a BIOS compatibility check on the FortiGate switch controller.
738759	Add DNS dashboard widget that shows latency to configured and dynamically retrieved DNS servers.
738904	When the FortiGate LAN extension controller is behind a NAT device, remote thin edge FortiExtenders must connect to the FortiGate via a backhaul address. This is an address on the upstream NAT device that forwards traffic to the FortiGate. It can be configured as an IP or FQDN on the FortiGate extender profile. When the default IKE port 500 is not accessible, it is possible to configure a custom IKE port on the FortiExtender and FortiGate.
739442	Add REST APIs to close multiple IPv4 or IPv6 sessions at once (previously, only a single session could be closed each time): • `POST https://<FortiGate IP>/api/v2/monitor/firewall/session/close-multiple` • `POST https://<FortiGate IP>/api/v2/monitor/firewall/session6/close-multiple` • `POST https://<FortiGate IP>/api/v2/monitor/firewall/session6/close-all`
740204	Supply better heartbeat timing information to the auto-scale callback URL. Previously, the auto-scale heartbeat request made to the auto-scale callback URL did not contain a timestamp or sequence number. This information was estimated in the cloud function called by the callback URL, but the cloud function platform's timing was not as reliable as initially expected.
740468	Configuring SAML single sign-on configurations can now be done from the GUI under *User & Authentication* > *User Groups*. The new GUI wizard helps generate the SP URLs based on the supplied SP address. The created SAML object can also be selected when defining a new user group.
742411	Support configuring 802.11ax specified VAP data rates from the FortiGate wireless controller in order to cover 802.11ax data rates and modulation schemes that 802.11ac does not support.

742424	It is now possible to configure auto-BSS coloring from the FortiGate wireless controller so that the FortiAP radios to automatically change colors when BSS coloring conflicts are detected. The new setting is set to `auto` by default.
	`config wireless-controller wtp-profile`
	`edit <profile>`
	`config <radio>`
	`set bss-color-mode {auto | static}`
	`end`

Bug ID	Description
	`    next` `end`

742855	Allow administrators to select which ciphers to use for TLS 1.3 in HTTPS connections, and which ciphers to ban for TLS 1.2 and below.
	`config system global`
	`    set admin-https-ssl-ciphersuites {<option1>}, [<option2]>, ...`
	`    set admin-https-ssl-banned-ciphers {<option1>}, [<option2>], ...`
	`end`

743835	Add fields in the custom OVF template for *License Token* and *Configuration URL* to allow users to input a Flex VM token code and a web URL where a bootstrap configuration for the FortiGate is stored.
749336	The FortiGate external threat feeds now support feeds that are in STIX/TAXII format. To point to a feed that is in STIX format, use the `stix://` prefix in the URI to denote the protocol.

752558	Support logging for FortiGate generated local out DNS traffic. A new setting is added for the local DNS log:
	`config system dns`
	`    set log {disable | error | all}`
	`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 7.0.2 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.2
FortiManager	• 7.0.2
FortiClient Microsoft Windows	• 7.0.0 build 0029 or later
FortiClient Mac OS X	• 7.0.0 build 0022 or later
FortiClient Linux	• 7.0.0 build 0018 or later
FortiClient iOS	• 6.4.6 build 0507 or later
FortiClient Android	• 6.4.6 build 0539 or later
FortiClient EMS	• 7.0.0 build 0042 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 26
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiSandbox	• 2.3.3 and later, 4.0.0 is recommended

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

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.2. When Security Fabric is enabled in FortiOS 7.0.2, all FortiGate devices must be running FortiOS 7.0.2.

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

IPsec interface MTU value

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

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

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

HA role wording changes

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

Strong cryptographic 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) will support strong ciphers in the future release of version 5.4.3.

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
```

How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1

To make L2TP over IPsec work after upgrading:

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
    set eip 210.0.0.254
    set sip 210.0.0.1
    set status enable
    set usrgrp "L2tpusergroup"
end
```

   Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "l2tp.root"
    next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`
- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects* > *NAT46 Policy*
- *Policy & Objects* > *NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects* > *Virtual IPs* related pages

Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.
- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip`/`vip6` and `ippool`/`ippool6`.

Example configurations

`vip46` object:

Old configuration	New configuration

`config firewall vip46`
`edit "test-vip46-1"`
`set extip 10.1.100.155`
`set mappedip 2000:172:16:200::55`
`next`
`end`
	`config firewall vip`
	`edit "test-vip46-1"`
	`set extip 10.1.100.150`
	`set nat44 disable`
	`set nat46 enable`
	`set extintf "port24"`
	`set ipv6-mappedip 2000:172:16:200::55`
	`next`
	`end`

`ippool6` object:

Old configuration	New configuration
config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end	config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 **set nat46 enable** next end

NAT46 policy:

Old configuration	New configuration
config firewall policy46 edit 1 set srcintf "port24" set dstintf "port17" set srcaddr "all" set dstaddr "test-vip46-1" set action accept set schedule "always" set service "ALL" set logtraffic enable set ippool enable set poolname "test-ippool6-1" next end	config firewall policy edit 2 set srcintf "port24" set dstintf "port17" set action accept **set nat46 enable** set srcaddr "all" set dstaddr "test-vip46-1" set srcaddr6 "all" set dstaddr6 "all" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname6 "test-ippool6-1" next end

`vip64` object

Old configuration	New configuration
config firewall vip64 edit "test-vip64-1" set extip 2000:10:1:100::155 set mappedip 172.16.200.155 next end	config firewall vip6 edit "test-vip64-1" set extip 2000:10:1:100::155 set nat66 disable **set nat64 enable** **set ipv4-mappedip 172.16.200.155** next end

`ippool` object

Old configuration	New configuration
config firewall ippool edit "test-ippool4-1"	config firewall ippool edit "test-ippool4-1"

