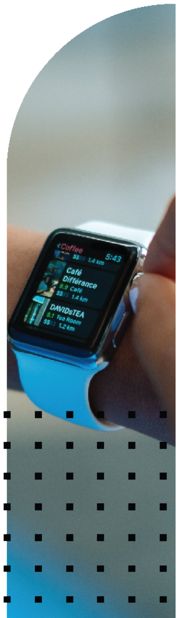
Release Notes

FortiOS 7.0.5



March 6, 2024
FortiOS 7.0.5 Release Notes
01-705-779589-20240306

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-02-09	Initial release.
2022-02-14	Updated Fortinet Security Fabric upgrade on page 12 and Known issues on page 24.
2022-02-22	Updated Known issues on page 24. Added Built-in IPS Engine on page 31.
2022-02-28	Updated Known issues on page 24.
2022-03-07	Updated Known issues on page 24.
2022-03-14	Updated Known issues on page 24.
2022-03-29	Updated Resolved issues on page 23 and Known issues on page 24.
2022-04-01	Updated Known issues on page 24.
2022-04-05	Updated Introduction and supported models on page 7.
2022-05-10	Added CAPWAP offloading compatibility of FortiGate NP7 platforms on page 10. Updated Known issues on page 24.
2022-05-16	Updated Known issues on page 24.
2022-05-30	Updated Known issues on page 24.
2022-06-09	Updated 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 on page 15.
2022-06-13	Updated Known issues on page 24.
2022-06-16	Updated 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 on page 15 and Add interface for NAT46 and NAT64 to simplify policy and routing configurations on page 16.
2022-06-22	Updated Introduction and supported models on page 7.
2022-06-27	Updated Known issues on page 24.
2022-07-11	Updated Known issues on page 24.
2022-07-25	Updated Known issues on page 24.
2022-08-08	Updated Known issues on page 24.
2022-08-29	Updated Product integration and support on page 20.
2022-09-06	Updated Known issues on page 24.
2022-09-21	Updated Known issues on page 24.
2022-10-03	Updated Known issues on page 24.

Date	Change Description
2022-10-17	Updated Known issues on page 24.
2022-10-24	Updated Known issues on page 24.
2022-11-02	Updated Known issues on page 24.
2022-11-14	Updated Known issues on page 24.
2022-11-29	Updated Known issues on page 24.
2022-12-12	Updated Known issues on page 24.
2023-01-09	Updated Known issues on page 24.
2023-02-21	Updated Known issues on page 24.
2023-03-06	Updated Known issues on page 24.
2023-04-04	Updated Known issues on page 24.
2023-04-17	Updated Known issues on page 24.
2023-05-02	Updated Known issues on page 24.
2023-05-15	Updated How VoIP profile settings determine the firewall policy inspection mode on page 15.
2023-05-17	Updated Known issues on page 24.
2023-05-29	Updated Known issues on page 24.
2023-06-14	Added IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10.
2023-08-08	Updated Known issues on page 24.
2023-08-22	Updated Known issues on page 24.
2023-09-06	Updated Known issues on page 24, Built-in AV Engine on page 30, and Built-in IPS Engine on page 31.
2023-10-17	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10.
2024-02-13	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10.
2024-03-06	Updated Known issues on page 24.

Introduction and supported models

This guide provides release information for FortiOS 7.0.5 build 0304.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.5 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 7.0.5. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0304.

FG-70F	is released on build 4530.
FG-71F	is released on build 4530.
FG-1800F	is released on build 4515.
FG-1801F	is released on build 4515.
FG-2600F	is released on build 4515.

FG-2601F	is released on build 4515.
FG-3000F	is released on build 4512.
FG-3001F	is released on build 4512.
FG-3500F	is released on build 4515.
FG-3501F	is released on build 4515.
FG-4200F	is released on build 4515.
FG-4201F	is released on build 4515.
FG-4400F	is released on build 4515.
FG-4401F	is released on build 4515.

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 and later:

- 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 and later.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms running FortiOS 7.0.1 and later, 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.

