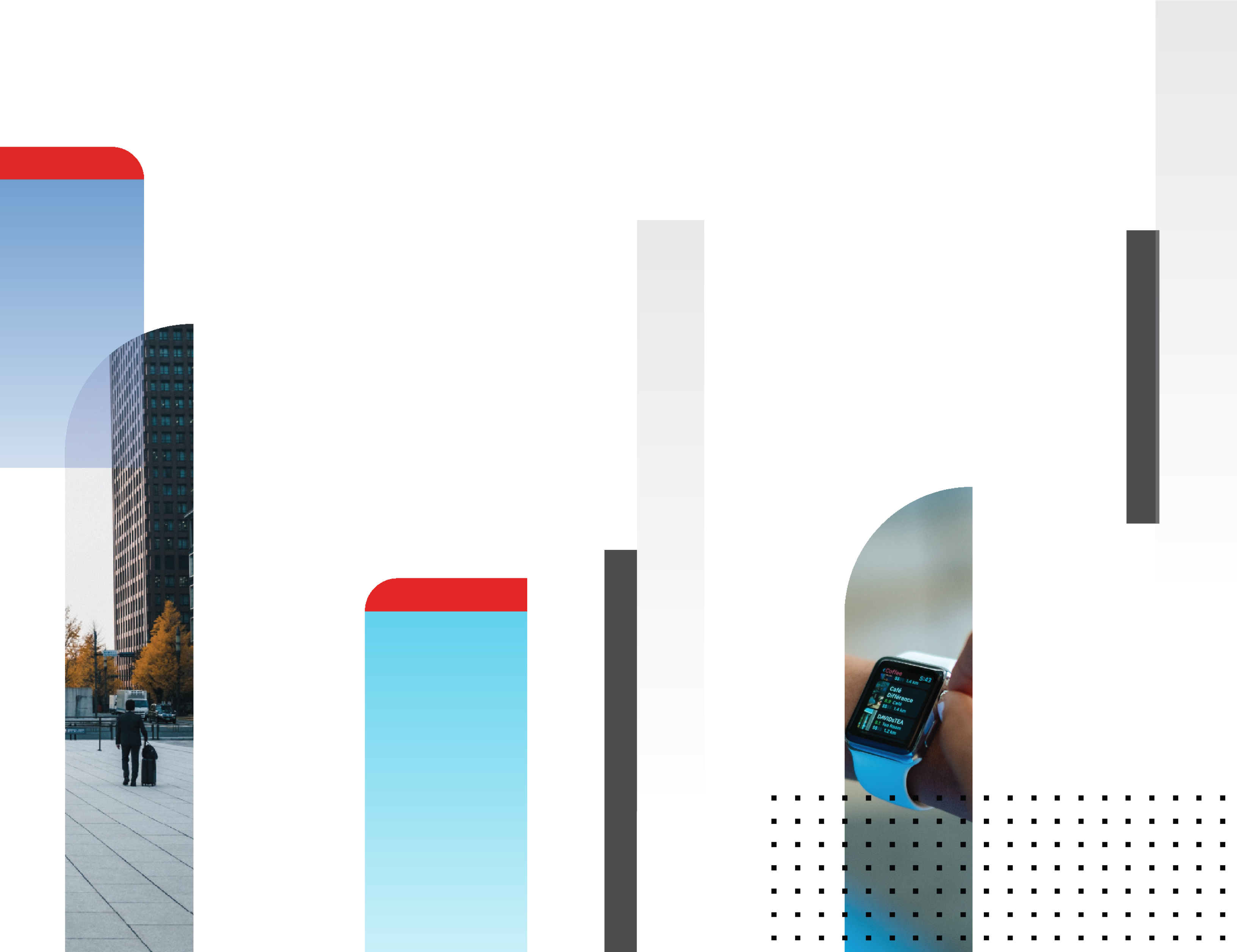
Release Notes

FortiOS 7.0.9



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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

November 22, 2022
FortiOS 7.0.9 Release Notes
01-709-855155-20221122

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-11-22	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.0.9 build 0444.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.9 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-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

Special notices

Azure-On-Demand image

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

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

GCP-On-Demand image

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

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

ALI-On-Demand image

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

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

Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1:

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

FEC feature design change

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

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

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

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

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.0.9 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For more information, refer to the Hyperscale Firewall Release Notes.