Old configuration	New configuration

`set startip 172.16.201.155`
`set endip 172.16.201.155`
`next`
`end`
	`set startip 172.16.201.155`
	`set endip 172.16.201.155`
	`set nat64 enable`
	`next`
	`end`

NAT64 policy:

Old configuration	New configuration

`config firewall policy64`
`edit 1`
`set srcintf "wan2"`
`set dstintf "wan1"`
`set srcaddr "all"`
`set dstaddr "test-vip64-1"`
`set action accept`
`set schedule "always"`
`set service "ALL"`
`set ippool enable`
`set poolname "test-ippool4-1"`
`next`
`end`
	`config firewall policy`
	`edit 1`
	`set srcintf "port24"`
	`set dstintf "port17"`
	`set action accept`
	`set nat64 enable`
	`set srcaddr "all"`
	`set dstaddr "all"`
	`set srcaddr6 "all"`
	`set dstaddr6 "test-vip64-1"`
	`set schedule "always"`
	`set service "ALL"`
	`set logtraffic all`
	`set ippool enable`
	`set poolname "test-ippool4-1"`
	`next`
	`end`

Product integration and support

The following table lists FortiOS 7.0.2 product integration and support information:

Web browsers	• Microsoft Edge 94 • Mozilla Firefox version 93 • Google Chrome version 94 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 0302 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

FortiExtender	• 3.2.1
AV Engine	• 6.00266
IPS Engine	• 7.00043

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 89 Google Chrome version 91
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 92 Google Chrome version 93
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 92 Google Chrome version 93
macOS Big Sur 11.2	Apple Safari version 14 Mozilla Firefox version 92 Google Chrome version 93
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 7.0.2. For inquires about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
743693	Anti spam engine crashes when extracting a malformed IP address from Received: headers.

Anti Virus

Bug ID	Description
665173	Crash logs are sometimes truncated/incomplete.
702646	Re-enable JavaScript heuristic detection and fix detection blocking content despite low rating.
724588	Flow AV quarantines a source IP when an AV scan error occurs.

Application Control

Bug ID	Description
701926	Stress test with application control only results in packet drops.

Data Leak Prevention

Bug ID	Description
745369	PDF corruption over HTTP by DLP.

DNS Filter

Bug ID	Description
722510	Rating requests to anycast SDNS server does not work as expected in SD-WAN.
724657	Anycast SDNS server IP is not added to non-index 0 DNS proxy workers.

Explicit Proxy

Bug ID	Description
674996	WAD encounters segmentation crash at `wad_ssl_arm_close`; crash occurred on explicit web proxy.
720363	When the client in web proxy mode uses the same session to send the HTTP requests with different host names, the HTTP host load balancing method does not take effect.
721039	Short disconnections of streaming applications (Teams and Whereby) through explicit proxy.
733863	Get 504 gateway timeout error when trying to access proxy.pac from remote users using dialup IPsec VPN.

Firewall

Bug ID	Description
644225	Challenge ACK is being dropped.
726040	If a SYN has a different ISN in the SYN_SEND/SYN_RECV state, the FortiGate will let the SYN pass without updating the TCP sequence number, but drops the reply SYN/ACK because it fails the sequence number check.
727809	Disabled deny firewall policy with virtual server objects is unable to be enabled after firewall reboot.
729245	HTTP/1.0 health check should process the whole response when `http-match` is set.
730803	Applying a traffic shaping profile and outbound bandwidth above 200000 blocks the traffic.
735031	IPv6 policy is only allowing the first MAC address from the source list.
736452	Unable to configure more than five health checks within virtual servers because of limitation of `firewall.vip:monitor`.
738584	Firewall is using the wrong NAT IP address to send out traffic after removing the VIP and its associated policy.

Bug ID	Description
741122	If a DCE/RPC packet has more than six string binding addresses, the expectation for the rest of the addresses will not be created, and the traffic will be denied.
743800	SNAT hairpin traffic NATs to the incorrect IP address when central NAT is enabled without a central NAT rule.
745853	FortiGate stops sending logs to Netflow traffic because the Netflow session cleanup routine runs for too long when there are many long live sessions in the cache.
748226	In `diagnose netlink interface list wan1`, the total bytes for the inbandwidth shaper is always `0`.

GUI

Bug ID	Description
608770	When there is no IP/IPv6 address setting for *Zone*, the GUI incorrectly displays *0.0.0.0/0.0.0.0* for *IP/Netmask* and *::/0* for *IPv6 Address*.
631201	When editing an SSL/SSH inspection profile, the *Show in Address List* toggle in *Edit Wildcard FQDN Address* does not work when creating a new wildcard FQDN address.
653952	*The web page cannot be found* is displayed when a dashboard ID no longer exists.
677611	On the *Network* > *SD-WAN* > *SD-WAN Rules* tab, an SD-WAN member with link status down is displayed as selected.
681643	On the *Network* > *Packet Capture* page, the interface dropdown incorrectly lists interfaces that belong to a virtual wire pair.
686500	Unable to specify a custom hostname during FortiGate setup.
689661	On the *Policy & Objects* > *Firewall Policy* page, policies that have enabled `internet-service-src-custom` and/or have specified an `internet-service-src-custom-group` are not listed in the policy list.
699508	When an administrator ends a session by closing the browser, the administrator timeout event is not logged until the next time the administrator logs in.
714304	Special characters `<`, `>`, `(`, `)`, `#`, `'`, and `"` are allowed in the name when set from the CLI. When set from the GUI they are flagged as invalid.
714716	*IPsec Monitor* shows the same usernames and IPSec tunnel names for different users when the peer ID is configured on the FortiGate and/or FortiClient.
716571	Missing inter-chassis link (ICL) between FortiSwitches in the same tier of a topology.
720613	The event log sometimes contains duplicated lines when downloaded from the GUI.
720657	Unable to reuse link local or multicast IPv6 addresses for multiple interfaces from the GUI.

