FortiOS - Release Notes

Version 6.4.4

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

December 11, 2020
FortiOS 6.4.4 Release Notes
01-644-677813-20201211

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-12-10	Initial release.
2020-12-11	Updated Introduction and supported models on page 6.

Introduction and supported models

This guide provides release information for FortiOS 6.4.4 build 1803.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.4 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-101E, 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 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

The FGR-60F and FGR-60F-3G4G will be released as special branches at a later date.

Special branch supported models

The following models are released on a special branch of FortiOS 6.4.4. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1803.

FG-80F	is released on build 5535.
FG-80F-BP	is released on build 5535.

FG-81F	is released on build 5535.
FG-100F	is released on build 5540.
FG-101F	is released on build 5540.

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.

FortiClient EMS Cloud registration

FortiOS 6.4.3 adds full support for FortiClient EMS Cloud service. Users will be able to register and use the service by mid-December 2020.

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`.

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`:

- There is no change to the behavior. The reply traffic will egress on the original incoming interface.

Changes in CLI

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>666855</td><td>FortiOS supports verifying client certificates with RSA-PSS series of signature algorithms, which causes problems with certain clients.
Add attribute to control signature algorithms related to client authentication (only affects TLS 1.2):
<pre>config vpn ssl settings
    set client-sigalgs {no-rsa-pss | all}
end</pre></td></tr>
</table>

Changes in default behavior

Bug ID	Description
537354	Interface egress shaping offloads to NPU when `shaping-offload` is set to `enable`.

New features or enhancements

More detailed information is available in the New Features Guide.

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>618359</td><td>In scenarios where the FortiGate is sandwiched by load-balancers and SSL processing is offloaded on the external load-balancers, the FortiGate can perform scanning on the unencrypted traffic by specifying the ssl-offloaded option in firewall profile-protocol-options. Previously, this was only supported in proxy mode. Now it is supported in proxy and flow mode.</td></tr>
<tr><td>641524</td><td>

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
```

</td></tr>
<tr><td>648602</td><td>When creating a Cisco ACI direct connector, configuring multiple IPs allows the FortiGate to connect to the server in a round-robin fashion. Only one server will be active, and the remaining IPs will serve as backups if the active one fails.</td></tr>
<tr><td>654032</td><td>The route-tag is a mechanism to map a BGP community string to a specific tag. The string may correspond to a specific network that a BGP router advertised. With this tag, an SD-WAN service rule can be used to define specific traffic handling to that network. IPv6 route tags are now supported.</td></tr>
<tr><td>660295</td><td>Provide specific SNMP objects (OIDs) that allow the status of the mobile network connection to be monitored.</td></tr>
<tr><td>661252</td><td>

Add object synchronization improvements:

- Simplify the conflict resolution procedure so a multi-step wizard is no longer required. All conflicts appear in one table for all FortiGates in the Fabric and supported tables.
- Add an object diff feature to display the difference between FortiGate objects that are in conflict.
- Add new CLI command for the root FortiGate:

  ```
  config system csf
      set fabric-object-unification {default | local}
  end
  ```

  When set to default, objects will be synchronized in the Security Fabric. On downstream FortiGates, if configuration-sync is set to local, the synchronized objects from the root to downstream FortiGates is not applied locally. However, the device will still send the configuration to lower FortiGates.

</td></tr>
</table>

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td></td><td>• The fabric-object {enable | disable} command was added to the following tables:
  • firewall.address
  • firewall.address6
  • firewall.addrgrp
  • firewall.addrgrp6
  • firewall.service.category
  • firewall.service.group
  • firewall.service.custom
  • firewall.schedule.group
  • firewall.schedule.onetime
  • firewall.schedule.recurring
Enabling fabric-object on the root starts synchronizing this object as a Fabric object to downstream devices. Disabling fabric-object makes the object local to the device.
• Add setting to define how many task worker process are created to handle synchronizations (1 - 4, default = 2). The worker processes dies if there is no task to perform after 60 seconds.
config system csf
    set fabric-workers <integer>
end</td></tr>
<tr><td>676063</td><td>Add support for OCI IMDSv2 that offers increased security for accessing instance metadata compared to IMDSv1. IMDSv2 is used in OCI SDN connectors and during instance deployments with bootstrap metadata.</td></tr>
</table>

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*.

In 6.4.4, a new sub-option, *Delete*, was added when right-clicking on the device. This option is not available when the device is online, or the device is retrieved from FortiClient.

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

- FortiAnalyzer 6.4.4
- FortiManager 6.4.4
- 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 6.4.4. When Security Fabric is enabled in FortiOS 6.4.4, all FortiGate devices must be running FortiOS 6.4.4.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.4 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 6.4.4 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 6.4.4 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 6.4.4 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	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 6.4.4, 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 6.4.4.

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 select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *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
```

