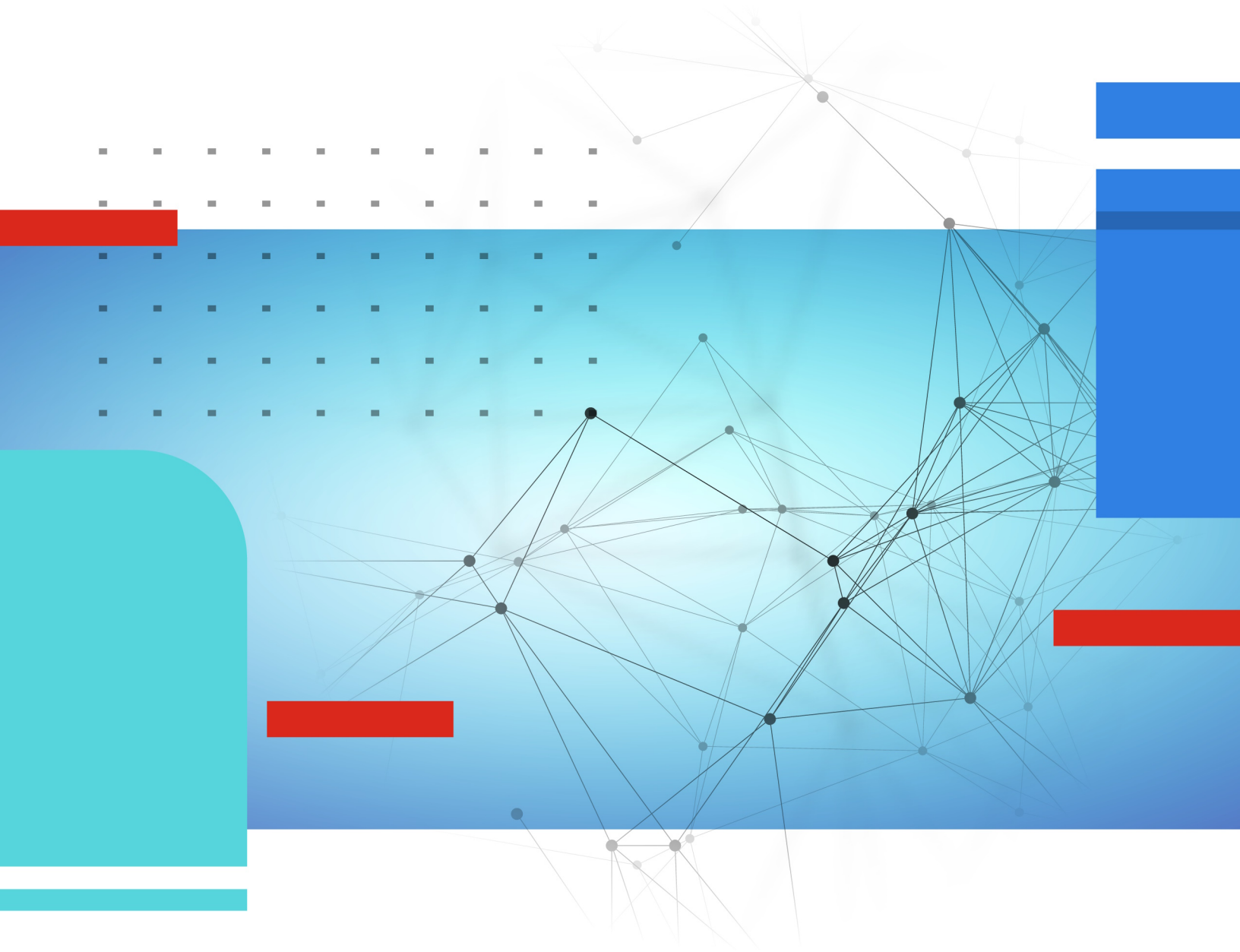
# Release Notes

## FortiOS 7.6.1



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

**FORTINET VIDEO LIBRARY**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

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

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

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

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

**FEEDBACK**
Email: techdoc@fortinet.com

June 12, 2025
FortiOS 7.6.1 Release Notes
01-761-1084726-20250612

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2024-11-28 | Initial release. |
| 2024-12-02 | Updated New features or enhancements on page 24 and Known issues on page 78. |
| 2024-12-05 | Added SSL VPN not supported on FortiGate 90G series models on page 13, Policies that use an interface show missing or empty values after an upgrade on page 43, and Managed FortiSwitch do not permit empty passwords for administrator accounts on page 43.<br>Updated New features or enhancements on page 24, Resolved issues on page 50, and Known issues on page 78. |
| 2024-12-09 | Updated Virtualization environments on page 46, Changes in table size on page 23, New features or enhancements on page 24, Resolved issues on page 50, and Known issues on page 78. |
| 2024-12-11 | Updated Policies that use an interface show missing or empty values after an upgrade on page 43, Changes in default behavior on page 20, New features or enhancements on page 24, Resolved issues on page 50, Known issues on page 78, Built-in AV Engine on page 86, and Built-in IPS Engine on page 87. |
| 2024-12-16 | Updated Resolved issues on page 50. |
| 2025-01-02 | Updated Changes in CLI on page 17, Resolved issues on page 50, and Known issues on page 78. |
| 2025-01-06 | Updated Changes in CLI on page 17. |
| 2025-01-13 | Updated Supported models on page 8. |
| 2025-01-14 | Added RADIUS vulnerability on page 14.<br>Updated Changes in CLI on page 17, Resolved issues on page 50, Known issues on page 78. |
| 2025-01-20 | Updated Resolved issues on page 50. |
| 2025-02-04 | Updated Known issues on page 78. |
| 2025-02-18 | Updated Special notices on page 9, New features or enhancements on page 24, Resolved issues on page 50, and Known issues on page 78. |
| 2025-03-03 | Added GUI cannot be accessed when using a server certificate with an RSA 1024 bit key on page 16.<br>Updated Changes in default behavior on page 20, New features or enhancements on page 24, Resolved issues on page 50, and Known issues on page 78. |
| 2025-03-04 | Updated New features or enhancements on page 24. |
| 2025-03-06 | Updated New features or enhancements on page 24. |

