FortiOS - Release Notes

Version 6.4.3

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

FORTINET TRAINING 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

May 29, 2023
FortiOS 6.4.3 Release Notes
01-643-655918-20230529

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-10-22	Initial release.
2020-10-26	Updated *Resolved issues* and *Known issues*.
2020-10-28	Added sections for *Built-in AV engine* and *Built-in IPS engine*.
2020-11-09	Updated *New features or enhancements*, *Resolved issues*, and *Known issues*.
2020-11-10	Added *FortiClient EMS Cloud registration* to *Special notices*. Added 651942 and 656208 to *Resolved issues*.
2020-11-13	Added *SSL traffic over TLS 1.0 will not be checked and will be bypassed by default* to *Special notices*. Updated *New features or enhancements*, *Resolved issues*, *Known issues*, and *Built-in IPS engine*.
2020-11-17	Updated *Resolved issues* and *Known issues*.
2020-11-23	Added FG-80F, FG-80F-BP, and FG-81F to *Special branch supported models*.
2020-11-24	Updated *Resolved issues* and *Known issues*.
2020-11-26	Added *Policy routing enhancements in the reply direction* to *Special notices*.
2020-11-27	Updated 655931 in *New features or enhancements*.
2020-12-07	Added FG-VM64-IBM to *Supported models*.
2020-12-08	Moved 649193 in *Resolved issues* to *Common Vulnerabilities and Exposures* section.
2020-12-09	Updated *FortiClient EMS Cloud registration* in *Special notices*.
2020-12-15	Updated *New features or enhancements*, *Resolved issues*, and *Known issues*. Added *Virtual WAN link member lost* to *Upgrade Information*.
2020-12-30	Updated *Resolved issues* and *Known issues*. Added 230997 to *Changes in default behavior*.
2021-01-05	Updated *Resolved issues*.
2021-01-12	Updated *Changes in CLI*, *Resolved issues*, and *Known issues*.
2021-02-05	Updated *New features or enhancements*, *Resolved issues*, and *Known issues*.
2021-02-23	Updated *Known issues*.
2021-05-03	Updated *Built-in IPS engine*, *Resolved issues*, and *Known issues*.
2021-05-18	Added *Changes in GUI behavior*. Updated *Azure-On-Demand image*.

Date	Change Description
2021-05-31	Updated *Resolved issues* and *Known issues*.
2021-06-03	Updated FortiClient compatibility in *Product integration and support*.
2021-06-10	Updated *Resolved issues* and *Known issues*.
2021-07-16	Updated *Policy routing enhancements in the reply direction* in *Special notices*.
2021-08-12	Updated *Virtual WAN link member lost*.
2021-08-23	Updated *Known issues*.
2021-09-07	Updated *Resolved issues*.
2021-10-06	Updated *Known issues*.
2021-10-20	Updated *Known issues*.
2022-05-03	Updated *Product integration and support*.
2023-05-29	Updated *SSL traffic over TLS 1.0 will not be checked and will be bypassed by default*.

Introduction and supported models

This guide provides release information for FortiOS 6.4.3 build 1778.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.3 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, 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-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-60F
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 6.4.3. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1778.

FG-80F	is released on build 5486.
FG-80F-BP	is released on build 5486.
FG-81F	is released on build 5486.

Special notices

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	• Removed *System* > *Advanced* menu (moved most features to *System* > *Settings* page). • Moved configuration script upload feature to top menu > *Configuration* > *Scripts* page. • Removed GUI support for auto-script configuration (the feature is still supported in the CLI). • Converted all compliance tests to security rating tests.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.0 has resolved bug 570575 to fix a FortiGate failing to provide power to ports. The PoE hardware controller, however, may require an update that must be performed using the CLI. Upon successful execution of this command, the PoE hardware controller firmware is updated to the latest version 2.18:

```
diagnose poe upgrade-firmware
```

AWS-On-Demand image

Bug ID	Description
589605	Starting from FortiOS 6.4.0, the FG-VM64-AWSONDEMAND image is no longer provided. Both AWS PAYG and AWS BYOL models will share the same FG-VM64-AWS image for upgrading and new deployments. Remember to back up your configuration before upgrading.

Azure-On-Demand image

Bug ID	Description
657690	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.

FortiClient EMS Cloud registration

FortiOS 6.4.3 and later adds full support for FortiClient EMS Cloud service.

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`, set the following to `block` in the SSL protocol settings:
  - in FortiOS 6.2.6 and later:

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl block
        end
    next
end
```

  - in FortiOS 6.4.3 and later:

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl-negotiation block
        end
    next
end
```

Policy routing enhancements in the reply direction

When reply traffic enters the FortiGate, and a policy route or SD-WAN rule is configured, the egress interface is chosen as follows.

With `auxiliary-session enabled` in `config system settings`:

- Starting in 6.4.0, the reply traffic will not match any policy routes or SD-WAN rules to determine the egress interface and next hop.
- Prior to this change, the reply traffic will match policy routes or SD-WAN rules in order to determine the egress interface and next hop.

With `auxiliary-session disabled` in `config system settings`:

- The reply traffic will egress on the original incoming interface.

Changes in CLI

Bug ID	Description

587183	Remove the intelligent mode option from the IPS global configuration:
	`config ips global`
	`    set intelligent-mode {enable | disable}`
	`end`

640620	In the `wireless-controller arrp-profile` configuration, the `include-weather-channel` and `include-dfs-channel` options have changed from `yes`/`no` to `enable`/`disable`.
657726	Remove option to rate images by URL for web filter profile in the GUI and CLI.

Changes in GUI behavior

Bug ID	Description
655380	Improve GUI error reports when users run into errors during configuration.

Changes in default behavior

Bug ID	Description
230997	Do not allow `match-vip` in firewall policies when the action is set to accept.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description

477886	PRP support for SoC4:
	• Configure ingress port to allow the PRP trailer to not be stripped off when the PRP packets come in.
	• Configure egress port to allow the PRP trailer to not be stripped off when the PRP packets go out.
	`config system npu`
	`    set prp-port-in "port1"`
	`    set prp-port-out "port2"`
	`end`

611992	Add a specific `auth-timeout` field in the SSL VPN monitor.
621725	Add settings to enable flow control and pause metering. Pause metering allows the FortiSwitch to apply flow control to ingress traffic when the queue is congested and to resume once it is cleared.
628963	When 802.1x authentication requests to a RADIUS server time out, the `authserver-timeout` settings within the `switch-controller security-policy 802.1x` will assign the port to a timeout VLAN.
634357	Add NPU support for GTP-U encapsulated in IPv6.