WanOpt and web cache statistics

The statistics for WanOpt and web cache have moved from *Monitor* to a widget in *Dashboard*.

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` before upgrade.

Product integration and support

The following table lists FortiOS 6.4.4 product integration and support information:

Web Browsers	• Microsoft Edge • Mozilla Firefox version 83 • Google Chrome version 87 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 16. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 6.4.4 must work with FortiManager 6.4.1 or later. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 16. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 16 and Fortinet Security Fabric upgrade on page 16. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiClient EMS	• 6.4.0
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	- 3.6.9 and later
FortiController	- 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	- 2.3.3 and later
Fortinet Single Sign-On (FSSO)	- 5.0 build 0295 and later (needed for FSSO agent support OU in group filters) - Windows Server 2019 Standard - Windows Server 2019 Datacenter - Windows Server 2019 Core - Windows Server 2016 Datacenter - Windows Server 2016 Standard - Windows Server 2016 Core - Windows Server 2012 Standard - Windows Server 2012 R2 Standard - Windows Server 2012 Core - Windows Server 2008 64-bit (requires Microsoft SHA2 support package) - Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) - Windows Server 2008 Core (requires Microsoft SHA2 support package) - Novell eDirectory 8.8
FortiExtender	- 3.2.1
AV Engine	- 6.00154
IPS Engine	- 6.00064
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 83 Google Chrome version 87
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 83 Google Chrome version 87
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 68
macOS Big Sur 11.0	Apple Safari version 14 Mozilla Firefox version 83 Google Chrome version 87
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 6.4.4. For inquires about a particular bug, please contact Customer Service & Support.

DNS Filter

Bug ID	Description
653581	Cannot pass DNS traffic through FortiGate or DNS traffic originated from FortiGate when external blocklist (threat feed) is updated.

Endpoint Control

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

Explicit Proxy

Bug ID	Description
662931	Browsers change default `SameSite` cookie settings to `Lax`, and Kerberos authentication does not work in transparent proxy.
664548	When the FortiGate is configured as an explicit proxy and AV is enabled on the proxy policy, users cannot access certain FTP sites.

File Filter

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

Firewall

Bug ID	Description
651321	`sflowd` is crashing due to invalid custom application category.
653828	When web filter and application control are configured, blocked sessions to play.google.com remain in the session table for 3600 seconds.
661777	Source NAT port reuses ports too quickly, and GCP/API fails to establish due to endpoint independence conflict.
665739	HTTP host virtual server does not work well when real server has the same IP but a different port.
666612	Get internet service name configuration error on version 7.01011 when FortiGate reboots or upgrades.
667696	Reputation settings in policies not working as expected.
669665	All ISDB groups are lost when upgrading from 6.2.5 to 6.4.2.

GUI

Bug ID	Description
490396	System administrator account profile overwrite does not work in the GUI if the remote administrator has 2FA enabled (CLI is OK).
567996	Slow load times for the *Managed FortiSwitch* and *FortiSwitch Ports* pages when there is a large number of 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.
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.
665444	Columns for log details do not resize, and they cover existing columns.
666500	The *Confirm version downgrade* option is not displayed after uploading a previous version's firmware file.
668020	Support displaying disclaimer users in the *Firewall Users* widget.
672906	GUI does not prompt system reboot progress page after successfully restoring configuration.
675170	In the *WiFi Clients* drilldown, applications and destinations are same for two different stations.
680541	The `logtype_mask` filter in the IoC drilldown is not support on the FortiAnalyzer side.