| Date | Change Description |
|---|---|
| 2025-03-10 | Updated Known issues on page 78. |
| 2025-03-17 | Updated New features or enhancements on page 24, Resolved issues on page 50, and Known issues on page 78. |
| 2025-03-31 | Updated Resolved issues on page 50 and Known issues on page 78. |
| 2025-04-14 | Updated Changes in default behavior on page 20, New features or enhancements on page 24, and Known issues on page 78. |
| 2025-04-28 | Updated New features or enhancements on page 24, Resolved issues on page 50, and Known issues on page 78. |
| 2025-05-13 | Updated Resolved issues on page 50 and Known issues on page 78. |
| 2025-05-27 | Updated Resolved issues on page 50 and Known issues on page 78. |
| 2025-06-05 | Updated Changes in default behavior on page 20. |
| 2025-06-09 | Added Removed speed setting affects SFP+ interfaces after upgrade on page 44.<br>Updated Resolved issues on page 50 and Known issues on page 78. |
| 2025-06-11 | Updated Changes in default behavior on page 20, Resolved issues on page 50, and Known issues on page 78. |
| 2025-06-12 | Updated SSL VPN not supported on FortiGate 90G series models on page 13. |

# Introduction and supported models

This guide provides release information for FortiOS 7.6.1 build 3457.

For FortiOS documentation, see the Fortinet Document Library.

## Supported models

FortiOS 7.6.1 supports the following models.

| | |
|---|---|
| **FortiGate** | FG-40F, FG-40F-3G4G, FG-60F, FG-61F, FG-70F, FG-71F, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F |
| **FortiWiFi** | FWF-40F, FWF-40F-3G4G, FWF-60F, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE |
| **FortiGate Rugged** | FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G |
| **FortiFirewall** | FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM |
| **FortiGate VM** | FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, 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 |

## FortiGate 6000 and 7000 support

FortiOS 7.6.1 supports the following FG-6000F, FG-7000E, and FG-7000F models:

| | |
|---|---|
| **FG-6000F** | FG-6001F, FG-6300F, FG-6301F, FG-6500F, FG-6501F |
| **FG-7000E** | FG-7030E, FG-7040E, FG-7060E |
| **FG-7000F** | FG-7081F, FG-7121F |

# Special notices



# FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal `private-data-encryption` key. Instead administrators simply enable the command, and a random `private-data-encryption` key is generated.

**Previous FortiOS CLI behavior**

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
1234567890123456789012345678 9abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
1234567890123456789012345678 9abc
Your private data encryption key is accepted.
```

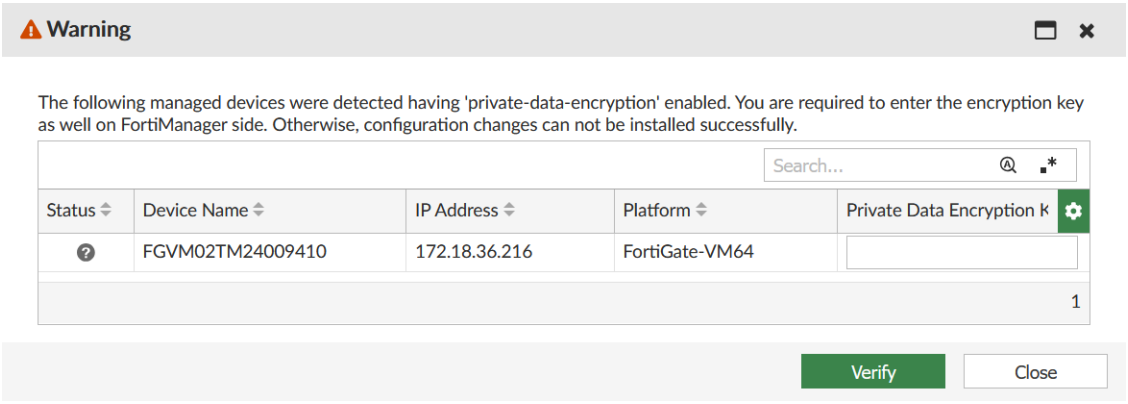
**New FortiOS CLI behavior**

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
```

```
operation!
Do you want to continue? (y/n)y
Private data encryption key generation succeeded!
```

### FortiManager behavior

Support for the FortiGate `private-data-encryption` key by the Device Manager in FortiManager 7.6.2 and earlier is unchanged. It automatically detects the remote FortiGate `private-data-encryption` key status and prompts the administrator to manually type the private key (see picture below). FortiManager 7.6.2 and earlier does not support the updated, random `private-data-encryption` key as the administrator will have no knowledge of the key generated in the FortiOS CLI command above. It will be supported in a later version of FortiManager.




### FortiOS upgrade behavior

If in FortiOS 7.4.5 or 7.6.0 the 32-digit hexadecimal private key is enabled, and then the FortiGate device is upgraded to 7.6.1, the 32-digit hexadecimal `private-data-encryption` key is preserved. As a result, FortiManager 7.6.2 and earlier is aware of the 32-digit hexadecimal `private-data-encryption` key and can continue to manage the FortiGate device. However, if the `private-data-encryption` key is enabled after an upgrade of FortiOS to 7.6.1, FortiManager 7.6.2 and earlier no longer can manage FortiGate devices running FortiOS 7.6.1.