638352	To avoid large number of new IKEv2 negotiations from starving other SAs from progressing to established states, the following enhancements have been made to the IKE daemon:
	• Prioritize established SAs.
	• Offload groups 20 and 21 to CP9.
	• Optimize the default embryonic limits for mid- and high-end platforms.
	The IKE embryonic limit can now be configured in the CLI:
	`config system global`
	`    set ike-embryonic-limit <integer>`
	`end`

641077	After authorizing a FortiAP, administrators can also register the FortiAP to FortiCloud directly from the FortiGate GUI.
647800	AWS and Azure now support FIPS ciphers mode.
649075	FortiGate-VMs on AWS now use Amazon EC2 instance metadata service version 2 (IMDSv2) to query and retrieve metadata from the AWS cloud.
650936	Add support for FortiFlex, an enterprise license agreement for virtual machine licensing where users can manage and monitor their VM subscription in the FortiCloud portal.
651866	FortiSwitch events now have their own category on the *Events* log page.

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>652003</td><td>In a tenant VDOM, allow `lldp-profile` and `lldp-status` to be configurable on a leased switch port.</td></tr>
<tr><td>652225</td><td>Configuring the DiffServ code in phase 2 of an IPsec tunnel allows the tag to be applied to the ESP packet. NPU offloading must be disabled for this tunnel.</td></tr>
<tr><td>652503</td><td>

By configuring the service chain and service index, NSX-T east-west traffic can be redirected to a designated FortiGate VDOM.

```
config nsxt setting
    set liveness {enable | disable}
    set service <service name>
end
config nsxt service-chain
    edit <ID>
        set name <chain name>
        config service-index
            edit <forward index>
                set reverse-index <value>
                set name <index name>
                set vd <VDOM>
            next
        end
    next
end
```

The default value for `reverse-index` is 1. The `vd` setting is required.

</td></tr>
<tr><td>655920</td><td>Support 802.11v load balancing and optimized roaming.</td></tr>
<tr><td>655931</td><td>

Adaptive Radio Architecture (ARA) allows FortiAPs to calculate the network coverage factor (NCF) based on radio interference. When Dynamic Radio Mode Assignment (DRMA) is enabled, if interference crosses a threshold, the radio becomes redundant by moving from AP mode to monitor mode.

```
config wireless-controller wtp-profile
    edit <profile>
        config radio-1
            set band 802.11n/g-only
            set drma {enable | disable}
            set drma-sensitivity {high | medium | low}
        end
    next
end
```

</td></tr>
<tr><td>656039</td><td>Allow SD-WAN duplication rules to specify SD-WAN service rules to trigger packet duplication. This allows SD-WAN duplication to occur based on an SD-WAN rule instead of the source, destination, or service parameters in the duplication rule.</td></tr>
<tr><td>657598</td><td>In an application control list, the `exclusion` option allows users to specify a list of applications they wish to exclude from an entry filtered by category, technology, or others.</td></tr>
</table>

Bug ID	Description

	`config application list`
	`    edit <list>`
	`        config entries`
	`            edit 1`
	`                set category <ID>`
	`                set exclusion <signature ID> ... <signature ID>`
	`            next`
	`        end`
	`    next`
	`end`

658006	Simplify FortiExtender deployment so it is displayed in the topology.
658525	The limit of BGP paths that can be selected and advertised has increased to 255 (originally 8).
659127	Add support to deploy FortiGate-VMs that are paravirtualized with SR-IOV and DPDK/vNP on OCI shapes that use Mellanox network cards.
659346	Add additional information such as DHCP server MAC, gateway, subnet, and DNS to wireless DHCP logs.

660250	Add global option `fortiipam-integration` to control FortiIPAM. When enabled, ipamd will run and report to FortiIPAM to allow automatic IP address/subnet management.
	`config system global`
	`    set fortiipam-integration {enable | disable}`
	`end`

660273	By default, the FortiGate uses the outbound interface's IP to communicate with a FortiSwitch managed over layer 3. The `switch-controller-source-ip` option allows the switch controller to use the FortiLink fixed address instead.
661131	Enabling IGMP snooping on an SSID allows the wireless controller to detect which FortiAPs have IGMP clients. The wireless controller will only forward a multicast stream to the FortiAP where there is a listener for the multicast group.
663530	IoT background scanning is disabled by default. Users can enable this option on the *FortiLink Interface* page in the GUI or with the `switch-controller-iot-scanning` in the CLI.
664312	Integrate Broadcom bnxt_en 1.10.1 driver to drive new vfNIC to replace 1.9.2 version. The following new cards are supported: • [BCM57508] = { "Broadcom BCM57508 NetXtreme-E 10Gb/25Gb/50Gb/100Gb/200Gb Ethernet" } • [BCM57504] = { "Broadcom BCM57504 NetXtreme-E 10Gb/25Gb/50Gb/100Gb/200Gb Ethernet" } • [BCM57502] = { "Broadcom BCM57502 NetXtreme-E 10Gb/25Gb/50Gb Ethernet" } • [BCM57508_NPAR] = { "Broadcom BCM57508 NetXtreme-E Ethernet Partition" } • [BCM57504_NPAR] = { "Broadcom BCM57504 NetXtreme-E Ethernet Partition" } • [BCM57502_NPAR] = { "Broadcom BCM57502 NetXtreme-E Ethernet Partition" } • [BCM58812] = { "Broadcom BCM58812 NetXtreme-S 2x50G Ethernet" }

Bug ID	Description
	- [BCM58814] = { "Broadcom BCM58814 NetXtreme-S 2x100G Ethernet" } - [BCM58818] = { "Broadcom BCM58818 NetXtreme-S 2x200G Ethernet" } - [NETXTREME_E_P5_VF] = { "Broadcom BCM5750X NetXtreme-E Ethernet Virtual Function" }

665735	The user device store allows user and device data collected from different daemons to be centralized for quicker access and performance:
	`diagnose user-device-store device memory list`
	`diagnose user-device-store device memory query mac <value>`
	`diagnose user-device-store device memory query ip <value>`
	`diagnose user-device-store device disk list`
	`diagnose user-device-store device disk query <SQL WHERE clause>`

668362	Support multiple LDAP server configurations for Kerberos keytab and agentless NTLM domain controller in multiple forest deployments.
668991	Security Fabric rating reports can now be generated in multi-VDOM mode, against all VDOMs. The Security Rating is visible under Global scope.