Upgrade information

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

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.0.9 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.5
FortiManager	• 7.0.5
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 12
FortiClient* EMS	• 7.0.0 build 0042 or later
FortiClient* Microsoft Windows	• 7.0.0 build 0029 or later
FortiClient* Mac OS X	• 7.0.0 build 0022 or later
FortiClient* Linux	• 7.0.0 build 0018 or later
FortiClient* iOS	• 6.4.6 build 0507 or later
FortiClient* Android	• 6.4.6 build 0539 or later
FortiSandbox	• 2.3.3 and later

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

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

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.9. When Security Fabric is enabled in FortiOS 7.0.9, all FortiGate devices must be running FortiOS 7.0.9.

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

IPsec interface MTU value

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

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

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

HA role wording changes

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

Strong cryptographic cipher requirements for FortiAP

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

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

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

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

How VoIP profile settings determine the firewall policy inspection mode

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

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

If the setting is not manually updated after upgrading, the VPN connection will be established, but it will not be accessible from the internal network (office network). This setting change is necessary regardless of whether route-based or policy-based IPsec is used.

To make L2TP over IPsec work after upgrading:

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

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

   Add a static route after upgrading:

   ```
   config router static
       edit 1
           set dst 210.0.0.0 255.255.255.0
           set device "l2t.root"
       next
   end
   ```

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

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

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

Upgrading

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

The following CLI commands have been removed:

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

The following GUI pages have been removed:

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

During the upgrade process after the FortiGate reboots, the following message is displayed:

```
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log read'
```

The following output is displayed after running the diagnose command:

```
# diagnose debug config-error-log read
>>> "config" "firewall" "policy64" @ root:command parse error (error -
61)
>>> "config" "firewall" "policy46" @ root:command parse error (error -
61)
```

Creating new policies

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

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

Example configurations

`vip46` object:

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

`ippool6` object:

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

NAT46 policy:

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

`vip64` object

Old configuration	New configuration

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

`ippool` object

Old configuration	New configuration

config firewall ippool
    edit "test-ippool4-1"
        set startip 172.16.201.155
        set endip 172.16.201.155
    next
end
	config firewall ippool
	    edit "test-ippool4-1"
	        set startip 172.16.201.155
	        set endip 172.16.201.155
	        set nat64 enable
	    next
	end

NAT64 policy:

Old configuration	New configuration

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

ZTNA configurations and firewall policies

Since FortiOS 7.0.2, ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration.

When upgrading from FortiOS 7.0.1 or below:

- If an `access-proxy` type `proxy-policy` does not have a `srcintf`, then after upgrading it will be set to `any`.
- To display the `srcintf` as *any* in the GUI, *System > Feature Visibility* should have *Multiple Interface Policies* enabled.
- All full ZTNA firewall policies will be automatically removed.

Default DNS server update

If both primary and secondary DNS servers are set to use the default FortiGuard servers prior to upgrading, the FortiGate will update them to the new servers and enable DoT after upgrading. If one or both DNS servers are not using the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

Product integration and support

The following table lists FortiOS 7.0.9 product integration and support information:

Web browsers	• Microsoft Edge • Mozilla Firefox version 105 • Google Chrome version 107 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	• 5.0 build 0304 and later (needed for FSSO agent support OU in group filters) • Windows Server 2022 Standard • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
AV Engine	• 6.00282
IPS Engine	• 7.00142

Virtualization environments

The following table lists hypervisors and recommended versions.

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

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 105 Google Chrome version 107
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 105 Google Chrome version 107
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 105 Google Chrome version 107
macOS Monterey 12.4	Apple Safari version 15 Mozilla Firefox version 105 Google Chrome version 107
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

Resolved issues

The following issues have been fixed in version 7.0.9. To inquire about a particular bug, please contact Customer Service & Support.

Explicit Proxy

Bug ID	Description
805703	FortiGate does not load balance requests evenly when the `ldb-method` is set to `least-session`.