# FortiGate cannot restore configuration file after private-data-encryption is re-enabled

In a new enhancement, enabling `private-data-encryption` will utilize a randomly generated private key. Therefore, FortiGate cannot restore the configuration file in the following sequence:

1. `private-data-encryption` enabled with random key, and configuration is backed up.
2. `private-data-encryption` disabled.
3. `private-data-encryption` enabled again, with new random key.
4. Restore configuration file in step 1.

When disabling `private-data-encryption`, a warning in the CLI will be displayed:

```
This operation will restore system default data encryption key!
```

```
Previous config files encrypted with the private key cannot be restored after this
operation!

Do you want to continue? (y/n)y
```

# Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.6.1 features.

# FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.6.1 features.

- FortiGate 6000 incompatibilities and limitations
- FortiGate 7000E incompatibilities and limitations
- FortiGate 7000F incompatibilities and limitations

# SSL VPN removed from 2GB RAM models for tunnel and web mode

On FortiGate models with 2GB of RAM or below, the SSL VPN web and tunnel mode feature will no longer be available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See SSL VPN to IPsec VPN Migration for more information.

FortiGate models not listed above will continue to have SSL VPN web and tunnel mode support.

# 2 GB RAM FortiGate models no longer support FortiOS proxy-related features

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, starting from version 7.4.4, FortiOS no longer supports proxy-related features.

This change impacts the FortiGate 40F and 60F series devices, along with their variants. See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

# FortiGate VM memory and upgrade

FortiGate virtual machines (VMs) are not constrained by memory size and will continue to support all available features after upgrading to FortiOS 7.6.0. However, it is recommended to setup VMs with at least 4 GB of RAM for optimal performance.

# Hyperscale NP7 hardware limitation

Because of an NP7 hardware limitation, for CGN traffic accepted by a hyperscale firewall policy that includes an overload with port block allocation (overload PBA) IP Pool, only one block is allocated per client. The setting of the hyperscale firewall policy `cgn-resource-quota` option is ignored.

Because of this limitation, under certain rare conditions (for example, only a single server side IP address and port are being used for a large number of sessions), port allocation may fail even if the block usage of the client is less than its quota. In cases such as this, if the client has traffic towards some other servers or ports, additional port allocation can become successful. You can also work around this problem by increasing the IP Pool block size (`cgn-block-size`).

# GUI access conflict with IPSec TCP tunnel on the same interface

In FortiOS version 7.6.1, the default IKE TCP port has been changed to port 443 on new deployments. See Bug ID 1051144 in Changes in default values on page 22.

This may affect GUI access for interfaces bound to an IPsec tunnel in the scenario that the GUI admin port is also using port 443.

In case GUI connectivity is lost, connect to the FortiGate by:

1. Connecting from an interface that is not bound to an IPsec tunnel.
2. Connecting to the interface using SSH, if SSH is enabled.
3. Connecting to the FortiGate from console.

To ensure continued functionality, users are recommended to either:

- Choose an alternative interface for GUI access by configuring:

```
config system global
    set admin-sport <port>
end
```

- Customize the `ike-tcp-port` to a value other than 443:

```
config system settings
    set ike-tcp-port <port>
end
```

# SSL VPN not supported on FortiGate 90G series models

The SSL VPN web and tunnel mode feature will not be available from the GUI or the CLI on the FortiGate 90G and 91G models. Settings will not be upgraded from previous versions.

Consider migrating to using IPsec Dialup VPN for remote access.

# RADIUS vulnerability

Fortinet has resolved a RADIUS vulnerability described in CVE-2024-3596. As a result, firewall authentication, FortiGate administrative GUI authentication, and WiFi authentication may be affected depending on the functionality of the RADIUS server software used in your environment. RFC 3579 contains information on the affected RADIUS attribute, message-authenticator.

In order to protect against the RADIUS vulnerability described in CVE-2024-3596, as a RADIUS client, FortiGate will:

1. Force the validation of message-authenticator.
2. Reject RADIUS responses with unrecognized proxy-state attribute.

Message-authenticator checking is made mandatory under UDP/TCP. It is not mandatory when using TLS. Therefore, if FortiGate is using UDP/TCP mode without RADSEC, the RADIUS server should be patched to ensure the message-authenticator attribute is used in its RADIUS messages.

### Affected Product Integration

- FortiAuthenticator version 6.6.1 and older
- Third party RADIUS server that does not support sending the message-authenticator attribute

### Solution

- Upgrade FortiAuthenticator to version 6.6.2, 6.5.6 or 6.4.10 and follow the upgrade instructions: https://docs.fortinet.com/document/fortiauthenticator/6.6.2/release-notes/859240/upgrade-instructions
- Upgrade the RADIUS server and/or enable it to send the correct message-authenticator attribute

# Changes to NP7 traffic shaping

The following known issues for the Queuing based Traffic Management (QTM) module on NP7 are fixed:

- Incorrect checksum for fragments after QTM.
- Packets longer than 6000 bytes cause QTM to hang.
- Refreshing causes QTM to hang.
- MTU is not honored after QTM, so the packet is not fragmented.

As a result of these changes, you can no longer use the following command to change QoS type used for traffic shaping for sessions offloaded to NP7 processors:

```
config system npu
    set default-qos-type {policing | shaping}
end
```

Instead, `default-qos-type` can only be set to `policing`.

For NP7 sessions, policy traffic shaping, per-IP shaping, and regular port shaping (outbandwidth enabled on an interface without a shaping profile) always use the NP7 accounting and traffic shaping module (called the TPE module). This is the same as changing the `default-qos-type` to `policing`.