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*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Mac-address-based device policies – Detected devices can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- MAC-address-based policies – A new address type is introduced (MAC address range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

In 6.4.0, device detection related GUI functionality has been relocated:

1. The device section has moved from *User & Authentication* (formerly *User & Device*) to a widget in *Dashboard*.
2. The email collection monitor page has moved from *Monitor* to a widget in *Dashboard*.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.4.3 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.4.3
- FortiManager 6.4.3
- FortiClient EMS 6.4.1 build 1498 or later
- FortiClient 6.4.1 build 1519 or later
- FortiAP 6.0.6 build 0075 or later
- FortiSwitch 6.0.6 build 0076 or later

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

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

⚠ If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.3. When Security Fabric is enabled in FortiOS 6.4.3, all FortiGate devices must be running FortiOS 6.4.3.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.3 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.4.3 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

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

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.4.3 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.4.3 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5
C5d
C5n
F1
G3
G4
H1
I3
I3en
Inf1
m4.16xlarge
M5
M5a
M5ad
M5d
M5dn
M5n
P2
P3
R4
R5
R5a
R5ad
R5d
R5dn
R5n
T3
T3a
u-6tb1.metal
u-9tb1.metal
u-12tb1.metal
u-18tb1.metal
u-24tb1.metal
X1
X1e
z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.4.3, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.4.3.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix Hypervisor 8.1 Express Edition

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V Server 2019 and Windows Server 2012R2 with Hyper-V role

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

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

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

- Optimal: Default dashboard settings in 6.4.1
- Comprehensive: Default Monitor and FortiView settings before 6.4.1

Filtering facets are available for FortiView widgets in full screen and standalone mode.

WanOpt configuration changes in 6.4.0

Port configuration is now done in the profile protocol options. HTTPS configurations need to have certificate inspection configured in the firewall policy.

In FortiOS 6.4.0, `set ssl-ssh-profile certificate-inspection` must be added in the firewall policy:

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.2.

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.

Virtual WAN link member lost

The member of `virtual-wan-link` is lost after upgrade if the `mgmt` interface is set to `dedicated-to management` and part of an SD-WAN configuration before upgrade.

Product integration and support

The following table lists FortiOS 6.4.3 product integration and support information:

Web Browsers	• Microsoft Edge 83 • Mozilla Firefox version 82 • Google Chrome version 86 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 21. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 21. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.4.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 21 and Fortinet Security Fabric upgrade on page 21. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.
FortiClient iOS	• 6.4.0 and later
FortiClient Android and FortiClient VPN Android	• 6.4.0 and later
FortiClient EMS	• 6.4.0
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0294 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	• 6.00154
IPS Engine	• 6.00058
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 82 Google Chrome version 86
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 82 Google Chrome version 86
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
macOS Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 82 Google Chrome version 86
iOS	Apple Safari Mozilla Firefox

Operating System	Web Browser
	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 6.4.3. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
560044	Secondary device blades occasionally report critical log event `Scanunit initiated a virus engine/definitions update`. Affected models: FG-5K, 6K, and 7K series.
635365	FortiGate enters conserve mode.

Application Control

Bug ID	Description
651019	For Google.Drive_File.Sharing signature, if it is set to deny in NGFW policy mode and followed by another policy with allow all, the client can still share file.

Data Leak Prevention

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

DNS Filter

Bug ID	Description
649985	Random SDNS rating timeout events on 6K/7K SLBC with FGSP.

Explicit Proxy

Bug ID	Description
644121	Explicit proxy error 504, DNS fails for a specific domain.
650540	FortiGate sends traffic to an incorrect port using a wrong source NAT IP address.
654211	When the category proxy address is applied in a proxy policy, if SOCKS traffic passes through the web proxy, when matching the SOCKS traffic with the proxy address, the WAD will crash with signal 11 at wad_url_choose_cate. Browsers may send SOCKS traffic in the background from time to time.
660703	Using the HTTP explicit proxy denies access to non-HTTP traffic and displays a policy violation.

Firewall

Bug ID	Description
586764	Abnormal prolonged CPU spike with cmdbsvr and WAD processes when making change to large policy list (10 000+ policies).
586995	Cluster VDOM policy statistics data is not correct when VFID is different for same VDOM on primary/secondary.
609027	SCTP secondary path not working in ECMP context; incorrect expectation session created from auxiliary session.
616220	ICMP reply packets dropped by the FortiGate.
635074	Firewall policy `dstaddr` does not show virtual server available based on virtual WAN link member.
643446	Fragmented UDP traffic is silently dropped when fragments have different ECN values.
647410	`append` command allows mixing VIP and firewall address as destination objects in a firewall policy.
648951	External threat feed entry `0.0.0.0/0` shows as invalid but it blocks traffic.
650700	There should be an event log when there are internet service remove/merge entries.
650867	Firewall does not track UDP sessions on the same port.
656678	Different ciphers for SSL/HTTPS virtual servers.
659142	TNS connection request limited to 500 per second when client is trying to reach database server through the firewall.
660461	Configuration changes take a long time, and ipsmonitor and cmdbsrv processes go up to 100% of CPU in a large, complex configuration.

FortiView

Bug ID	Description
643198	*Threats* drilldown for *Sources*, *Destinations*, and *Country/Region* (1 hour, 24 hours, 7 days) gives the error, *Failed to retrieve FortiView data*.