HA

Bug ID	Description
615001	LAG does not come up after link failed signal is triggered.
650624	HA GARP sending was delayed due to lots of transceiver reading
653095	Inband management IP connection breaks when failover occurs (only in virtual cluster setup).
677246	Unable to contact TACACS+ server when using HA dedicated management interface in 6.4.3.

Intrusion Prevention

Bug ID	Description
671322	IPS engine reloads, or FortiGate reboots and displays CMDB `__bsearch_index()` duplicate value insertion errors.

IPsec VPN

Bug ID	Description
566076	IKED process signal 11 crash in an ADVPN and BGP scenario.
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.
663648	BGP over dynamic IPsec VPN tunnel with `net-device enable` not passing through traffic after rebooting.
667129	In ADVPN with SLA mode, traffic does not switch back to the lowest cost link after its recovery.
673258	FortiGate to Cisco IKEv2 tunnel randomly disconnects after rekey.

Log & Report

Bug ID	Description
587916	Logs for local-out DNS query timeout should not be in the DNS filter UTM log category.
670741	Unable to configure syslog filter data size more then 512 characters.

Proxy

Bug ID	Description
657905	Firewall policy with UTM in proxy mode breaks SSL connections in active-active cluster.
661063	If a client sends an RST to a WAD proxy, the proxy can close the connection to the server. In this case, the relatively long session expiration (which is usually 120 seconds by default) could lead to session number spikes in some tests.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
628896	DHCP relay should follow SD-WAN rules.
654032	SD-WAN IPv6 route tag command is not available in the SD-WAN services.
659409	FortiGate blocks IPv6 but allows IPv4 for traffic that looks asymmetric with `asymroute` is disabled.
663396	SD-WAN route changes and packet drops during HTTP communication, even though `preserve-session-route` is enabled.
667469	SD-WAN members and OIFs keep reordering despite the health check status being stable.
668982	Possible memory leak when BGP table version increases.
670017	FortiGate as first hop router sometimes does not send register messages to the RP.
673603	Only the interface IP in the management VDOM can be specified as the health check source IP.
675442	Weight-based load-balance algorithm causes local-in reply traffic egress from wrong interface.
676685	VRRP does not consider VRF when looking up destination in routing table.

Security Fabric

Bug ID	Description
660624	FortiAnalyzer Cloud should be taken into consideration when doing CLI check for CSF setting.
666242	Automation stitch CLI scripts fail with greater than 255 characters; up to 1023 characters should be supported.
669436	Filter lookup for Azure connector in subnet and virtual network does not show all results.

SSL VPN

Bug ID	Description
586035	The policy `script-src 'self'` will block the SSL VPN proxy URL.
615453	WebSocket using Socket.IO could not be established through SSL VPN web mode.
646339	SSL-SSH inspection profile changes to `no-inspection` after device reboots.
653349	SSL VPN web mode not working for Ec***re website.
661290	https://mo***.be site is non-accessible in SSL VPN web mode.
662871	SSL VPN web mode has problem accessing some pages on FortiAnalyzer 6.2.
664276	SSL VPN host check validation not working for SAML user.
665330	SDT application can no longer load secondary menu elements in SSL VPN web mode.
665408	Occasionally, 2FA SSL VPN users are unable to log in when two remote authentication servers with the same IP are used.
666855	FortiOS supports verifying client certificates with RSA-PSS series of signature algorithms, which causes problems with certain clients.
667780	Policy check cache should include user or group information.
667828	SSL VPN web mode authentication problem when accessing li***.com.
668574	Unable to load a video in SSL VPN web mode
669144	HTTPS access to ERP Sage X3 through web mode fails.
669497	Cannot view TIFF files in SSL VPN web mode.
669685	Split tunneling is not adding FQDN addresses to the routes.
669707	The jstor.org webpage is not loading via SSL VPN bookmark.
670042	Internal website, http://si***.ar, does not load a report over SSL VPN web portal.
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.
676345	SSL VPN web mode is unable to open some webpages on the internal site, https://vi***.se, portal.
677167	SSL VPN web mode has problem accessing Sapepronto server.