For NP7 sessions, shaping profiles on interfaces now only use QTM for traffic shaping (equivalent to setting `default-qos-type` to `shaping`). Shaping profiles on interfaces are also called Multiclass shaping (MCS). The interface can be a physical interface, LAG interface, and VLAN interface (over physical or LAG). The FortiGate supports shaping profiles on a maximum of 100 interfaces.

# GUI cannot be accessed when using a server certificate with an RSA 1024 bit key

The GUI cannot be accessed when using an admin server certificate with an RSA 1024 bit key after upgrading to FortiOS 7.6.1, 7.4.8, or 7.2.11. An RSA key of at least 2048 bits is required. Certificates that are using an RSA key of less than 2048 bits are no longer supported.

# Changes in CLI

| Bug ID | Description |
|---|---|
| 974985 | Before 7.6.0, the adv-interval accepted values from 1 to 255 seconds. Starting with FortiOS 7.6.0, adv-interval accepts values in milliseconds, ranging from 250 to 255000. This change allows for quicker VRRP failovers. For more information, see Configure the VRRP hello timer in milliseconds. |
| 1009740 | Renamed the server-type setting's `iot-query` option to `vpatch-query`.<br>`config system central-management`<br>`  config server-list`<br>`  edit <id>`<br>`  set server-type {update\|rating\|vpatch-query\|iot-collect}`<br>`  set server-address <x.x.x.x>`<br>`  next`<br>`  end`<br>`end` |
| 1013290 | Added `wids-entry-cleanup` in `config wireless-controller timers`:<br>`config wireless-controller timers`<br>`  set wids-entry-cleanup 5`<br>`end`<br>Added `max-wids-entry` in `config wireless-controller global`:<br>`config wireless-controller global`<br>`  set max-wids-entry 1024`<br>`end` |
| 1017835 | Application bandwidth tracking in the CLI has been relocated from the `system` to `global` settings. To enable application bandwidth tracking:<br>`config system global`<br>`  set application-bandwidth-tracking enable`<br>`end` |
| 1035072 | The options `empty-cert-action`, `user-agent-detect`, and `client-cert` have been removed from system.access-proxy. Instead, they are added to the following configuration commands:<br>`config firewall access-proxy-virtual-host`<br>`  set empty-cert-action <action>`<br>`  user-agent-detect {enable\|disable}`<br>`  client-cert {enable\|disable}`<br>`end`<br>`config firewall vip`<br>`  set type access-proxy` |

| Bug ID | Description |
|---|---|
| | `set empty-cert-action <action>`<br>`user-agent-detect {enable\|disable}`<br>`client-cert {enable\|disable}`<br>`end` |
| 1059775 | Add comment setting in wtp configuration.<br>`config wireless-controller wtp`<br>`edit <name>`<br>`set comment <string>`<br>`next`<br>`end` |
| 1064394 | The `server-type` option, the type of Syslog server, is added in the wireless syslog configuration.<br>`config wireless-controller syslog-profile`<br>`edit one-profile`<br>`set server-type [standard \| fortianalyzer]`<br>`next`<br>`end"` |

# Changes in GUI behavior

| Bug ID | Description |
|---|---|
| 834860 | Users are allowed to create a policy using IP or MAC addresses directly from the FortiView pages and Log Viewer. This feature streamlines the policy creation process, making it more efficient and user-friendly. |
| 966534 | GUI support for configuring SCIM client has been added under the *User & Authentication* > *SCIM Clients* page. |
| 969758 | Added GUI support for creating Internet Service Group. This allows users to create and manage Internet Service Groups more intuitively and efficiently, providing a more user-friendly experience. |
| 976480 | Added GUI support for creating local-in policies. This allows users to create local-in policies more intuitively and efficiently, providing a more user-friendly experience. |
| 976976 | In an IPsec dial-up VPN configuration using IKEv2, users can now configure Remote Gateway Match and security posture tags within the VPN tunnel configuration in the GUI. |
| 987210 | GUI Enhancement for Firewall Policy Management. Users have the option to apply logical and operations among various policy objects within the GUI, providing a more detailed level of control over the configuration of firewall policies. |
| 988573 | The Backup heartbeat interfaces option is added to the *System* > *HA* page. |
| 1000836 | FortiGate EMS connector settings now supports configuring FortiClient Cloud access key within the GUI. |

# Changes in default behavior

| Bug ID | Description |
|---|---|
| 949997 | LDAPS authentication behavior changed. FortiOS 7.6.1 and later enhances the security standards for LDAPS by requiring FortiOS to trust the server certificate during the TLS handshake. If the LDAP server's CA certificate was not present and is not added after upgrading to FortiOS 7.6.1, LDAPS authentication will fail. To ensure smooth operation, import the LDAP server's CA certificate to FortiGate prior to upgrading. For more details, see Configuring client certificate authentication on the LDAP server. |
| 1043962 | Auto Firmware Upgrade Control<br>In FortiOS version 7.4.5 and later, the option to control automatic firmware upgrades has been updated. Previously, this option was enabled only on entry-level models and disabled by default on all other models, allowing users to manually control firmware upgrades. In version 7.4.5 and later, this option is now enabled by default on all FortiGate models, including FortiGate-VMs. This means the system will automatically upgrade to the latest firmware unless manually configured otherwise.<br>If you prefer to manage firmware upgrades manually, please review and adjust the auto-upgrade settings according to your requirements. |
| 1061121 | Starting with FortiOS 7.6.1, the default neighbor detection method has been updated. Previously, the default method was FortiLink. With this release, the default neighbor detection method is now LLDP. |
| 1063233 | The BIOS security level is updated from levels 0/1/2 to levels Low and High. Level High will correspond to previous behaviors in level 2, and level Low will correspond to behaviors in level 1. BIOS that still uses levels 0 will now behave like level 1/Low. |
| 1066082 | Starting with version 7.6.1, a password is required when setting up a new HA member. If upgrading from a previous version without an HA password, the system will skip the password check. However, any subsequent modifications to the system.ha settings will enforce the password check and require the HA password.<br>  The password should be added across all cluster members and must be the same for all members.<br>To set the password:<br>`config system ha`<br>`set password <passwd>`<br>`end` |
| 1076795 | When enabling `private-data-encryption`, instead of asking users to input a 32-digit hexadecimal string as the `master-encryption-password`, the FortiGate will generate the random password itself. This increases security where the `master-encryption-password` is not known and cannot be stolen or leaked. |