GUI

Bug ID	Description
446427	Using the GUI to update a VDOM license fails when the new license has a lower VDOM count than the current license.
543192	Source IP is not used when using the GUI to query the FortiGuard filtering service.
547123	The help message for `gui-dynamic-profile-display` is not correct.
561889	When creating a firewall with an invalid subnet mask, an error is not generated.
588159	When disabling *Allow Endpoint Registration* on the *VPN Creation Wizard*, the action succeeds, but the error *Unable to setup VPN* is incorrectly displayed.
606814	When creating a profile group with an SSL/SSH profile of *no-inspection*, the profile group correctly displays this, but when you edit the profile, *certificate-inspection* is displayed.
612066	GUI does not allow user to select SSL VPN tunnel when configuring *Multicast* routing.
634550	GARP is not sent when using the GUI to move a VDOM from one virtual cluster to another. GARP is sent when using the CLI.
638752	FortiGates in an HA A-P configuration may lose GUI access to the HA secondary device after a period of 8 days of inactivity, when at least one static IPv6 address is configured on an interface.
638822	On *Dashboard Setup* page, changes made by super administrator and administrator of multiple VDOMs should be reflected in all managed VDOMs.
645441	FortiAnalyzer Cloud card on the *Fabric Connectors* page shows a connected icon when it is not connected.
645606	GUI does not allow users to select SD-WAN as a destination interface in an SSL VPN policy while CLI does.
646327	Web filter profile dialog cannot load URL filter table if there are a lot of URL filters.
649027	The *FortiLink Interface* pane incorrectly displays high CPU usage and poor health.
650307	GUI does not show the configured external FortiGuard category in the SSL-SSH profile's exempt list.
650800	Unable to delete multiple phase 2 selectors at the same time from the VPN IPsec tunnels dialog.

Bug ID	Description
651412	Unable to print user data for guest management.
651711	Unable to select an address group when configuring *Source IP Pools* for an SSL VPN portal.
652975	Cannot access FortiGate GUI over IPv6 after configuring IPv6 for the first time.
653240	When refreshing the FortiGuard page, connectivity status for *Web Filtering* and *Anti-Spam* incorrectly changes from up to down.
653422	When VDOM is enabled, the GUI cannot be used to edit a remote user group from within the *Administrators* dialog.
654018	When there are more than 600 quarantined IP addresses, the *Quarantine Monitor* (GUI and CLI) will not properly display them.
654186	The top charts of the *Device Inventory Monitor* dashboard are empty when the visualization is set to table view.
654250	Firewall users cannot change their password via web captive portal when password renewal is enforced by the firewall policy for remote users.
654256	GUI interface speed test fails when there are multiple VDOMs.
654339	GUI search does not work in the interface list if DHCP client and range columns are present.
654626	Unable to change the action setting of *Freeware and Software Downloads* using the *FortiGuard Category Based Filter* of the DNS filter profile.
655255	FortiGuard resource retrieval delay causes GUI pages to respond slowly. Affected pages include: *Firewall Policy*, *Settings* (log and system), *Explicit Proxy* (web and FTP), *System Global*, and *System CSF*.
655568	Users cannot deselect *Administrative Access* options for VLAN interfaces from the GUI; the CLI must be used.
655891	Web CLI console cannot load due to `Connection lost` if port 8080 is used (HTTP).
656139	When editing the *Interface* column from the *Multicast Policy* page, an empty column appears when the *any* entry is selected from *Select Entries* and applied. The same occurs from the NAT64 and NAT46 policy pages.
656429	Intermittent GUI process crash if a managed FortiSwitch returns a reset status.
656974	`ip6-mode` was changed from `delegated` to `static` after the interface was edited from the GUI.
657322	For AV profiles, the outbreak-prevention setting on enabled protocols is not automatically configured when enabling *Use External Malware Block List*.
657545	Enabling the *Dynamic Gateway* toggle for a static route fails without warning when the configuration is incorrect.
661582	*Date/Time* filter does not work on FortiGate Cloud logs.
663737	Re-add the FortiView facets filtering bar to full screen or standalone mode.

Bug ID	Description
663818	When filtering log view entries by IP address range, entries higher than the upper limit of the range are shown.
663956	Unable to load web CLI console for LDAP admin with a login name that contains a space.
668646	FortiSwitch topology is not shown on *Managed FortiSwitch* page topology view.

HA

Bug ID	Description
421335	Get one-time hasync crash when running HA scripts for FIPS-CC.
583059	In Hyper-V HA, CLI will falsely report `can not set mac address` when MAC address is set.
637711	CSR on cluster primary is generating out-of-sync alerts on secondary and tertiary units.
640327	Duplicate logs are created by both primary and secondary devices for IPsec VPN.
643958	Inconsistent data from FFDB caused several confsyncd crashes.
647679	Inconsistent values for HA cluster inside the SNMP.
651177	When secondary device reboots, it adds an interface to the virtual switch. Secondary cannot synchronize after it starts, as that interface disappears in `system interface` and `virtual-switch`.
651674	Long sessions lost on new primary after HA failover.
654341	The new join-in secondary chassis failed to sync, while primary chassis has 6K policies in one VDOM.
656099	The mgmt interfaces are excluded for heartbeat interfaces (even if `dedicate-mgmt` is not enabled).
657376	VLAN interfaces are created on a different virtual cluster primary instead of the root primary do not sync.
662893	HA cluster goes out of sync if SAML SSO admin logs in to the device.

Intrusion Prevention

Bug ID	Description
655371	Logging is intermittent for FortiGate IDS passive in one-armed sniffer mode.
660111	SSL VPN web mode IPS detection with HTTP does not work, even though it works with HTTPS.

IPsec VPN

Bug ID	Description
592361	Cannot pass traffic over ADVPN if: `tunnel-search` is set to `nexthop`, `net-device disable`, `mode-cfg enable`, and `add-route disable`.
614483	Add IKEv2 phase 2 initiator traffic selector narrowing for Cisco compatibility.
638352	In extreme situations when thousands of tunnels are negotiating simultaneously (IKEv2), iked process gets exhausted and stuck.
638573	FortiGate is not deleting the shortcut tunnel for ISPA (primary ISP) when ISPA is down.
639806	User name log empty when IPsec dialup IKEv2 has client RSA certificate with empty subject.
646012	DHCP over IPsec randomly works when `net-device` is disabled.
647285	IKE HA sync IPsec SA fails on receiver when ESP null crypto algorithm is used.
650599	IKE HA sync truncates phase 2 option flags after the first eight bits.
655739	`local-gw` is replaced with primary IP on a secondary device when the secondary IP is used as a `local-gw`.
659535	Setting same `phase1-interface` in SD-WAN member and SD-WAN zone causes iked watchdog timeout.
660472	Could not locate phase 1 configuration for IPv6 dialup IPsec VPN.
666693	If NAT-T IP changes, the dynamic IPsec spoke add route entry is stuck on hub.
668554	Upon upgrading to FortiOS 6.4.2, a device with IPsec configured may experience IKE process crashes when any configuration change is made or an address change occurs on a dynamic interface.