Bug ID	Description
721710	Data fails to load when the Security Fabric is enabled for a downstream FortiGate that has an upstream PPPoE interface to connect to the root.
722133	On the *Policy & Objects* > *Central SNAT* page, one-to-one IP pools do not appear in the NAT policy.
722450	The rating rule *Disable Username Sensitivity Check* incorrectly fails for remote LDAP users with two-factor authentication disabled.
722669	On the *Network* > *Interfaces* page, the DHCP range is incorrectly displayed when *DHCP Server* (status) is disabled.
722832	When LDAP server settings involve FQDN, LDAPS, and an enabled server identity check, the following LDAP related GUI items do not work: LDAP setting dialog, LDAP credentials test, and LDAP browser.
723988	On the *WiFi & Switch Controller* > *FortiSwitch Ports* page, the *PoE* option is grayed out so is cannot be configured. The CLI must be used.
727035	Unable to change FortiSwitch port status when native VLAN is empty.
727644	When the first row of sequence group in a policy table is deleted, the sequence group disappears.
728651	When populating the BGP global table from the GUI (*Network* > *BGP*), BGPD process memory increases until it exhausts memory and goes into conserve mode.
728742	Unable to reorder *Favorites* after upgrading to FortiOS 7.0.
729075	Tooltip for FortiView *Comprised Host* fails with a JavaScript error.
729675	*System* > *Settings* page does not load for a FortiGate in carrier mode with an administrator profile that has `custom` firewall settings.
730069	On the *Network* > *Static Routes* page, users are unable to create a static route with *Automatic gateway retrieval* enabled when a DHCP interface is specified.
730211	Interface widget does not show data when the browser time differs from FortiGate UTC time.
732618	On the *Network* > *Interfaces* page, when *Dedicated Management Port* is enabled on an interface and the *Trusted Host 1* IP address is set to *0.0.0.0/0*, settings cannot be saved.
733375	On the *VPN* > *SSL-VPN Settings* page, after clicking *Apply*, `source-address` objects become `source-address6` objects if IPv6 is enabled.
733582	The *IP/Mac Based Access Control* radio button is no longer present in the *Firewall Policy* dialog from implicit policy projects.
734417	When upgrading firmware from 7.0.0 to 7.0.1, GUI incorrectly displays a warning saying this is not a valid upgrade path.
734773	On the *System* > *HA* page, the HA primary device status differs from what is displayed in the CLI (`get system ha status`) when virtual cluster is enabled and the management VDOM is not the root VDOM.
735114	In *FortiView Sources*, on a multi-VDOM FortiGate, if there is no cache for IOC (compromised hosts), a request to filter by IOC is sent to all VDOMs on the FortiGate, not just the current VDOM.

Bug ID	Description
739543	On the *Network* > *Interfaces* page, unable to create or edit a VLAN switch as the VLAN ID validation incorrectly fails.
742561	After upgrading to FortiOS 6.4.7, a previously valid VLAN switch VLAN ID of 0 now displays the error message, *The minimum value is 2*. This issue is not present when upgrading to 7.0.1 and later.
743477	On the *Log & Report* > *Forward Traffic* page, filtering by *Source* or by *Destination* does not work when the *NOT* option is included in the filter.
743743	httpsd crashes due to `GET /api/v2/log/.../virus/archive` request when the `mkey` is not provided.
744168	On the *Security Profiles* > *SSL/SSH Inspection* page, a new SSL/SSH inspection profile cannot be created when the *Inspection method* is *SSL Certificate Inspection*.
744860	On the *System* > *Settings* page, when the time zone is set to (GMT-6:00) Central America, the current system time is off by one hour during Daylight Saving Time (DST).
745325	When creating a new (public or private) SDN connector, users are unable to specify an *Update interval* that contains *60*, as it will automatically switch to *Use Default*.
745998	Unable to delete IPsec phase 1 interface if the name contains a `/`.
746012	FortiGate Cloud IOC (*Compromised hosts*) is unable to generate IOC events on the FortiGate.

HA

Bug ID	Description
694984	Session count of UDP traffic gradually decreases on the secondary unit in a FGSP-TP cluster.
695067	When there are more than two members in a HA cluster and the HA interface is used for the heartbeat interface, some RX packet drops are observed on the HA interface. However, no apparent impact is observed on the cluster operation.
705237	Remote two-factor authentication is not working for HA secondary management interface.
709963	When cluster members have a different size log disk configurations in the cluster system, failure occurs when users input a size higher than the default value on the primary device.
714788	Uninterruptible upgrade might be broken in large scale environments.
717788	FGSP has problem at failover when NTurbo or offloading is enabled (IPv4) with virtual wire pair traffic.
721929	In an HA A-P scenario during failover, the new passive WCCP router ends up choosing a change number during the regular WCCP configuration initiation that will not trigger an assignment, which causes the WCCP assignment to be lost.
723130	`diagnose sys ha reset-uptime` on the secondary devices triggers a failover on a cluster with more than two members.

Bug ID	Description
725240	HA cluster goes out of sync due to mismatched `vpn.certificate.crl` checksum.
728670	In FGSP HA mode, the synchronizing mechanism of VWL daemon causes a synchronization message that goes back and forth infinitely, which causes the CPU and memory usage to keep increasing.
729590	DDNS registration fails on vcluster2 VDOMs.
729607	FTP transfers drop in active-active mode in cases where expectation sessions accumulated in the secondary unit reach the maximum number (128).
734138	HA standby management IP does not reply to ping if the `link-failed-signal` option is enabled and when the monitor interface is down.
738350	In some cases, the hasync process has high memory on HA secondary device.
744826	API key (token) on the secondary device is not synchronized to the primary when `standalone-config-sync` is enabled.
746008	DNS may not resolve on the correct blade in a 6K/7K virtual cluster environment.