| Bug ID | Description |
|---|---|
| 1091890 | The default behavior for the following manage- options will now be enabled. For users upgrading to 7.6.1, it will only be enabled if IPAM is currently disabled. If IPAM is enabled, existing configurations will remain unchanged to avoid disruptions.<br>`config system ipam`<br>`set manage-lan-addresses {enable \| disable}`<br>`set manage-lan-extension-addresses {enable \| disable}`<br>`set manage-ssid-addresses {enable \| disable}`<br>`end` |
| 1093412 | The `sess-sync` feature does not work after enabling encryption.<br>Previously the `sess-sync` feature was not affected when encryption was enabled, but the `sess-sync` traffic was not encrypted. |

# Changes in default values

| Bug ID | Description |
|---|---|
| 1051144 | Before FortiOS version 7.6.1, IPSec dialup VPN by default has *Auto* mode enabled where if UDP connection is blocked then the client connection will fallback to TCP using port 4500. Some environments may have TCP port 4500 blocked locally or by their ISP, therefore the default IPSec TCP IKE port is now changed to 443.<br>Previous CLI Behavior<br>`config system settings`<br>`    set ike-tcp-port 4500`<br>`end`<br>New CLI Behavior<br>`config system settings`<br>`    set ike-tcp-port 443`<br>`end`<br>This change applies to new FortiGate configurations only. Upon upgrade, the old `ike-tcp-port` value will be retained.<br>For information about possible conflict with GUI access on port 443, please see GUI access conflict with IPSec TCP tunnel on the same interface on page 13. |

# Changes in table size

| Bug ID | Description |
|---|---|
| 1030001 | On the 200-400 series FortiGates, increase the number of VDOMs from 10 to 25.<br>On the 500-900 series FortiGates, increase the number of VDOMs from 10 to 50. |
| 1042266 | On high-end FortiGate models, increase the number of policy routes and policy routes6 from 2048 to 5000. |
| 1059858 | On entry-level FortiGate models, increase the number of firewall on-demand-sniffer to 6. |
| 1064311 | On 90xG FortiGate models, increase the number of firewall addresses and firewall addresses6 from 20000 to 40000. |
| 1070828 | On FortiGate, increase maximum number of configurable IPv6 tunnels from 4 to 32. |
| 1073677 | On 90xG FortiGate models, increase the number of zones from 200 to 500. |

# New features or enhancements

More detailed information is available in the New Features Guide.

# Cloud

See Public and private cloud in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 1007607 | AzureSDN connectors support IPv6 address objects. |
| 1029721 | FortiOS Azure SDN connector moves private IP on the trusted NIC during A/P HA failover. |
| 1031828 | Introduce GraphQL bulk query to FortiGate on Azure to reduce the number of API queries going out to Azure and as a result, reducing the time taken to resolve SDN connector Dynamic objects in a large environment.<br>Configure the `FGT_VM64_AZURE` SDN connector and firewall address objects. The following IP address filters are supported:<br>`Spoke_1 (AZ) # show`<br>`config firewall address`<br>`edit "AZ"`<br>`set uuid 6b18eb16-7069-51ef-c174-58f82ee3d1b2`<br>`set type dynamic`<br>`set sdn "6899_AutoScale_1"`<br>`next`<br>`end`<br>`Spoke_1 (AZ) # set filter`<br>`<key1=value1> [& <key2=value2>] [\| <key3=value3>]`<br>Available filter keys are:<br>`<Vm><Tag.><Size><Location><SecurityGroup>`<br>`<Vnet><Subnet><ResourceGroup><ApplicationSecurityGroup><Vmss><Subscription>`<br>`<LoadBalancer><ApplicationGateway>`<br>`<ServiceTag><Region>`<br>`<K8S_Cluster><K8S_Namespace><K8S_ServiceName><K8S_NodeName>`<br>`<K8S_PodName><K8S_Region><K8S_Zone><K8S_Label.>` |

| Feature ID | Description |
|---|---|
| 1055813 | FortiGate-VM supports AWS Nitro TPM 2.0 specification. |
| 1061195 | FortiOS version 7.6.1 supports the use of MLX5/4 and the upcoming MANA NIC on Azure Dv6/Ev6 instance types. |
| 1071411 | Azure SDN connectors support GraphQLbulk queries. |

# GUI

See GUI in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 754766 | Introducing the new *Asset Details* slide-in page, accessible using the action buttons/menus on multiple GUI pages. This page provides comprehensive endpoint information, streamlining the diagnostic process and reducing reliance on CLI commands. |
| 987321 | Introducing a new tab in the command palette called *Diagnostics*. This new tab provides a list of troubleshooting commands, allowing users to browse and search for debug commands directly within the GUI, enhancing efficiency and ease of use. |
| 1058456 | Enhancements to IPSec Monitoring. This feature improves the VPN tunnel monitor page with dockable, filterable widgets, pie charts for tunnel status and uptime, and quick access to various tools, boosting usability and visualization for better VPN management. |