Log & Report

Bug ID	Description
642941	For URLs over 66 characters, the FortiGate replaces remaining characters with dots (.) in `dstname` field when forwarded to syslog/FortiAnalyzer.
643840	`vwlservice` should log the SD-WAN rule and not an internet service; impacts FortiAnalyzer SD-WAN monitor widgets and reports.
645914	Move `eventtime` field to the beginning of the log to save performance on Splunk or other logging systems.
647741	On FG-60F, logging and FortiCloud reporting incorrect IPv6 bandwidth usage for sessions with NPU offload.

Bug ID	Description
650325	miglogd crashes with signal 11.
651581	FortiGate tried to connect to FortiGate Cloud with the primary IP after reboot, although the secondary IP is the source in the FortiGuard log.
654363	Traffic log shows *Policy violation* for traffic hitting the allow policy in NGFW policy mode.
658665	Cannot retrieve logs from FortiAnalyzer on non-root VDOM.

Proxy

Bug ID	Description
550350	Should not be able to set `inspection-mode proxy` with IPS-enabled only policy.
579902	Proxy deep inspection fails if server chooses to sign with ECDSA-SHA1.
619707	When Kerberos (negotiate without NTLM) authentication method is used for web proxy user authentication, there may be a rare memory leak issue. This memory leak issue may eventually cause the FortiGate to go into conserve mode once it occurs after many users are authenticated by Kerberos repeatedly over time.
633108	When FOH server is disconnected from a HTTP session, the HTTP session client port peer is not cleared. After this, the HTTP client port shutdown causes a crash because the peer port is freed.
638039	Delete validation is not working for *Protecting SSL Server* profile.
648831	WAD memory leak caused by Kerberos proxy authentication.
653099	Wildcard URL filter in proxy mode with `?` and `*` not always handled properly.
655356, 660857	Proxy deep inspection fails if server uses TLS 1.3 cookies or record padding.
656830	FortiGate should be in SSL bypass mode for TLS 1.2 certificate inspection with client certificate request.
658654	Cannot access specific website using proxy-based UTM with certification inspection due to delays from the server in replying to ClientHello message when a second connection from the same IP is also waiting for ClientHello.
663088	Application control in Azure fails to detect and block SSH traffic with proxy inspection.
666522, 666686	Proxy mode is blocking web browsing for some websites due to certificate inspection.

Routing

Bug ID	Description
585816	SD-WAN route selection does not use the most specific route in the routing table when selecting the egress path.
613716	Local-out TCP traffic changes output interface when irrelevant interface is flapping and causes disconnections.
639884	`diagnose ip proute match` gives wrong result when VRF is configured.
641050	Need support for SSL VPN web mode traffic to follow SD-WAN rules/policy route.
644461	Unable to redistribute BGP into OSPF based on community (in VRF 0).
649558	ISDB policy routes are not removed when the SD-WAN member is down.
653096	PMTU calculation for VPN interfaces is not working. FortiGate ignores ICMP type 3 code 4 messages and does not update the routing cache.
654482	SD-WAN route tag is removed with multiple BGP paths in place.
655447	BGP prefix lifetime resets every 60 seconds when scanning BGP RIB.
655480	Upgrading to FortiOS 6.4.2 breaks all SD-WAN performance SLAs that use HTTP.
660285	Editing an existing route map rule to add `set-weight 0` results in `unset set-weight` behavior.
660300	Application vwl signal 11 (segmentation fault) received when HA receives 0 bytes of data.
660311	Application vwl signal 6 (aborted) received due to wrong memory allocation for SD-WAN service when creating an ADVPN shortcut.
661769	SD-WAN rule disappears when an SD-WAN member experiences a dynamic change, such as during a dynamic PPPoE interface update.
662655	The OSPF neighborship cannot be established; get MD5 authentication error when the wrong MD5 key is deleted after modifying the key.
662696	If a session is initiated from the server side, SD-WAN application control does not work as expected.
662845	HA secondary also sends SD-WAN `sla-fail-log-period` to FortiAnalyzer.
663057	IPv6 routing does not work properly to be a dual stack.
666829	Application bfdd crashes.
668218	SD-WAN HTTP health check does not work for URLs longer than 35 characters.

Security Fabric

Bug ID	Description
649344	When viewing CSF child *Dashboard* > *WiFi* from parent FortiGate, GUI reports, *Cannot read property 'spectrum_analysis' of undefined*.
652737	FortiGate does not send interface configuration to FortiIPAM.
653368	Root FortiGate fails to load Fabric topology if HA downstream device has a trusted device in both primary and secondary FortiGates.
660250	The ipamd process is causing high memory usage after a few days as the JSON was not freed.
662128	*Security Rating Summary* trigger is not available in multi-VDOM mode.

SSL VPN

Bug ID	Description
548599	SSL VPN crashes on parsing some special URLs.
613733	Access problem for website.
615453	WebSocket using Socket.IO could not be established through SSL VPN web mode.
620793	A page inside a bookmark not opening in SSL VPN web mode.
620946	All sslvpnd daemons use 99.9% CPU when policy is being updated.
630771	SSL VPN rewrites the URL inside the emails sent in Outlook (webmail).
637217	Internal webpage, di***, is not loading in web mode.
641379	Internal SharePoint 2019 website cannot be accessed in SSL VPN web portal.
642838	Redirected URLs do not work in web mode for am***.com.
645973	Content from internal Microsoft Dynamics CRM cr***.local portal is not loading properly in SSL VPN web mode.
646295	When DNS domain is configured, requests with NTLM of host name-only bookmark could not get response from server.
647202	fas crashes when using FortiToken Cloud to access SSL VPN tunnel.
648433	Internal website loading issue in SSL VPN web portal for ca***.fr.
649130	SSL VPN log entries display users from other VDOMs.
651942	For RADIUS server, `all-usergroup` does not work if there is a same remote user created but not used by SSL VPN.
652060	BMC Remedy Mid Tier 9.1 web app is not displayed properly in SSL VPN web mode.