Intrusion Prevention

Bug ID	Description
669089	IPS profile dialog in GUI shows misleading *All Attributes* in the *Details* field for filter entries with a CVE value.
693800	IPS memory spike on firmware running version: 5.00229.
698725	Custom IPS signature with deprecated options is causing a delay for the unit to boot up.
699775	Fortinet logo is missing on web filter block page in Chrome.
713508	Low download performance occurs when SSL deep Inspection is enabled on aggregate and VLAN interfaces when nTurbo is enabled.
746467	IPS engine crashes when IPS injects packets to vNP and vNP/DPDK fails to restart (crashes and sometimes is out of service).

IPsec VPN

Bug ID	Description
668997	*Duplicate entry found* error shown when assigning multiple dialup IPsec tunnels with the same secondary IP in the GUI.

Bug ID	Description
685668	Modify IKE to check `config firewall security-policy` for the user or group entry instead of checking `config firewall policy` if it is in NGFW mode.
707547	RADIUS accounting messages (IKEv2 EAP authentication) does not include the Class attribute (group name).
722564	Missing peer ID in IKEv2 and IKEv1 main mode.
726362	It is possible to add multiple domains, even though that functionality is currently not supported.
726450	Local out dialup IPsec traffic does not match policy-based routes.
729012	The NAT-T keep alive messages are being logged incorrectly, causing the FortiGate to generate a huge number of logs.
729760	The ADVPN forwarder does not currently track the shortcut query that it forwards. Shortcut queries and replies are forwarded or terminated solely based on the route lookup.
729879	Static IPsec tunnel with signature authentication method cannot be established on FIPS-CC mode FortiGate because the certificate subject verification changes to RDN bitwise comparison based.
730449	SD-WAN service traffic will be interrupted after upgrading to 7.0.1 if all of the following conditions are matched in its 6.4.x configuration: • Using `set gateway enable` in a particular SD-WAN service • Having `mode-cfg` configured • Not having ADVPN configured on the hub
735430	TCP SYN-ACKs are silently dropped if the traffic is sourced from a dialup IPsec tunnel and UTM is enabled.
735477	IKEv1 aggressive mode may crash if the initiator received its own message as the first response.
743732	If a failure happens during negotiating a shortcut IPsec tunnel, the original tunnel NAT-T setting is reset by mistake.

Log & Report

Bug ID	Description
718140	Logs are missing on FortiGateCloud from a certain point.
724827	Syslogd is using the wrong source IP when configured with `interface-select-method auto`.
726690	Forward traffic log from disk is missing for virtual wire pair policy.
731154	SSL VPN tunnel down event log (log ID 39948) is missing.
745310	A corner case might lead to queued logs getting stuck in the queue and not being sent.

Proxy

Bug ID	Description
520176	Multiple WAD crashes observed with signal 6. The issue could be reproduced with a slow server that will not respond the connection in 10 seconds, and if the configuration changes during the 10 seconds.
582464	WAD SSL crash due to wrong cipher options chosen.
604373	When proxy-based deep inspection is enabled, a server requests a certificate from the client over TLS 1.2 and the client returns an ECDSA certificate. In a best case scenario, the handshake will fail. In a worst case scenario, WAD will crash.
663088	Application control in Azure fails to detect and block SSH traffic with proxy inspection.
688792	WAD crashes at `wad_http_req_exec_video_filter_check` with signal 11.
696012	Video filter cannot block embedded video calling by channel or category.
700073, 714109	YouTube server added new URLs (`youtubei/v1/player, youtubei/v1/navigator`) that caused proxy option to restrict YouTube access to not work.
706786	Multiple SSL connections without policies are being matched with multiple configuration changes for certificate updates, which may trigger a WAD crash.
715280	When the user/interface count reaches the respective maximum, the operation of reducing this count could impact the CPU and cause WAD to crash.
717995	Proxy mode generates untagged traffic in a virtual wire pair.
719681	Flow control failure occurred while transferring large files when `stream-scan` was running, which sometimes resulted in WAD memory spike.
724129	WebSocket connection is not successful when IPS and application control are enabled in a proxy inspection policy.
724670	Crash seen in WAD user information daemon when updating user group count upon user log off.
725628	WAD HTTP parser string leak for hostname and scheme with `trace-auth-no-rsp` enabled.
726270	In deep scan mode when there is no SNI, WAD will use the server certificate CNAME for the URL filter check and ignores the host header.
726999	WAD crash on `wad_hash_map_del`.
728641	SSL renegotiation fails when Firefox offers TLS 1.3, but the server decides to use TLS 1.2.
733760	Proxy inspection firewall policy with proxy AV blocks POP3 traffic of the Windows 10 built-in Mail app.
737438	ZTNA HTTPS access proxy traffic is denied when a regular VIP and access proxy VIP (AP VIP) have the same external IP address.
737737	WAD crashes when firewall FQDN address is null.

Bug ID	Description
738331	Excluded members in the address group are not excluded when the group is added to a proxy policy.
744746	When a policy has both IPS and AV features enabled, WAD has a memory spike when downloading large files.
744756	Web proxy forward server group could not recover sometimes if the FQDN is not resolved.
744882	When using STARTTLS, proxyd performs deep inspection even when `inspect-all` is not set to `deep-inspection`.
748194	Oversize log is not generated for a large EXE file when the `uncompressed-oversize-limit` option is set to `0`.