# LAN Edge

See LAN Edge in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 909824 | FOS supports QinQ for the switch controller, allowing MSSPs to manage multiple clients networks by having a unique customer VLAN for each client and each client can have its own, self-managed 4K VLAN range in their virtual domain. This ensures better segregation and control over network traffic. |
| 984616 | Introducing Split Tunnel Mode for FortiExtender in LAN extension mode. With this feature, specific traffic patterns defined by the split service are sent directly to the FEXT local gateway. This reduces the load on the central FGT by routing less traffic through the LAN extension tunnel, thereby enhancing efficiency and network performance. |

| Feature ID | Description |
|---|---|
| 1005045 | Previously, VLAN optimization could only be enabled or disabled. The new VLAN pruning feature selectively allows only necessary VLANs on the path between destinations on auto-generated trunks, reducing traffic congestion and enhancing network performance. |
| 1039228 | Added support for VLANs over a FortiExtender configured as a LAN extension. VLAN support is configured on the FortiGate Access Controller using the GUI or using these CLI commands:<br>`config extension-controller extender-profile`<br>`edit <FortiExtender Profile>`<br>`set extension lan-extension`<br>`config lan-extension`<br>`config downlinks`<br>`edit <id>`<br>`set type port`<br>`set port <port>`<br>`set pvid <vlanid>`<br>`next`<br>`end`<br>`end`<br>`next`<br>`end`<br>Where `port` is the VLAN interface added to the FortiExtender interface and `vlanid` is the desired VLAN ID. |
| 1058402 | FortiOS now includes advanced Wireless Intrusion Detection System (WIDS) options, enhancing the detection and reporting of a wider range of wireless threats. This upgrade boosts security, providing customers with superior detection against potential intrusions. |
| 1058404 | FortiGate can now register authorized FEXT (FortiExtender) devices. Previously, it could only register FAP (FortiAP) and FSW (FortiSwitch) devices. This new feature ensures comprehensive network management by including all connected devices. |
| 1059461 | The FOS WiFi Controller now includes a `called-station-id-type` setting, allowing customization of the `Called-Station-Id` attribute in RADIUS *Access-Request* packets to use MAC:SSID, IP:SSID, or APName:SSID formats, enhancing network configuration flexibility.<br>`conf wireless-controller vap`<br>`edit <name>`<br>`set called-station-id-type {mac \| ip \| apname}`<br>`next`<br>`end` |
| 1060780 | FortiAP now supports console, SSH, or HTTPS login using remote user accounts from a third-party TACACS server, enhancing flexibility and security in account management. |
| 1068898 | FortiGate now generates accounting messages when WiFi clients connect to an SSID with MPSK created through the FortiGuest self-registration portal, enhancing network management and user accountability. |

| Feature ID | Description |
|---|---|
| 1078491 | The FortiOS WiFi controller now supports pushing RADIUS server settings using TCP or TLS protocols to FortiAP's for Local-Bridge mode Captive Portal SSIDs, enhancing security and reliability compared to the previous UDP-only support. |

# Network

See Network in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 961038 | Add 2.5G and 5G speed options for the 10/1 GigE RJ45 interfaces (port1-16) on the FortiGate 2600F platform. Also add an auto option (the new default) that automatically adjusts the port speed. Existing port speed configurations will be maintained during the firmware upgrade. |
| 1032512 | Support including denied multicast sessions in the session table. This feature allows the creation of sessions for denied multicast traffic, enabling subsequent packets to be directly matched and dropped, reducing CPU usage and improving performance.<br>`config system setting`<br>`  set ses-denied-multicast-traffic {disable \| enable}`<br>`end` |
| 1040296 | To support VRF route leaking, on FortiGates with NP6 and NP7 processors, you can use the following command to enable accelerated NPU inter-VDOM links without enabling multi-VDOM mode.<br>`config system global`<br>`  set single-vdom-npuvlink {enable \| disable}`<br>`end` |
| 1040394 | Enhanced flexibility and performance in network with smaller configurable TTL for UDP traffic on hyperscale firewall VDOMs. Previously, the minimum TTL for UDP traffic was set at 120 seconds for Hyperscale firewall VDOMs. This enhancement removes that restriction, allowing users to configure the TTL to 1 second or more. This change offers greater flexibility in network management and enhances network performance. |
| 1048011 | Extended VRF ID Range for Enhanced Network Scalability. Previously, up to 252 Virtual Routing and Forwarding (VRF) instances could be configured per VDOM, with VRF IDs ranging from 0 to 251. With this enhancement, the VRF ID range has been extended to 0-511, allowing for a minimum of 512 unique VRFs per VDOM. This enhancement allows for greater scalability and flexibility in network configurations. |
| 1049910 | FortiGate now supports inspecting 802.1ah packets within a virtual wire pair configuration. This enhancement enables deep packet inspection and UTM scanning. By leveraging this capability, FortiGate can effectively analyze and inspect the 802.1ah header, perform the necessary inspection, and then re-add the header, ensuring robust protection against a wide range of cyber threats. |

| Feature ID | Description |
|---|---|
| 1060303 | Previously, local-out traffic could not specify a Virtual Routing and Forwarding (VRF) instance, but now it can, allowing for traffic segregation, optimized routing, and enhanced policy enforcement, which improves network organization, security, and performance. |
| 1061705 | Introducing a new FortiGate feature that disables IP address translation within the SIP payload in 464XLAT environments. This ensures SIP packets with IPv4 information reach user equipment without translation, preventing RTP connection issues and improving the reliability of SIP-based services. |
| 1067117 | Added support for specifying the outgoing interface and VRF for a web proxy forward server or a web proxy isolator server, such as FortiIsolator.<br>`config web-proxy forward-server`<br>`edit <name>`<br>`set interface-select-method specify`<br>`set interface <port>`<br>`set vrf-select <vrf-id>`<br>`next`<br>`end`<br>`config web-proxy isolator-server`<br>`edit <name>`<br>`set interface-select-method specify`<br>`set interface <port>`<br>`set vrf-select <vrf-id>`<br>`next`<br>`end` |
| 1071614 | The `hw-session-sync-dev` option now supports multiple physical interfaces, up to twice the number of Network Processors (NPs). Additionally, it now shares the ports between hardware and software session-sync devices. This enhancement increases reliability and flexibility in network configurations. |
| 1082763 | PIM now supports all VRFs (up to 511) and is aware of IPv4 multicast routing/forwarding over a single overlay, enhancing network scalability and flexibility compared to the previous VRF 0-only support. |