Bug ID	Description
652070	BMC Remedy Mid Tier 8.1 web application elements are not displayed properly in SSL VPN web mode.
652762	SSL VPN web mode HTTPS bookmark fails to load (times out).
652880	SSL VPN crashes in a scenario where a large number of groups is sent to fnbam for authentication.
653349	SSL VPN web mode not working for Ec***re website.
654534	SAML authentications occurring through SSL VPN web mode are not completing.
655374	SSL VPN web portal bookmark not loading internal web page after login credentials are entered.
656208	Users with explicit web proxy authentication lose their proxy authentication group.
657689	The system allows enabling split tunnel when the SSL VPN policy is configured with destination `all`. It is not consistent with 5.6.x and 6.0.x.
657890	Internal website, https://*.da***.cz, is not working correctly in SSL VPN web mode due to source link error.
658036	When adding an FTP link to download FortiClient and accessing it through the portal, the colon is dropped from the string.
659234	FortiGate keeps replying to an ARP request for an IP address that was once assigned to an SSL VPN user, who has already disconnected and been deleted.
659312	Unable to load HTTPS bookmark in Safari (`TypeError: 'text/html'`).
659481	Internal websites not displayed successfully in SSL VPN web portal.
661372	SSL VPN incorrectly rewrites the script URL.
661835	ASUS ASMB9-iKVM application shows blank page in SSL VPN web mode.
662042	The https://outlook.office365.com and https://login.microsoft.com websites cannot be accessed in the SSL VPN web portal.
663298	The internal website is not working properly using SSL VPN.
663433	SSL VPN web mode cannot open DFS shared subdirectories, get *Invalid HTTP request* error as sslvpnd adds `NT`.
664121	SCM VPN disconnects when performing an SVN checkout.
664804	User cannot use column header for data sorting (bookmark issue).
665879	When sslvpn processes the HTTP/HTTPS response with content disposition, it will change the response body since the content type is HTML.
666194	WALLIX Manager GUI interface is not loading through SSL VPN web mode.

Switch Controller

Bug ID	Description
649913	HA cluster not synchronizing when configuring an active LACP with MCLAG via FortiManager.
652745	Compatibility issues with FortiGate in 6.0 branch and FortiSwitch 424E-Fiber.

System

Bug ID	Description
581496	FG-201E stops sending out packets and NP6lite is stuck.
582536	Link monitor behavior is different between FGCP and SLBC clusters.
585882	Error in log, `msg="Interface 12345678001-ext:64 not found in the list!"`, while creating a long name VDOM in FG-SVM.
594577	Out-of-order packets for an offloaded multicast stream.
598464	Rebooting FG-1500D in 5.6.x during upgrade causes an L2 loop on the heartbeat interface and VLAN is disabled on the switch side.
603194	NP multicast session remains after the kernel session is deleted.
609660	NPU offloading enabled dropping traffic from IPsec VPN tunnel remote gateway.
627236	TCP traffic disruption when traffic shaper takes effect with NP offloading enabled.
627269	Wildcard FQDN not resolved on the secondary unit.
630146	FG-100F memory configuration check.
631132	Symantec connector does not work if management VDOM is not root vdom and root VDOM has no network connection.
631296	Forward or local bi-directional traffic from NPU inter-VDOM links through separate VDOMs is subject to high latency.
631689	FG-100F cannot forward fragmented packets between hardware switch ports.
633827	Errors during fuzzy tests on FG-1500D.
636999	LTE does not connect after upgrading from 6.2.3 on FG-30E-3G4G models.
637014	FortiGate in LENC mode unable to pass firmware signature verification and shows as uncertified after GUI upgrade.
637983	FG-100F memory configuration check fails because of wrong threshold.
642005	FortiGate does not send `service-account-id` to FortiManager via fgfm tunnel when FortiCloud is activated directly on the FortiGate.

Bug ID	Description
642327	FortiGate unable to boot with kernel panic by cmdbsvr when VLAN is configured on redundant interface with non-NPU port.
642958	FG-80E terminates the firewall session abruptly when the end-users download large files.
644380	FG-40F/60F kernel panic if upgrading from 6.4.0 due to configuration file having a name conflict of `fortilink` as both aggregate interface and virtual switch name.
645723	Cannot set overlap IP on global level if `allow-subnet-overlap` on management VDOM is disabled.
648014, 661784	FortiDDNS is unable to update the renewed public IP address to FortiGuard server in some error conditions.
648083	cmdbsvr may crash with signal 11 (segmentation fault) when frequently changing firewall policies.
650878	DHCP relay will honor the broadcast flag set to 0 (unicast) in only one VDOM at a time in a multi-VDOM environment.
653289	FortiExtender virtual interface cannot get IP after rebooting the system.
654159	NP6Xlite traffic not sent over the tunnel when NPU is enabled.
654624	Error message shown (`get_ha_sync_obj_sig_4dir delete broken symbolic link /etc/cert/ca/5c44d531.0`) when upgrading from 6.4.1.
656412	The interface speed setting should be kept after deleting the virtual switch.
656504	Kernel panic happened on FWF-61F and FWF-40F.
657632	IPv6 passes though the DNS filter with application control enabled.
659539	FortiGate running 6.4.2 GA cannot validate license via FortiManager due to FortiManager hardware missing Fortinet_CA2 and Fortinet_SUBCA2001.
662208	Configuration changes take a long time and cmdbsrv processes use up to 100% CPU.
662239	FGR-60F-3G4G hardware switch span does not work.
663603	The maximum number of IPS supported by each NTurbo load balancer should be 7 instead of 8 on FG-3300E and FG-3301E.
663815	Low IPS HTTP throughput on SoC4 platforms.
665000	HA LED off issue on FG-1100E/1101E models.

Upgrade

Bug ID	Description
646877	FortiOS allows the elimination of interfaces, although it still has a VIP reference used in firewall policies.
656869	FG-100F/101F may continuously boot upon upgrading from FortiOS 6.4.0.

Bug ID	Description
	Workaround: back up the 6.4.0 configuration, perform a clean install via TFTP of FortiOS 6.4.2, and restore the 6.4.0 configuration.