Switch Controller

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

System

Bug ID	Description
521213	Read-only administrators should be able to run `diagnose sniffer packet` command.
606360	HQIP loopback test failed with configured software switch.
627236	TCP traffic disruption when traffic shaper takes effect with NP offloading enabled.
630861	Support FortiManager when `private-data-encryption` is enabled in FortiOS.
634202	STP does not work in transparent mode.
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
651420	Add support for `interface-shaping-offload` under `system npu` on SoC3 and SoC4 models.
657629	FG-101F cannot retrieve power fan status and BGP status via SNMP.
660709	The sflowd process has high CPU usage when application control is enabled.
662681	Policy package push from FortiManager fails the first time, and succeeds the second time if it is blank or has no changes.
662687	Asynchronous SDK call may take a long time and cause HA A-P to have `Kernel panic - not syncing` error.
663083	Offloaded traffic from IPsec crossing the NPU VDOM link is dropped.
664268	No `filename` setting on BOOTP response when option 67 is set on the DHCP server.
664478	Kernel crash caused race condition on `vlif` accessing.
666030	Empty firewall objects after pushing several policy deletes.
666205	High CPU on L2TP process caused by loop.
666852	FortiGate local-out system DNS traffic for host names lookup continuously generates timeout DNS log if the primary server cannot resolve them.
668410	NP6lite SoC3 adapter drops packets after handed from kernel.
670838	It takes a long time to set the member of a firewall address group when the member size is large. In the GUI, cmdbsvr memory usage goes to 100%. In the CLI, newcli memory usage goes to 100%.

Bug ID	Description
673263	High memory issue is caused by heavy traffic on the VDOM link.
673918	Read-only administrator with packet capture read-write permission cannot run `diagnose sniffer` command.
675418	FortiManager CLI script for 2FA FortiToken mobile push does not trigger activation code email.

User & Authentication

Bug ID	Description
643583	`radius-vdom-override` and `accprofile-override` do not work when administrator has 2FA enabled.
658794	FortiGate sent CSR certificate instead of signed certificate to FortiManager when retrieve is performed.
663685	The authd process truncates user names to a length of 35 characters (this breaks RADIUS accounting and logging for very long user names).
665391	The authd process gets stuck with high CPU due to slow route lookup when the routing table is big. FSSO stops processing new authentication events.
666268	The authd process may crash if the FSSO server connection is disconnected.

VM

Bug ID	Description
641038	SSL VPN performance problem on OCI due to driver.
656701	FG-VMX service manager enters conserve mode; cmdbsvr has high memory utilization.
659333	Slow route change for HA failover in GCP cloud.
669822	Hot adding multiple CPUs at once to Xen-flavored VMs can result in a kernel panic crash.
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).
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.
680503	The current Fortinet_Wifi certificate will expire on 2021-02-11.

Known issues

The following issues have been identified in version 6.4.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Explicit Proxy

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

Firewall

Bug ID	Description
667772	When NGFW mode is set to policy mode and a security policy is configured, the Quard daemon should start when either an anti-virus, web filter, application, IPS, or DLP profile is enabled.

FortiView

Bug ID	Description
628225	*Compromised Hosts* has error 500 when FQDN is set in `config log fortianalyzer setting`.
683413	Some FortiView pages/widgets fail to query data from FortiAnalyzer Cloud if the local FortiAnalyzer is not enabled. Affected pages/widgets: *Compromised Hosts*, *FortiView Cloud Applications*, *FortiView VPN*, *FortiView Web Categories*, *Top Admin Logins*, *Top Endpoint Vulnerabilities*, *Top Failed Authentication*, *Top System Events*, *Top Threats*, *Top Threats - WAN*, and *Top Vulnerable Endpoint Devices*.