IP pools and VIPs are not considered local addresses for certain FortiOS versions

For FortiOS 6.4.9 and later, 7.0.1 to 7.0.12, 7.2.0 to 7.2.5, and 7.4.0, all IP addresses used as IP pools and VIPs are not considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is not considered a destination for those IP addresses and cannot receive reply traffic at the application layer without special handling.

- This behavior affects FortiOS features in the application layer that use an IP pool as its source IP pool, including SSL VPN web mode, explicit web proxy, and the phase 1 local gateway in an interface mode IPsec VPN.
- The FortiGate will not receive reply traffic at the application layer, and the corresponding FortiOS feature will not work as desired.
- Configuring an IP pool as the source NAT IP address in a regular firewall policy works as before.

For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

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.

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

FortiAnalyzer	• 7.0.2
FortiManager	• 7.0.2
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 14
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
19. FortiTester
20. FortiMonitor

⚠ If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.5. When Security Fabric is enabled in FortiOS 7.0.5, all FortiGate devices must be running FortiOS 7.0.5.

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, go to *Support > Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *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 and later 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.

In the case when customers are using the following settings in 6.4:

```
config system settings
    set default-voip-alg-mode proxy-based
end
```

```
config firewall policy
    edit 0
        set inspection-mode flow
        unset voip-profile
    next
end
```

In 6.4, by default, SIP traffic is handled by proxy-based SIP ALG even though no VoIP profile is specified in a firewall policy.

After upgrading, the firewall policy will remain in `inspection-mode flow` but handled is by flow-based SIP inspection.

Due to the difference in which the SIP traffic is handled by flow-based SIP versus proxy-based SIP ALG inspection in 7.0.0 and later, if customers want to maintain the same behavior after upgrading, they can manually change the firewall policy's `inspection-mode` to `proxy`:

```
config firewall policy
    edit 0
        set inspection-mode proxy
        unset voip-profile
    next
end
```

Or prior to upgrading, they can assign a `voip-profile` to the firewall policies that are processing SIP traffic to force the conversion to `inspection-mode proxy` 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 and later, 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"	config firewall ippool6 edit "test-ippool6-1"

Old configuration	New configuration
set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end	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	config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155

Old configuration	New configuration
next end	**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

Starting in FortiOS 7.0.4, 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 7.0.5 product integration and support information:

Web browsers	• Microsoft Edge 94 • Mozilla Firefox version 96 • Google Chrome version 97 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 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	• 6.00270
IPS Engine	• 7.00105

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 96 Google Chrome version 97
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 96 Google Chrome version 97
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 96 Google Chrome version 97
macOS Monterey 12.0	Apple Safari version 15 Mozilla Firefox version 96 Google Chrome version 97
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 7.0.5. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
778298	Traffic is blocked when an AV profiled is enabled in proxy inspection mode in an IPsec scenario with NPU offloading enabled.

Firewall

Bug ID	Description
761646	FQDN address and FQDN custom service do not work as expected in security policy.

Proxy

Bug ID	Description
772041	WAD crash at signal 11.
778659	Proxy inspection fails due to `ipsapp session open failed: all providers busy`.

System

Bug ID	Description
778474	dhcpd is not processing discover messages if they contain a 0 length option, such as 80 (rapid commit). The warning, `length 0 overflows input buffer`, is displayed.
779748	When IPS and AV are enabled in flow mode, traffic cannot be redirected to NTurbo in interface-based IPsec scenario.

Known issues

The following issues have been identified in version 7.0.5. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

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.

Firewall

Bug ID	Description
770541	Within the *Policy & Objects* menu, the firewall, DoS, and traffic shaping policy pages take around five seconds to load when the FortiGate cannot reach the FortiGuard DNS servers. **Workaround**: set the DNS server to the FortiGuard DNS server.

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.

Bug ID	Description
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.
713529	When a FortiGate is managed by FortiManager with FortiWLM configured, the HTTPS daemon may crash while processing some FortiWLM API requests. There is no apparent impact on the GUI operation.
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.
777145	*Managed FortiSwitches* page incorrectly shows a warning about an unregistered FortiSwitch even though it is registered. This only impacts transferred or RMAed FortiSwitches. This is only a display issue with no impact on the FortiSwitch's operation. **Workaround**: confirm the FortiSwitch registration status in the FortiCare portal.
787565	When logged in as guest management administrator, the custom image shows as empty on the user information printout. **Workaround**: use the regular *Guest Management* page.