# Operational Technology

See Operational Technology in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 1000362 | FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G include a general purpose input output (GPIO) module, also known as, a digital I/O (DIO) module. Added support for SNMP traps or notifications and automation stitch notifications when DIO module alarm functionality is activated, that is, when a change in any digital input is detected and the digital output is activated. Notification support depends on previously configured `config system digital-io` and `execute digital-io set-output` settings prior to event notification.<br>SNMP and automation stitch notifications can be configured using these CLI commands on FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G devices only:<br>• For automation stitch support, in `config system automation-condition` added new options `set condition-type input` and `set input-state open \| close`<br>• For SNMP support, in `config system snmp community` added new option `set events dio` |
| 1075708 | FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G include a general purpose input output (GPIO) module, also known as, a digital I/O (DIO) module. This module is used for activating a digital output when triggered by a change in any digital input. For example, when a switch change from open to closed or a voltage change from low to high is detected, then a digital output is activated. In this example, the digital input is connected to a cabinet door and the output is connected to a buzzer.<br>Added CLI support for configuring the above DIO alarm functionality on FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G devices only:<br>• `config system digital-io`: command to configure input mode<br>• `execute digital-io set-output`: command to configure output mode<br>• `diag sys digital-io state`: command to check current input/output status |

# Policy & Objects

See Policy and objects in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 1003586 | Added support for a web proxy isolator server, such as FortiIsolator, in proxy policies and added a new *Isolate* action in proxy-policy to distinguish isolated traffic from normal traffic in logs. Isolators are fundamentally the same as web proxy forward servers because both will redirect HTTP/HTTPS requests to an HTTP/HTTPS proxy server. However, isolators have the specific function of isolating potentially unsafe traffic from a user environment.<br>To support configuration of isolator servers for explicit web proxy and transparent web proxy types:<br>• Added CLI commands:<br>  • `config web-proxy isolator-server` for configuring isolator servers<br>  • `set action isolate` and `set isolator-server <name>` for `config firewall proxy-policy`, `set proxy explicit-web`, or `set proxy transparent-web` |

| Feature ID | Description |
|---|---|
| 1027037 | Support Fully Qualified Domain Name (FQDN) address groups within the Internet Service Database (ISDB), addressing the challenge of frequently changing IP addresses and ensuring accurate and reliable firewall policies. |
| 1040199 | The current Port block allocation (PBA) and Fixed port range (FPR) IP Pool mechanisms use a sequential port selection algorithm, assigning the next available non-conflicting port within the specified range. This enhancement introduces the `port-random` firewall policy option for enabling a randomized port selection algorithm, making the allocation process less predictable, thus enhancing security. |
| 1046509 | FortiOS has introduced a new dynamic address object subtype, RSSO, which can be used in both the source and destination fields of firewall policies. This enhancement allows for more granular and precise policies based on RSSO group membership, enhancing security and flexibility in managing network traffic and enforcing policies. |
| 1058411 | Introducing a new ISDB entry for Fortinet SOCaaS, Fortinet-FortiGuard.SOCaaS. This feature enables customers to configure policies for devices to forward data to SOCaaS collectors without relying on DNS. By eliminating the dependency on DNS, this enhancement reduces the risk of DNS mapping failures, ensuring a more reliable and seamless data forwarding process. |
| 1058516 | Hyperscale FortiOS now supports a configurable interim log for PBA NAT logging. This enables continuous access to PBA event logs during an ongoing session, providing comprehensive logging throughout the session's lifespan.<br>`config firewall ippool`<br>`edit <name>`<br>`set type cgn-resource-allocation`<br>`set pba-interim-log`<br>`next`<br>`end`<br>The `log-interval` range is 600 to 86400 seconds. Default is 0 which disables interim logging. Interim logging is supported by the NP7 hardware log module and host hardware logging. Interim logging is also compatible with per-session, per-mapping, and per-session ending logging modes and works with the NetFlow and syslog log formats.<br>Interim logging for PBA sessions was added to mainstream FortiOS version 7.6.0. |
| 1070831 | A new default local-in-policy has been added with internet service source enabled for Malicious-Malicious.Server, Tor-Exit.Node, and Tor-Relay.Node. This policy is designed to utilize these 3 ISDB sources to identify known malicious threat actors and prevent them from accessing any interface on the FortiGate on any service and port. |
| 1085702 | Previously, MAP-E utilized the RA IPv6 prefix for deployment. With this enhancement, MAP-E can now operate in DHCPv6-PD environments, providing greater flexibility, improved automation, and scalability in network configurations. |