REST API

Bug ID	Description
731136	The following API has a change in response format, which may break backward compatibility for existing integration: `POST /api/v2/monitor/system/config/restore` New format results: `{'config_restored': True}` Old format results: `{'restore_started': True, 'session_id': 'nTuRkV'}` Note that only the response format is changed. The actual configuration restoration operation still works as before. The integration application should handle this new response format so it can return correct response message back to the user.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
724574, 731248	BFD neighborship is lost between hub and spoke. One side shows BFD as down, and other side does not show the neighbor in the list.
725322	Improve the distance help text to indicate that 255 means unreachable.
729002	PIM/PIM6 does not send out unicast packet with the correct source IP if interface is not specified.
729621	High CPU on hub BGPD due to hub FortiGate being unable to maintain BGP connections with more than 1K branches when `route-reflector` is enabled.
730194	When syncing a large number of service qualities, there is a chance of accessing out-of-boundary memory, which causes the VWL daemon to crash.

Bug ID	Description
730208	Traffic is not going through when the returning interface is changed.
731683	SD-WAN did not check and properly handle cases of address groups with exclusion.
733187	FortiGate to FortiManager connection issue when using a loopback interface with a non-default VRF as the source for central management.
734628	SDNS traffic to the anycast IP servers does not follow the SD-WAN mode set in `config system fortiguard`.
736705	ZEBOS launcher is unable to start and crashes constantly if `aspath` has more than 80 characters in the `config router router-map > set-aspath` setting.
737898	OSPFv3 cannot install IPv6 ECMP routes when both ABR next hops are in the same subnet.
740377	HTTP probe response sends reset packets when the number of probes increases.
741844	IPsec VPN does not come up due to incorrectly routed IKE packets.
741947	SD-WAN routes are not installed in the kernel or FIB.
742648	Health check over shortcut tunnel is dead after `auto-discovery-receiver` is disabled/enabled and VWL crash occurs.
743138	OSPF does not use the correct netmask length after upgrading to 7.0.1 when sending a hello packet on an IPsec interface.
743675	RIPv2 multiple routing entries are not reflected when receiving RIP updates via 802.3ad aggregate interface.
746000	Multicast streams sourced on SSL VPN client are not registered in PIM-SM.

Security Fabric

Bug ID	Description
635183	ACI dynamic address cannot be retrieved in HA vcluster2 from SDN connector.
670451	ACI SDN connector (connected by `aci-direct`) shows `curl` error 7 when updating from second VDOM.
695424	SDN connector for GCP ignores project settings.
717080	csfd shows high memory usage due to the JSON object not being used properly and the reference not being released properly.
724071	Log disk usage from user information history daemon is high and can restrict the use for general logging purposes.
726831	Security rating for *Local Log Disk Not Full* reporting as failed for FortiGate models without log disks.
731292	Dashboard *Security Fabric* widget takes a long time to load in the GUI.

Bug ID	Description
731314	Security rating fails and displays *Duplicate Firewall Objects* message for FTP, FTP_GET, and FTP_PUT service objects.
732268	Dynamic address configured with SDN connector for VMware is collecting less IP addresses than expected.
733511	Automation stitch trigger count does not update when target device is a downstream device.
735717	vmwd gives an error when folders are created in the vSphere web interface, and vmwd ignores the IP addresses from vApp.
738344	When CSF root synchronizes a large automation setting (over 16000) to the downstream FortiGate, csfd crashes while trying to process the relay message.
740673	OCI Fabric connector has DNS failure in UK government region.
741346	The variable `%%date%%` resolves into `1900-01-00` instead of actual date when the schedule trigger type is used.
742603	Security rating fails due to duplicate address objects, even when no duplicate address objects exist.
742743	Security rating Issue with unused deny policies.
745263	*AV & IPS DB Update* automation trigger is not working when clicking *Update Licenses & Definitions Now* in the GUI.
746950	When an Azure network interface ID contains upper case letters, the Azure SDN connector may not retrieve that network interface.

SSL VPN

Bug ID	Description
586035	The policy `script-src 'self'` will block the SSL VPN proxy URL.
640169	When the FortiGate is set as the DUT monitored by another FortiGate , the SSL VPN has a memory leak because it continues to receive HTTP requests and creates an HTTP state and tasks to process the request.
664276	SSL VPN host check validation not working for SAML user.
677031	SSL VPN web mode does not rewrite playback URLs on the internal FileMaker WebDirect portal.
706646	SolarWinds Orion NPM platform's web application has issues in SSL VPN web mode.
710657	The `dstaddr`/`dstaddr6` of an SSL VPN policy can be set to `all` when split tunnel mode is enabled and only the default portal is set.
711503	SSL VPN web mode access to internal web server http://10.2.1.78 is broken after upgrading to 7.0.0.
711974	SSL VPN bookmarks are not working correctly with multiple SD-WAN zones.

Bug ID	Description
714155	SSL VPN bookmarks are not working correctly with customer internal website, https://it***.nt***.lo***.
716289	Navigation menu of the internal web server, https://lm***.lm***.au***.vw***, is having issues in the SSL VPN web portal.
718133	In some conditions, the web mode JavaScript parser will encounter an infinite loop that will cause SSL VPN crashes.
718142	The map integrated in the public site is not visible when using SSL VPN web mode.
718165	SSL VPN web mode redirection issue with http://10.3.24.14.
718817	Customer internal website, http://192.168.*.28/mo***/index.php, cannot be shown SSL VPN web mode due to proxy error.
722329	After SSL VPN proxy rewrite, some Nuage JS files have problems running.
725986	SSL VPN web mode does not work as expected when accessing http://ot***.de***.sp***.go***.
726338	The wildcard matching method does not always work as expected because the kernel sometimes does not have the address yet.
726624	Jira web application (to***.cs***.tc***.co**) via SSL VPN web mode does not display website correctly.
727286	Unable to browse directories hosted on Nextcloud server through SSL VPN.
729426	The wildcard FQDN does not always work reliably in cases where the kernel does not have the address yet.
729700	An internal website (https://cm***.va***.it***/cm***) does not load properly when connecting via SSL VPN web mode.
729889	NexGEN server could not be displayed in SS LVPN web mode.
730416	Forward traffic log does not generate logs for HTTP and HTTPS services with SSL VPN web mode.
731278	Customer internal website (ac***.sa***.com) does not load properly when connecting via SSL VPN web mode.
731606	Internal server (sa***.be***.com) is not loading after logging in with SSL VPN web mode.
732943	If the client certificate is only set in a specific authentication rule of the SSL VPN, the peer user may not log in successfully.
736436	Internal website (https://gg****.gl***.com/) shows a blank page in SSL VPN web mode.
736822	Non-US keyboard layout in RDP session with SSL VPN web mode does not work correctly.
737150	Internal website (oh***.com) could not be displayed in SSL VPN web mode.
737154	Slow RDP response when using SSL VPN web mode access.
737341	Some links and buttons are not working properly when accessing them through SSL VPN web mode.