HA

Bug ID	Description
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.
830463	After shutting down the HA primary unit and then restarting it, the uptime for both nodes is zero, and it fails back to the former primary unit.

Hyperscale

Bug ID	Description
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.

Intrusion Prevention

Bug ID	Description
780194	IPS engine 7.00105 has `signal 14 (Alarm clock)` crash during stress testing.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
773221	Traffic that goes through IPsec based on a loopback interface cannot be offloaded.
778243	When `net-device` is enabled on the hub, the tunnel interface IP is missing in the routing table.
810833	IPsec static router gateway IP is set to the gateway of the tunnel interface when it is not specified.
822651	NP dropping packet in the incoming direction for SoC4 models.

Log & Report

Bug ID	Description
776929	When submitting files for sandbox logging in flow mode, `filetype="unknown"` is displayed for PDF, DOC, JS, RTF, ZIP, and RAR files.

Proxy

Bug ID	Description
727629	An error case occurs in WAD while handling the HTTP requests for an explicit proxy policy.
766158	Video filter FortiGuard category takes precedence over allowed channel ID exception in the same category.
783112	FortiGate goes into conserve mode due to high memory usage of WAD `user-info` process. The WAD `user-info` process will query the user count information from the LDAP server every 24 hours. If any of the LDAP query messages are closed by exceptions, there is a memory leak. If `obtain-user-info` is enabled under `config user ldap`, this memory leak will be triggered on daily basis. **Workaround**: create an automation stitch to restart the WAD daemon every day to avoid conserve mode.

Routing

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>745856</td><td>The default SD-WAN route for the LTE wwan interface is not created.
<b>Workaround</b>: add a random gateway to the wwan member.<pre>
config system sdwan
    config members
        edit 2
            set interface "wwan"
            set gateway 10.198.58.58
            set priority 100
        next
    end
end
</pre></td></tr>
</table>

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
779181	Security rating *Optimization* card shows failure for system uptime due to low uptime for FortiAP (less than 24 hours).
793234	*Fabric Management* page incorrectly shows some FortiAPs with an unregistered FortiCare status even though the FortiAP is already registered. This is just a display issue and does not impact FortiAP operation.
794703	Security Rating report for *Rogue AP Detection* and *FortiCare Support* checks show incorrect results.

SSL VPN

Bug ID	Description
757450	SNAT is not working in SSL VPN web mode when accessing an SFTP server.
852566	User peer feature for one group to match to multiple user peers in the authentication rules is broken.

System

Bug ID	Description
644782	A large number of detected devices causes httpsd to consume resources, and causes entry-level devices to enter conserve mode.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
708228	A DNS proxy crash occurs during `ssl_ctx_free`.
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. **Workaround**: set the `auto-asic-offload` option to `disable` in the firewall policy.
751715	Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed.
758490	The value of the `extra-init` parameter under `config system lte-modem` is not passed to the modem after rebooting the device.
763185	High CPU usage on platforms with low free memory upon IPS engine initialization.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.
768979	On a FortiGate with many FortiSwitches and FortiAPs, the *Device Inventory* widget and `user-device-store list` are empty.
798091	After upgrading from 6.4.9 to 7.0.5, the FG-110xE's 1000M SFP interface may fail to auto-negotiate and cannot be up due to the missed auto-negotiation.
799570	High memory usage occurs on FG-200F.
812957	When setting the `speed` of 1G SFP ports on FG-180xF platforms to `1000full`, the interface does not come up after rebooting.
847077	`Can't find xitem. Drop the response.` error appears for DHCPOFFER packets in the DHCP relay debug.

User & Authentication

Bug ID	Description
754725	After updating the FSSO DC agent to version 5.0.0301, the DC agent keeps crashing on Windows 2012 R2 and 2016, which causes lsass.exe to reboot.
765184	RADIUS authentication failover between two servers for high availability does not work as expected.
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.

VM

Bug ID	Description
756510	FG-ARM64-AWS kernel panic occurs (`Kernel panic - not syncing: Fatal exception in interrupt`).

Web Filter

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

Built-in AV Engine

AV Engine 6.00270 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.00105 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

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