User & Authentication

Bug ID	Description
643191	FSSO TS-Agent is not working properly when FortiGates use NGFW policy-based mode.
655422	A space after a comma within `CN` is incorrectly removed during the bind request causing authentication failure (LDAP).
656118	Password displayed as clear text in FortiManager installation log when resetting the system admin user password via FortiManager.
658228	The authd and foauthd processes may crash due to crypto functions being set twice.
658794	FortiGate sent CSR certificate instead of signed certificate to FortiManager when retrieve is performed.
659456	REST API authentication fails for API user with PKI group enabled due to fnbamd crash.
662391	Persistent sessions for de-authenticated FSSO users.
663399	`interface-select-method` not working for RADIUS configuration.

VM

Bug ID	Description
637376	In FG-VM64-HV, 802.1Q does not work on interfaces with DPDK enabled.
640532	ESXi 6.0 gets `Kernel panic - not syncing: Attempted to kill init!` message.
645798	In FG-VM64-HV, `portX: can not set mac address(16).` error displayed in console after HA is enabled and all interfaces lose connections.
647800	Merge FIPS ciphers to 6.4.3 and 7.0 trunk (visible to AWS and Azure only).
652416	AWS Fabric connector always uses root VDOM even though it is not a management VDOM.
657785	On FG-AWS, changing health check protocol to `tcp-connect` causes kernel panic and reboot.
662969	Azure SDN connector filter count is not showing a stable value.
663276	After cloning the OCI instance, the OCID does not refresh to the new OCID.
663487	Should add router policy in `vdom-exception` list.

Bug ID	Description
664312	Support vfNIC driving for Broadcom 100G NIC.
668131	EIP is not updating properly on FG-VM Azure.
670166	FG-VM64-KVM configuration revisions lost after upgrading from 6.2.5.

Web Filter

Bug ID	Description
587018	Add URL flow filter counters to SNMP.
610553	User browser gets URL block page instead of warning page when using HTTPS IP URL.
650916	Loopback interface as source IP is not getting applied to FortiGuard web filter rating.
654160	Web filter profile count decreased after upgrading to 6.4.0 on FG-100F.
654675	Unable to get complete output of `diagnose test application ipsufd 1`.
655972	Custom category action set to allow in web filter profile causes the URL to use the FortiGuard category rather than the custom category.
661713	Global web filter profile is not applied after changes to allowed/blocked categories.

WiFi Controller

Bug ID	Description
609549	In the CLI, the WTP profile for `radio-2` 802.11ac and 80 MHz channels does not match the syntax collection files.
647703	HTTPS server certificate is not presented when WiFi controller feature is disabled in *Feature Visibility*.
655689	Wireless hostapd daemon crashes upon WPA3-SAE connection.
656804	Spectrum analysis disable/enable command removed in CLI from `wtp-profile` and causing a bottleneck for APs, such as FAP-222C/223C at 100% CPU.
657391	FG-600E has cw_acd crash with `*** signal 8 (Floating point exception) received ***` in 6.2.4.
660991	FAP-U431F cannot view what channel is operating, and the override channel setting must be unset to change to a different channel.
665766	Client failed to connect SSID with WPA2-Enterprise and user group authentication.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
649193	FortiOS 6.4.3 is no longer vulnerable to the following CVE references: • CVE-2020-9497 • CVE-2020-9498

Known issues

The following issues have been identified in version 6.4.3. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
752420	If a .TAR.BZ2 or .TAR.GZ archive contains an archive bomb inside its compressed stream, the AV engine will time out.

Endpoint Control

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

Firewall

Bug ID	Description
666612	Get internet service name configuration error on version 7.01011 when FortiGate reboots or upgrades.
669665	All ISDB groups are lost when upgrading from 6.2.5 to 6.4.2.

FortiView

Bug ID	Description
621453	FortiGate cannot get detailed information on FortiClient vulnerabilities from FortiAnalyzer.
683627	FortiView does not display any data when FortiAnalyzer Cloud is the data source.

GUI

Bug ID	Description
567996	Managed FortiSwitch and FortiSwitch *Ports* pages cannot load when there is a large number of managed FortiSwitches.
602102	Warning message is not displayed when a user configures an interface with a static IP address that is already in use.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.
650708	When the client browser is in a different time zone from the FortiGate, the *Guest Management* page displays an incorrect expiry time for guest users. The CLI returns the correct expiry.
652394	GUI cannot change action for the web-based email category in DNS filter profile.
656668	On the *System* > *HA* page, GUI tooltip for the reserved management interface incorrectly shows the connecting IP address instead of the configured IP address.
662873	Editing the LDAP server in the GUI removes the line `set server-identity-check disable` from the configuration.
663351	Connectivity test for RADIUS server using CHAP authentication always returns failure.
664007	GUI incorrectly displays the warning, *Botnet package update unavailable, AntiVirus subscription not found.*, when the antivirus entitlement is expiring within 30 days. The actual botnet package update still works within the active entitlement duration.
665444	*Log Details* does not resize the log columns and covers existing log columns.
665712	When multiple favorite menus are configured, the new features video pops up after each GUI login, even though user previously selected *Don't show again*.
666999	When editing the *Poll Active Directory Server* page, the configured LDAP server saved in FSSO polling is not displayed. Users must use the CLI to modify the setting.
668020	Disclaimer users are not shown in the user monitor; they must be displayed in the CLI with `diagnose firewall auth list`.
668470	FortiGuard DDNS setting incorrectly displays truncated unique location and empty server selection after saving changes.
672599	After performing a search on firewall *Addresses*, the matched count over total count displayed for each address type shows an incorrect total count number. The search functionality still works correctly.
672906	GUI does not redirect to the system reboot progress page after successfully restoring a configuration.
673478	Some FortiView graphs and drilldown views show empty data due to filtering issue. Affected graphs/views: *Top System Events*, *Top Authentication Failures*, *Policy View*, and *Compromised Host View*.

Bug ID	Description
675170	The *Applications* and *Destinations* tabs on the *Diagnostic and Tools* pane show the same data for different clients on the *WiFi Clients* monitor page.
680805	The list of firewall schedules displays time based on the browser time, even though the global time preference is set to use the FortiGate system time. The *Edit Schedule* page does not have this issue.
682008	On *SSL-VPN Settings* page, the option to send an SSL VPN configuration to a user for FortiClient provisioning does not support showing a domain name for the VPN gateway.
688016	GUI interface bandwidth widget does not show correct data for tunnel interface when ASIC offload is enabled on the firewall policy.
689605	On some browser versions, the GUI displays a blank dialog when creating custom application or IPS signatures. Affected browsers: Firefox 85.0, Microsoft Edge 88.0, and Chrome 88.0.