Bug ID	Description
737751	HTML5 page is not fully loading for SSL VPN web mode users.
738711	FortiClient error message is not pertinent when the client does not meet host checking requirements.
738715	Contents of Jira application (in***.ds***.com) in SSL VPN web mode are not displayed correctly.
738723	Video streaming does not work in SSL VPN web mode on https://te***.fortiddns.com:10443.
739711	SSL VPN bookmark button for Jira (sa***.con***.com) malfunctions.
740335	Internal website, https://te***.ko***.com, is not accessible in SSL VPN web mode.
740378	Windows FortiClient 7.0.1 cannot work with FortiOS 7.0.1 over SSL VPN when the tunnel IP is in the same subnet as one of the outgoing interfaces and NAT is not enabled.
741453	Unable to log in to VMware vSphere vCenter 7.0 through SSL VPN web portal.
742332	SSL VPN web portal redirect fails in http://qu***.jj***.bu***.
744494	Memory occupied by the SSLVPN daemon increase significantly while the process is busy.
744899	SSL VPN RDP bookmark is not working when using Chrome 93 32-bit. Firefox 64-bit and Chrome 64-bit are still not supported on Windows 32-bit.
745499	In case where a user is establishing two tunnel connections, there is a chance that the second session knocks out the first session before it is updated, which causes a session leak.
746938	Unable to authenticate to outlook.com/owa/vw***.com website in SSL VPN web mode.
746990	RADIUS accounting messages after SSL VPN do not include the Class attribute (Group name).
747352	Internal web server page, https://te***.ss***.es:10443, is not loading properly in SSL VPN web mode.
747851	SSL VPN bookmark works on one URI (cu***.co***.cr***) and is not working on different URIs to the same destination server.
749918	Keyboard keys do not work with RDP bookmarks when PT-BR and PT-BR-ABNT2 layouts are chosen.

Switch Controller

Bug ID	Description
723501	When STP is enabled on a hardware switch interface, FortiLink loses its connection to FortiSwitch.

System

Bug ID	Description
488400	FGFM sessions time out when the session between two EMAC VLANs with no VLAN IDs are offloaded.
619839	In FIPS-CC mode, keep getting `fcron_set_mgmt_vdom()-122: Invalid mgmt- vfid=-1` message on console.
644616	NP6 does not update session timers for traffic IPsec tunnel if established over one pure EMAC VLAN interface.
645848	FortiOS is providing self-signed CA certificate intermittently with flow-based SSL certificate inspection.
671824	On FG-40F, get `NP6XLITE: failed to read lif accounting` message on console.
681791	Install preview does not show all changes performed on the FortiGate.
684563	Uploading a wrong script in the GUI can cause a continuous error.
696852	Failure to synchronize with FortiGate NTP server, even if the FortiGate NTP server is not properly synchronized with its higher tier NTP server.
698003	When creating a new administrator, the administrator profile's reference is visible in other administrator accounts from different VDOMs.
698590	The `dhcp6-client-options`" is missing on internal interfaces for IPv6.
700664	When the SD-WAN interface select method is configured in `system dns`, the rules are not applied to AXFR DNS database local out traffic.
702966	There was a memory leak in the administrator login debug that caused the getty daemon to be killed.
706686	LAG interface between FortiGate and Cisco switch flaps when adding/removing member interface.
710635	GUI should hide the *FortiGate Setup* dialog if all setup steps are complete.
712156	Remote access management from FortiCloud log in fails if trusted hosts are configured for the administrator account.
713835	The BLE pin hole behavior should not be applied on FG-100F generation 1 that has no BLE built in.
715647	In VWP with `set wildcard-vlan enable`, for some special cases the SKB `headlen` is not long enough for handling. It may cause a protective crash when doing `skb_pull`.
715978	NTurbo does not work with EMAC VLAN interface.
720858	DDNS update interval is abnormal on FG-140E-POE.
721487	FortiGate often enters conserve mode due to high memory usage by httpsd process.
722248	When `lag-out-port-select` is enabled, FortiCarrier ESP packets drops in NPU link.
722273	SA is freed while its timer is still pending, which leads to a kernel crash.