Firewall

Bug ID	Description
834301	Session dropped with timeout action after policy changes.
835413	Inaccurate sFlow interface data reported to PRTG after upgrading to 7.0.
843274	Source interface filter (`srcintf-filter`) is not working with virtual servers.

GUI

Bug ID	Description
719476	FortiLink NAC matched device is displayed in the CLI but not in the GUI under *WiFi & Switch Controller > NAC Policies > View Matched Devices*.
831885	Unable to access GUI via HA management interface of secondary unit.

HA

Bug ID	Description
832634	HA failovers occur due to the kernel hanging on FG-100F.

Bug ID	Description
840954	The HA pair primary keeps sending `fgFmTrapIfChange` and `fnTrapIpChange` after upgrading to 7.0.6.
843907	Session load balancing is not working in HA A-A configuration for traffic flowing via the VLAN interface when the port1 link is down on platforms with a 4.19 kernel.

IPsec VPN

Bug ID	Description
819276	After changing the password policy to enable it, all non-conforming IPsec tunnels were wiped out after rebooting/upgrading.
832920	Unable to edit the parent interface from the IPsec configuration if it was configured on an IPIP tunnel.
840153	Unexpected dynamic selectors block traffic when `set mesh-selector-type subnet` is configured.
840940	Unable to reestablish a new IPsec L2TP connection for 10 minutes after the previous one disconnected. The issue conditions are local in traffic and a policy-based IPsec tunnel.
842528	Improper IKEv1 quick mode fragmentation from third-party client can cause an IKE crash.

Proxy

Bug ID	Description
827807	WAD crash at signal 11 is observed after configuring 250 CGN VDOMs (full offload is enabled in the VDOMs).
837095	WAD daemon runs high with many child processes and is not coming down after configuring 250 CGN VDOMs.

Routing

Bug ID	Description
817670	IPv6 route redistribution metric value is not taking effect.
833800	The `speed-test-server` list cannot be loaded due to limited buffer size.

Bug ID	Description
836077	IPv6 SD-WAN health check is not working after a disconnection.
840691	FortiGate as an NTP server is not using SD-WAN rules.

Security Fabric

Bug ID	Description
837347	Upgrading from 6.4.8 to 7.0.5 causes SDN firewall address configurations to be lost.
843043	Only the first ACI SDN connector can be kept after upgrading from 6.4.8 if multiple ACI SDN connectors are configured.

SSL VPN

Bug ID	Description
705880	Updated empty group with SAML user does not trigger an SSL VPN firewall policy refresh, which causes the SAML user detection to not be successful in later usage.
808569	sslvpnd crashes when no certificate is specified.
808634	SSL VPN daemon sometimes could not be recovered, even when setting the server certificate back from empty to a specific certificate.
820536	SSL VPN web mode bookmark incorrectly applies a URL redirect.
822432	SSL VPN crashes after copying a string to the remote server using the clipboard in RDP web mode when using RDP security.
856316	Browser displays an *Error, Feature is not available* message if a file larger than 1 MB is uploaded from FTP or SMB using a web bookmark, even though the file is uploaded successfully. There are no issues with downloading files.

System

Bug ID	Description
798992	Get newcli crash when running the `diagnose hardware test memory` command.
827736	As the size of the internet service database expands, `ffdb_err_msg_print: ret=-4, Error: kernel error` is observed frequently on 32-bit CPU platforms, such as the FG-100E.

Bug ID	Description
831486	HQIP memory test failed and triggered a log out with a newcli process crash.
844316	IPS and application control is causing the FortiGate (VWP) to change either the source MAC address or the destination MAC address based on the flow.
844908	Outbandwidth does not control traffic properly on platforms with a 4.19 kernel when VDOM links are used.
844937	FG-3700D unexpectedly reboots after the COMLog reported a kernel panic due to an IPv6 failure to set up the master session for the expectation session under some conditions.
850430	DHCP relay does not work properly with two DHCP relay servers configured.
855151	There may be a race condition between the CMDB initializing and the customer language file loading, which causes the customer language file be removed after upgrading.