HA

Bug ID	Description
615001	LAG does not come up after link failed signal is triggered.
677246	Unable to contact TACACS+ server when using HA dedicated management interface in 6.4.3.
678309	Cluster is out of sync because of `config vpn certificate ca` after upgrade.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.

668631	IPS is constantly crashing, and ipshelper has high CPU when IPS extended database has too many rules (more than 256) sharing the same pattern. Affected models: SoC3-based FortiGates.
	Workaround: disable CP or disable the extended database.
	`config ips global`
	`    set database regular`
	`    set cp-accel-mode none`
	`end`

IPsec VPN

Bug ID	Description
652774	OCVPN spoke-to-spoke communication intermittently fails with mixed topology where some spokes have two ISPs and some have one, but the hubs have two.
655895	Unable to route traffic to a spoke VPN site from the hub FortiGate when the dialup IPsec VPN interface is dual stacked (IPv4/IPv6).
663126	Packets for the existing session are still forwarded via the old tunnel after the routing changed on the ADVPN hub.
667129	In ADVPN with SLA mode, traffic does not switch back to the lowest cost link after its recovery.

Log & Report

Bug ID	Description
661040	Cyrillic characters not displayed properly in local reports.

Proxy

Bug ID	Description
657905	Firewall policy with UTM in proxy mode breaks SSL connections in active-active cluster.
684168	WAD process consumes memory and crashes because of a memory leak that happened due to a coding error when calling the FortiAP API. The API misbehaves when there are no FortiAP appliances in the cluster.

Routing

Bug ID	Description
654032	SD-WAN IPv6 route tag command is not available in the SD-WAN services.
669380	Router daemons get stuck after rebooting when executing `get router info routing-table all`.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
666242	Automation stitch CLI scripts fail with greater than 255 characters; up to 1023 characters should be supported.

SSL VPN

Bug ID	Description
670803	Internal website, http://gd***.local/share/page?pt=login, log in page does not load in SSL VPN web mode.
675878	When matching multiple SSL VPN firewall policies, SSL VPN checks the group list from bottom to top, and the user is mapped to the incorrect portal.
684012	SSL VPN crashed with signal 11 (segmentation fault) `uri_search` because of rules set for a special case.

Switch Controller

Bug ID	Description
671135	flcfg crashes while configuring FortiSwitches through FortiLink.

System

Bug ID	Description
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
630861	Support FortiManager when `private-data-encryption` is enabled in FortiOS.
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
651103	FG-101F crashed and rebooted when adding `vlan-protocol 8021ad` VLAN.
657629	ARM-based platforms do not have sensor readings included in SNMP MIBs.

Bug ID	Description
662681	Policy package push from FortiManager fails the first time, and succeeds the second time if it is blank or has no changes.
663083	Offloaded traffic from IPsec crossing the NPU VDOM link is dropped.
666030	Empty firewall objects after pushing several policy deletes.
666205	High CPU on L2TP process caused by loop.

User & Authentication

Bug ID	Description
643583	`radius-vdom-override` and `accprofile-override` do not work when administrator has 2FA enabled.
682394	FortiGate is unable to verify the CA chain of the FSSO server if the chain is not directly rooted to FSSO endpoint.

VM

Bug ID	Description
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
617046	FG-VMX manager not showing all the nodes deployed.
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
669822	Hot adding multiple CPUs at once to Xen-flavored VMs can result in a kernel panic crash. **Workaround**: add one CPU at a time. Alternatively, shut down the VM, add the CPUs, and restart the VM.
671279	FG-VM64-AZURE-PAYG license/serial number get lost after downgrading to 6.2.6 from 6.4.3.
672312	Azure SDN connector does not offer all service tags.

WiFi Controller

Bug ID	Description
643854	Client traffic was dropped by CAPWAP offloading when it connected from a mesh leaf Forti-AP managed by a FWF-61F local radio.

672920	CAPWAP tunnel traffic is dropped when offloading is enabled (with FAP managed by a VLAN interface). There are three workarounds:
	• Disable `capwap-offload` in `system npu` and reboot.
	• Set `dtls-policy dtls enabled` in `wireless-controller wtp-profile`. This may cause traffic to slow.
	• Enable UTM in the firewall policy (does not require reboot). This workaround cannot be applied on NP6Xlite FortiGates (FG-6xF and FG-10xF).
	`config firewall policy`
	`    edit <id>`
	`        set utm-status enable`
	`        set ssl-ssh-profile "certificate-inspection"`
	`        set av-profile "g-default"`
	`    next`
	`end`

673211	CAPWAP traffic drops on FG-300E when FortiAP is managed by VLAN interface.
674342	The cw_acd crashes after upgrading to 6.4.3 at cwAcLocal.

Built-in AV engine

Resolved engine issues

Bug ID	Description
632769	Fixed UTF-8 characters not displaying properly after archive extraction.
637845	Fixed AV engine inability to properly scan files containing gfxdata payloads.
648561	Fixed AV engine PDF parser crash.
652492	Fixed AV engine crashing when large files are scanned.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
539833	Fix invalid memory access crashes in HTTP fake body.
624928	Fix memory leaks in PCRE pattern extractor.
625371	Fix crash on derived packet processing.
637084	Use existing private keys in FortiGate for certificate resigning.
645848	Turn off SNI verification via the existing CLI in SSL-SSH profile.
647330	Use integer instead of lightuserdata to avoid bad lightuserdata pointer.
648079	Support virus URL cache for DLP sensor.
657466	Local URL filter configuration in flow mode web filter does not work when the matching FortiGuard category is also enabled in the web filter profile.
658482	High memory usage by ipsmonitor and ipsengine processes.
660489	Web filter URL filter check is skipped in flow mode certificate inspection if SNI is not present in the TLS client hello.
662573	Fix NULL pointer dereference crash.
662785	Signatures for services other than SSL traffic with the drop action are showing as detected for SSL traffic.
662964	PCAP from IPS not dumped as configured in `packet-log-history` and `packet-log-post-attack` settings.
664728	Traffic failing in NGFW policy-based mode when TCP source port range includes a zero value.

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.

FORTINET®