Bug ID	Description
722547	Fragmented SKB size occurs if the tail room is too small to carry the NTurbo `vtag`, which causes packets to be dropped.
724065	`Power supply 2 DC is lost` log only appears when unplugging the power cable from power supply 2.
724446	High CPU for cmdbsvr when editing an address group.
724779	HPE setting of NTurbo host queue is missing and causes IPS traffic to stop when HPE is enabled.
725264	FG-600E copper speed LED does not work.
726634	NTP daemon is not responding when using the manual setting.
727343	Quarantined IP is not synchronized in FortiController mode.
727829	DNS FQDN was not synchronized amongst all the working blade, so each blade might have different IP from the same FQDN. If policy a uses the FQDN as the address, it will cause the IP address of FQDN to not be in the list for the current blade, so the traffic will not match this FQDN policy.
728647	DHCP discovery dropped on virtual wire pair when UTM is enabled.
729636	FTLC1122RDNL transceiver is showing as not certified by Fortinet on FG-3800D.
729939	Multiple processes crashing at the same time causes the device's management functionality to be unavailable when the packet size is smaller than `FSAE_HEADER_SIZE(6).`
731708	The FG-traffic VDOM is lost after restoring the configuration if split-VDOM mode is set in the configuration file.
731789	Unable to set VDOM ID as filter in CLI for `diagnose debug flow`.
731821	MAP-E DDNS update request is not sent after booting up the device.
732760	SNMP trap packets are sometimes not sent from the primary `ha-direct` interface to all SNMP managers after upgrading.
734120	IPv6 Ready Phase 2 test failed on destination options (local link).
734565	Link monitor shows incorrect number of out-of-sequence packets.
734631	SSH UMAC cipher was not configured for umac-128, which causes `message authentication code incorrect` SSH error.
737711	When snmpd updates a huge table (~ 100K+) that might need more time than the SNMP client's timeout, the SNMP client meets a timeout error.
738332	Connectivity issue with FortiGuard after upgrading from 7.0.0 to 7.0.1 when `ha-direct` is enabled.
740649	FortiGate sends CSR configuration without double quote (`"`) to FortiManager.
742416	DNS does not resolve on FIM01, but resolves on other blades.
742471	Parsing FFDB may cause a crash when loading at reboot if the versions of FFDB_APP and FFDB_GEO_ID_FILE are different.

Bug ID	Description
743431	DDNS hostname is not correct when two VDOMs are configured.
743735	Potential DHCP memory leak when lease is mocked from reserved address.
745017	`get system checksum status` should only display checksums for VDOMs the current user has permissions for.
748628	Modem `init-string` failed on 7.0.0 and 7.0.1 because it was unable to find the endpoint address.
748987	L2TP tunnel is not working properly for Android; only ping traffic passes.

User & Authentication

Bug ID	Description
556724	LLDP neighbors cannot be seen on virtual switch ports.
691838	Memory leaks and crashes observed during stress long duration performance test when using FortiToken Cloud.
707057	TACACS server traffic will not go through the specific interface from the GUI irrespective of the interface set under the TAC.
709964	Apple devices cannot load the FortiAuthenticator captive portal via the system pop-up only.
711263	`diagnose fortitoken-cloud sync` fails when user email address is longer than 35 characters.
713503	When IdP uses optional SAML parameters, the firewall stops processing the login request.
721747	Client certificate authentication fails with Windows Hello for Business certificates.
725056	FSSO local poller fails after recent Microsoft Windows update (KB5003646, KB5003638, ...).
725327	FSSO user fails to log in with principal user name.
725988	CRLs with the same name in different non-management VDOMs cannot be updated automatically.
732413	Device IP is in the firewall user list , but it has no user name and group name, so the portal page cannot load.
733065	When deauthorizing from the GUI, the notification is sent to fsae rather than fssod, even the if the authentication type is FSSO.
739350	RADIUS response is sent even when the `rsso-radius-response` attribute is set to `disable`.
739702	There are unknown user logins on the FortiGate and the logs do not have any information for the unknown user.
741403	Unknown user log in to FortiGate does not provide any information for the unknown user.
742047	RADIUS Request Account-Status-Type Interim-Update Message does not have the Class attribute.
744014	LLDP neighbors cannot be seen on virtual switch ports.

VM

Bug ID	Description
582123	EIP does not fail over if the primary FortiGate is rebooted or stopped from the Alibaba Cloud console.
656701	FortiGate VMX Service Manager enters conserve mode (cmdbsvr has high memory utilization).
721439	Problems occur when switching between HA broadcast heartbeat to unicast heartbeat and vice versa.
722290	Azure slow path NetVSC SoftNIC has stuck RX. If using an IPsec tunnel, use UDP/4500 for ESP protocol (instead of IP/50) when SR-IOV is enabled. On the phase 1 interface, use `set nattraversal forced`. UDP/4500 is the fast path for Azure SDN, and IP/50 is the slow path that stresses guest VMs and hypervisors to the extreme. If using cross-site IPsec data backup, use Azure VNet peering technology to build raw connectivity across the site, rather than using the default IP routing based on the assigned global IP address.
729811	ASG synchronization is lost between secondary and primary instances if the secondary instance reboots. Affected platforms: all public cloud VMs and KVMs.
732556	AliCloud SDN connector will not fetch information from the secondary ENI, so filtering IP addresses by Vswitch ID and security group might be incorrect.
734148	The vmtoolsd and openvmtools processes are using a high amount of memory.
736067	NSX connector sometimes stops updating addresses.
739376	vmwd gives an error when folders are created in the vSphere web interface, and vmwd ignores the IP addresses from vApp.
747194	EIP failed to update on Azure FG-VM.

WAN Optimization

Bug ID	Description
735049	The HEAD request fails when `webcache` is enabled.

Web Filter

Bug ID	Description
677234	Unable to block webpages present in the external list when accessing them through the Google Translate URL.

Bug ID	Description
739349	Web filter local rating configuration check might strip the URL, and the URL filter daemon does not start when `utm-status` is disabled.
744303	Websites are blocked when *FortiGuard Category Based Filter* is disabled in web filter profile while doing an SSL-exempt check.
747591	Default web filter policy allows many of the potentially liable categories by default instead of blocking them.