VM

Bug ID	Description
848279	SFTP backup not working with Azure storage account.

Web Application Firewall

Bug ID	Description
838913	The WAF is indicating malformed request false positives caused by incorrect setups of four known headers: Access-Control-Max-Age, Access-Control-Allow-Headers, Access-Control-Allow-Methods, and Origin.

Web Filter

Bug ID	Description
742483	System events logs randomly contain a `msg=UrlBwl-black gzopen fail` message.
847676	`Unrated` is displayed, even if the system language is set to Japanese when the policy inspection mode is set to flow.

WiFi Controller

Bug ID	Description
844172	The cw_acd process is deleting dynamic IPsec tunnels on the secondary device, which causes the FortiAPs to disconnect on the primary device.

Known issues

The following issues have been identified in version 7.0.9. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
818092	CDR archived files are deleted at random times and not retained.

Endpoint Control

Bug ID	Description
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.

Explicit Proxy

Bug ID	Description
823319	Authentication hard timeout is not respected for firewall users synchronized from WAD user.

Firewall

Bug ID	Description
631814	*Static route configuration* should not be shown on address dialog page if the address type is an IP range.
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic.

Bug ID	Description
	Workaround: rename the custom section to unique name between IPv4 and IPv6 policies.
728734	The VIP group hit count in the table (*Policy & Objects* > *Virtual IPs*) is not reflecting the correct sum of VIP members.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. **Workaround**: use Chrome, Edge, or Safari as the browser.
755177	When upgrade firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
810225	An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
818426	Unable to add spokes or retrieve the configuration key from ADVPN.
853352	On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
777394	The flip timer does not start counting down when there is a ping sever failure following a previous outage.
810175	`set admin-restrict-local` is not working for SSH.
810286	FGSP local sessions exist after rebooting an HA pair with A-P mode, and the HW SSE/session count is incorrect.
811535	HA failure occurs on pair of FG-2600s due to packet loss on heartbeat interface.
813207	Virtual MAC address is sent inside GARP by the secondary unit after a reboot.
831051	A port with a disabled status still shows in the GUI as being up. The device information in the CLI also shows the `Admin` and `link_status` as up.
839549	Secondary FortiGate unit in an HA cluster enters conserve mode due to high memory consumption by node scripts.

Hyperscale

Bug ID	Description
763966	FGSP synchronizes NP sessions of all VDOMs when syncvd is only set for hyperscale VDOM.
782674	A few tasks are hung on issuing `stat verbose` on the secondary device.
795853	VDOM ID and IP addresses in the IPL table are incorrect after disabling EIF/EIM.
807476	After packets go through host interface TX/RX queues, some packet buffers can still hold references to a VDOM when the host queues are idle. This causes a VDOM delete error with `unregister_vf`. If more packets go through the same host queues for other VDOMs, the issue should resolve by itself because those buffers holding the VDOM reference can be pushed and get freed and recycled.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.
836976	Traffic impact on changing from log to hardware to log to host during runtime (with PPA enabled).
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
839958	`service-negate` does not work as expected in a hyperscale deny policy.
841712	The `nat64-force-ipv4-packet-forwarding` command is missing under `config system npu`.

Bug ID	Description
842008	After HA failover, session count cannot synchronize on secondary FortiGate.
842659	`srcaddr-negate` and `dstaddr-negate` are not working properly for IPv6 traffic with FTS.
843132	After dynamically adding an ACL policy, the existing matched session is not cleared immediately.
843197	Output of `diagnose sys npu-session list`/`list-full` does not mention policy route information.
843266	Diagnose command should be available to show `hit_count`/`last_used` for policy route and NPU session on hyperscale VDOM.
843305	Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up.
844421	The `diagnose firewall ippool list` command does not show the correct output for overload type IP pools.
846520	NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover.

Intrusion Prevention

Bug ID	Description
813727	Custom signatures are not shown in the list when filters (server, client, or critical severity) are applied in an IPS sensor.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
822651	NP dropping packet in the incoming direction for FG-200F.

Log & Report

Bug ID	Description
820940	On the *Log Settings* page, a VDOM administrator can force a FortiCloud log out of for all VDOMs.