GUI

Bug ID	Description
602397	FortiSwitch port page is noticeably slow for large topology.
665111	Unable use break function or other add a line break when editing replacement messages in the GUI.
673496	Red highlight appears when attempting to save phase 2 configurations using the *Complete Section* button.
676165	Script pushed from FortiManager 6.4.2 to FortiOS 6.4.2 to add address objects and address group succeeds. FortiOS GUI shows the new address group as empty.

HA

Bug ID	Description
540600	The HA `hello-holddown` value is divided by 10 in the hatalk daemon, which makes the `hello-holddown` time 10 times less than the configuration.
653642	FortiGate HA failover from FortiManager is not successful.
675781	HA cluster goes out of sync with new custom DDNS entry, and changes with respect to the `ddns-key` value.

Intrusion Prevention

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

IPsec VPN

Bug ID	Description
642543	IPsec did not rekey when keylife expired after back-to-back HA failover.
644780	Rectify the consequences if we cancel password renewal is canceled on FortiClient.

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.
670025	IKEv2 `fragmentation-mtu` option is not respected when EAP is used for authentication.
673049	FortiGate not sending its external interface IP in the IKE negotiation (Google Cloud Platform).

Log & Report

Bug ID	Description
661040	Cyrillic characters not displayed properly in local reports.
667274	FortiGate does not have log disk auto scan failure status log.
675347	In local log search, results returned immediately when there are checked logs.

Proxy

Bug ID	Description
658257	StartTLS-SMTP traffic gets blocked by the firewall when certificate inspection (proxy mode) and the IPS sensor are enabled in a policy.

Routing

Bug ID	Description
672061	In IPsec topology with hub and ~1000 spokes, hundreds of spoke tunnels are flapping, causing BGP instability for other spokes.
677928	SD-WAN with `sit-tunnel` as a member creates an unwanted default route.

SSL VPN

Bug ID	Description
550819	guacd is consuming too much memory and CPU resources during operation.
610995	SSL VPN web mode gets error when accessing internal website at https://st***.st***.ca/.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
555616	When NTurbo is enabled, it is unexpectedly provided with the wrong traffic direction information (from server or from client) to decide the destination for the data. This causes the traffic to be sent back to the port where it came from.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
647309	HA kernel crash at `filter4` module and subsequent loop of `failure at mm/vmalloc.c:1341/__get_vm_area_node()!`.
649937	The `diagnose geoip geoip-query` command fails when `fortiguard-anycast` is disabled.
651103	FG-101F crashed and rebooted when adding `vlan-protocol 8021ad` VLAN.
668856	Offloaded traffic passing through two VDOMs connected with EMAC-VLANs is sometimes dropped.
669951	confsyncd may crash when there is an error parsing through the internet service database, but no error is returned.
672183	UDP 4500 inter-VDOM traffic not offloaded, causing BFD/IPsec to drop.
675508	When provisioning FortiGate and FortiSwitch with enforced 6.4.2 firmware in FortiManager, the physical port for FortiLink is down and cannot connect to the FortiSwitch.

User & Authentication

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW.

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).

Bug ID	Description
646161	FG-VM8 does not recognize all memory allocated in Hyper-V.
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
682420	Dialup IPsec tunnel from Azure may not be re-established after HA failover.

Web Filter

Bug ID	Description
675436	YouTube channel home page on blocklist is not blocked when directed from a YouTube search result.

WiFi Controller

Bug ID	Description
625630	FWF-60E hangs with looping kernel panic at WiFi driver.
662714	The `security-redirect-url` setting is missing when the `portal-type` is `auth-mac`.
672136	Log severity for wireless events in FortiWiFi and FortiAP should be reconsidered for CAPWAP teardown.
677994	Newly discovered and authorized FortiAP will cause HA sync issue. On the HA secondary member, if the WTP profile has a radio in monitor mode, it will be changed to AP mode and unset the band.

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.