WiFi Controller

Bug ID	Description
700356	CAPWAP daemon crashing due to IoT detection.
719217	*Interface Bandwidth* widget should exclude bridge VAP interface (and mesh VAP interface).
720674	cw_acd is crashing on FG-40F.
733608	FG-5001D unable to display managed FortiAPs after upgrading.
741946	FortiGate is not recognizing attribute 49, Acct-Terminate-Cause Value (6) Admin Reset, from RFC 2866.
748154	802.1X clients are disconnected following FortiGuard update.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
722821	FortiOS 7.0.2 is no longer vulnerable to the following CVE References: • CVE-2020-24586 • CVE-2020-24587 • CVE-2020-24588
726300	FortiOS 7.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2021-36169
753587	FortiOS 7.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2021-41024

Known issues

The following issues have been identified in version 7.0.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
752569	Per IP shaper under application list does not work as expected for some applications.

Endpoint Control

Bug ID	Description
708545	The WAD daemon is triggered to fetch the FortiClient information based on a ZTNA EMS tag enabled for checking in a proxy policy. It is then possible to get a ZTNA EMS tag in the firewall dynamic address and get the expected traffic control.
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.

Explicit Proxy

Bug ID	Description
664380	When configuring an explicit proxy with a forward server, if `ssl-ssh-profile` is enabled in the proxy policy, WAD is unable to learn the destination type correctly and the destination port is set to `0`, but the squid proxy server does not like such a request and returns an error.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	IPsec tunnel interfaces not created under the management VDOM may be displayed in the global view with a different tunnel state than what is displayed in the VDOM view.
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.
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	SSH from web portal does not copy/paste in Firefox.
713529	When FortiAnalyzer is configured, the HTTPS daemon may crash while processing some FortiAnalyzer log requests. There is no apparent impact on the GUI operation.
735248	On a mobile phone, the WiFi captive portal may take longer to load when the default firewall authentication login template is used and the user authentication type is set to HTTP. **Workaround**: edit the login template to disable HTTP authentication or remove the href link to googleapis.
738027	*Device Inventory* widget displays *No results* although devices are listed in the CLI.
746953	TFTP server (under *DHCP Server*) configured in the CLI is not reflected in the GUI.
748010	When creating or editing a ZTNA rule from the GUI, users cannot select the *any* option interface for *Incoming Interface*. Users can still configure this option in the CLI.

HA

Bug ID	Description
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.

IPsec VPN

Bug ID	Description
699973	IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages.

Proxy

Bug ID	Description
712584	WAD memory leak causes device to go into conserve mode.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
753056	Recommendation information for *Failed Login Attempts* security rating rule should display *Lockout duration should be at least 30 minutes*, instead of 1800 minutes.
753358	Unable to trigger automation trigger with FortiDeceptor Fabric event.

SSL VPN

Bug ID	Description
753515	DTLS does not work for SSL VPN and switches to TLS.

System

Bug ID	Description
639861	Support FEC (forward error correction) implementations in 10G, 25G, 40G, and 100G interfaces for FG-3400E and FG-3600E.
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
675558	SFP port with 1G copper SFP always is up.
679035	NP6 drops, and bandwidth limited to under 10 Gbps.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
683299	Port group members have different speeds after the port speed is changed using a CLI script.
685674	FortiGate did not restart after restoring backup configuration.
699152	QinQ (802.1ad) support needed on the following models: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3600E, and FG-3601E.
716341	SFP28 port flapping when the speed is set to 10G.

User & Authentication

Bug ID	Description
750551	DST_Root_CA_X3 certificate is expired. **Workaround**: see the Fortinet PSIRT blog, https://www.fortinet.com/blog/psirt-blogs/fortinet-and-expiring-lets-encrypt-certificates, for more information.

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.

WAN Optimization

Bug ID	Description
728861	HTTP/HTTPS traffic cannot go through when `wanopt` is set to manual mode and an external proxy is used. **Workaround**: set `wanopt` to automatic mode, or `set transparent disable` in the `wanopt profile`.
754378	When an AV profile is enabled in a WANOpt proxy policy on a server side FortiGate, EICAR sent over HTTPS will not get blocked.

WiFi Controller

Bug ID	Description
726266	GUI becomes unresponsive on FWF-60E with a wrong WTP entry.

Built-in AV engine

Resolved engine issues

Bug ID	Description
703918	AV engine scanunitd crash caused by a dead loop.
710610	Fix bug where content disarm and reconstruction removes pages from the original file.
729105	Add file typing support to DrawingML objects embedded in MSOFFICEX documents.
733158	Fix AV engine crash due to stack exhaustion.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
645848	FortiOS is providing self-signed CA certificate intermittently with flow-based SSL certificate inspection.
678890	IPS engine stalled, and alarm clock crash occurs at `pat_search_nocase`.
687885	Inconsistent system performance with RFC 2544 Ixia BreakingPoint testing.
691338	Performance issue with download dropping to 0 Kbps and slow website access after firmware upgrade.
709968	FortiGate drops UDP port 5440 traffic after rebooting both FortiGates.
712352	Firewall goes into conserve mode and IPS consumes high memory (6.00071).
720943	UTM does not work when the GRE session is created by a specific direction.
721435	Download breaks when the policy is flow-based with deep inspection, and the NCP application is used on the host.
728492	Unable to load instagram.com from Chrome browser without changing `TLS Post-Quantum Confidentiality` flag from default to enable.
729249	Web filter categorizes private IP address and local URLs as `Newly Observed Domain`.
730137	Unable to access website using policy in flow-based mode with web filter enabled.
731459	In NGFW policy mode, disabling a security policy does not stop the current traffic from passing through the firewall.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.
736906	The default `np-accel-mode basic` seems to cause sporadic HTTPS deep inspection transaction failures with application control.
738144	The UTM function only works for a few seconds in a GRE session.
741643	Traffic may be incorrectly blocked or match the wrong security policy in NGFW policy mode.
744352	Some websites open very slow in flow mode with SSL deep inspection (5.0245 and 5.0246).
744888	FortiGate drops Server Hello when accessing a website using a flow-based policy with SSL deep inspection.
745163	The ad.doubleclick.net website is not able to open in flow mode with deep packet inspection and a security profile in Chrome.

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