Proxy

Bug ID	Description
727629	WAD encounters signal 11 crash at `wad_http_marker_uri`.
836101	WAD memory leak occurs.
837724	WAD crash at `wad_port_general_update_dctx`.

Routing

Bug ID	Description
618684	Static route will still in routing table after HA failover, and the BFD is down on the new primary.
847037	FortiGate is sometimes not following the policy route to forward traffic and sens unreasonable ARP requests.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
794703	Security Rating report for *Rogue AP Detection* and *FortiCare Support* checks show incorrect results.
825291	FortiAnalyzer connection security rating fails for FortiAnalyzer Cloud.

SSL VPN

Bug ID	Description
719740	The *No SSL-VPN policies exist* warning should not be shown in the GUI when a zone that has ssl.root as a member is set in an SSL VPN policy.
746230	SSL VPN web mode cannot display certain websites that are internal bookmarks.
803576	Comments in front of `<html>` tag are not handled well in HTML file in SSL VPN web mode.

Switch Controller

Bug ID	Description
813216	FortiLink goes down when CAPWAP offloading is enabled or disabled.
818116	Add link status to managed FortiSwitch switch ports.

System

Bug ID	Description
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.
743831	When global daylight saving time (DST) is disabled, the system time in the GUI still shows the time with DST.
784169	When a virtual switch member port is set to be an alternate by STP, it should not reply with ARP; otherwise, the connected device will learn the MAC address from the alternate port and send subsequent packets to the alternate port.
799487	The debug zone uses over 400 MB of RAM.
813162	Kernel panic occurs after traffic goes through IPsec VPN tunnel and EMAC VLAN interface.
818452	The `ifLastChange` SNMP OID only shows zeros.
818795	Kernel panic observed on FG-3700D.
827240	Unexpected reboot occurs on FG-100F.
847314	NP7 platforms may encounter random kernel crash after reboot or factory reset.
847664	Console may display `mce: [Hardware Error]` error message after fresh image burn or reboot.
850683	Console keeps displaying `bcm_nl.nr_request_drop ...` after the FortiGate reboots because of the `cfg-save revert` setting under `config system global`. Affected platforms: FG-10xF and FG-20xF.
850688	FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs.
855573	False alarm of the PSU2 occurs with only one installed.

Upgrade

Bug ID	Description
792831	`[2062] fap_fsw_lst_req: buf of https is too small: 853` debug message appears in console when upgrading to certain builds.
850691	The `endpoint-control fctems` entry `0` is added after upgrading from 6.4 to 7.0.8 when the FortiGate does not have EMS server, which means the `endpoint-control fctems` feature was not enabled previously. This leads to a FortiManager installation failure. **Workaround**: upgrade from FortiOS 6.4.x to 7.0.7 and then 7.0.8. If you have already upgraded to FortiOS 7.0.8, reboot the FortiGate to automatically set `endpoint-control fctems` to `1`.

User & Authentication

Bug ID	Description
765184	RADIUS authentication failover between two servers for high availability does not work as expected.
813969	SAML SSO login for VDOM administrator still works when logging in to the FortiGate and the connecting interface does not belong to that VDOM.
836082	LLDP packets are not being received if mgmt is used as an HA management reservation interface.
846683	Downloading the CSR certificate from global with a custom account profile (read/write) causes GUI/CLI errors due to unauthorized requests.

WAN Optimization

Bug ID	Description
728861	HTTP/HTTPS traffic cannot go through when `wanopt` is set to manual mode and an external proxy is used. **Workaround**: set `wanopt` to automatic mode, or `set transparent disable` in the `wanopt profile`.

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

ZTNA

Bug ID	Description
832508	The EMS tag name (defined in the EMS server's *Zero Trust Tagging Rules*) format changed in 7.0.8 from `FCTEMS<serial_number>_<tag_name>` to `EMS<id>_ZTNA_<tag_name>`. After upgrading, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled. **Workaround**: unset the `ztna-ems-tag` in the ZTNA firewall proxy policy, and then set it again.
848222	ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type. An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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

www.fortinet.com