# SD-WAN

See SD-WAN in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 951494 | In this enhancement, support for a new FortiGuard SLA Database (SLA Database), which includes popular SaaS and Internet destinations and recommended settings that can be selected as probe servers for SD-WAN Performance SLA configuration in the GUI using the *Performance SLA* and *SLA Target* fields in the *New Performance SLA* page and in the CLI using these commands:<br>`config system sdwan`<br>`  config health-check`<br>`  edit <health-check name>`<br>`  set fortiguard enable`<br>`  set fortiguard-name <target-name-from-SLA-Database>`<br>`  next`<br>`  end`<br>`end`<br>The FortiGate requires a valid SD-WAN Network Monitor (SWNM) entitlement to be applied for the FortiGuard SLA Database to be downloaded or updated. |
| 1002494 | In this enhancement, an SD-WAN wizard is added to the *SD-WAN > SD-WAN Zones* page to provide guided configuration of these settings for a simple SD-WAN setup (maximum of two members can be added in the SD-WAN wizard):<br>• *Interface*<br>• *Networking*<br>• *Performance SLA*<br>• *SD-WAN Rule*<br>After the wizard is used, a default static route using the newly created SD-WAN interface must still be configured.<br>The FortiGate requires a valid SD-WAN Network Monitor (SWNM) entitlement to be applied for the SD-WAN wizard to be visible. |
| 1025701 | In this enhancement, support has been added for passive application performance monitoring (APM) by measuring and logging these metrics per TCP session:<br>• Network response time<br>• Server response time<br>• Original retransmits<br>• Reply retransmits<br>• SYN retransmits<br>• SYN-ACK retransmits<br>• Original or reply resets<br>These passive measurements are configured in firewall policies with the SD-WAN zone as the destination interface using these CLI commands:<br>`configure firewall policy`<br>`  edit <entry>`<br>`  set app-monitor <enable \| disable>`<br>`  next`<br>`end` |

| Feature ID | Description |
|---|---|
| | Upon enabling this feature, NPU offloading for the firewall policy is disabled automatically.<br>This feature assists with monitoring performance of TCP traffic and locating potential network issues. TCP metrics can be displayed using `diag sys session list` in the CLI and in forward traffic logs displayed in either the CLI or the GUI.<br>SD-WAN traffic steering remains independent from the measured TCP session metrics. |
| 1025704 | In this enhancement, when a spoke advertises routes using iBGP to a hub, introduced mapping of SD-WAN member priorities into the BGP MED attribute using these CLI commands:<br>`config system sdwan`<br>`  config neighbor`<br>`  edit <bgp-peer-IP>`<br>`  set member <num_1> <num_n>`<br>`  set route-metric priority`<br>`  set health-check <health-check-name>`<br>`  next`<br>`  end`<br>`end`<br>Routes to prefixes behind spokes are advertised by the SD-WAN hub to eBGP peers on an external network. The relative values of the BGP MED attribute for each hub are used to indicate to eBGP peers the more preferred paths, namely, the preferred hub used to route to spoke prefixes.<br>This enhancement depends on the spoke SD-WAN configuration defined in the *Embed SLA priorities in ICMP probes* feature and hub SD-WAN and BGP configuration defined in the *Embed SLA status in ICMP probes* feature. |
| 1048430 | Hubs are not necessarily connected to all the same underlay transports as Spokes. For ADVPN 2.0, added support for shortcuts between Spokes using transports to which Hubs are not connected using overlay placeholders. For example, if Spokes are configured with an overlay over the Internet and an overlay over MPLS using this tunnel interface as a placeholder since it is not established with the Hub, ADVPN 2.0 allows a shortcut tunnel to be established over MPLS if this path is in-SLA and is the best quality. Each Spoke should be configured with these CLI commands:<br>`config vpn ipsec phase1-interface`<br>`  edit <placeholder_phase1_interface_name>`<br>`  set type dynamic`<br>`  ...`<br>`  set net-device enable`<br>`  ...`<br>`  set auto-discovery-dialup-placeholder enable`<br>`  next`<br>`end` |
| 1071495 | Users can now specify an SD-WAN zone as an interface in the following policies:<br>• Local-in policy<br>• DoS policy<br>• Interface policy<br>• Multicast policy<br>• TTL policy |

| Feature ID | Description |
|---|---|
| | • Central SNAT map<br>This update simplifies policy management and boosts operational efficiency. |

# Security Fabric

See Security Fabric in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 980693 | Add Known Exploited Vulnerabilities (KEVs) information to IoT/OT vulnerabilities stored in the user/device store, and display KEV counts and warnings accordingly on the GUI Asset Identity Center page, thereby enhancing security visibility for users. |
| 1034551 | OCI SDN connectors support IPv6 address objects. |
| 1038134 | GCP SDN connectors support IPv6 address objects. |
| 1039660 | Users can now hide non-relevant Security Rating tests, streamlining the user experience by displaying only pertinent information. |
| 1039849 | OCI SDN connectors support IPv6 for dynamic firewall addresses and high availability failover. |
| 1053400 | Generic Connector for Importing Addresses. This new feature allows seamless integration with any third-party database using a JSON-based REST API, converting each JSON entry into an address object on the FortiGate, thus automating the process and enhancing efficiency. |
| 1062547 | Introducing controls for CA (Certificate Authority) and CN (Common Name) fields. Previously, FortiSandbox could not verify certificates or automatically retrieve CNs from remote FSAs. Now, users can manually set a trusted CA and expected CN or enable automatic CN retrieval and verification, improving FortiSandbox TLS connection security. |
| 1089998 | Supports mTLS for threat feed (external resource) connections, allowing admins to configure a trusted client certificate for mTLS authentication during the TLS handshake. |

# Security Profiles

See Security profiles in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 968707 | In this enhancement, risk level rating is added to the FortiGuard URL rating service. FortiGate can query the rating service to retrieve the risk score for a URL. This risk score rates the likelihood that a website has malicious intent. This risk score and level can be used in a webfilter profile to apply a block or monitor action, or it can be used as a match criteria for a web proxy policy. |

| Feature ID | Description |
|---|---|
| 1027296 | A new `ocr-only` option has been added to the ICAP profile, allowing you to forward only image files (such as JPEG, JPG, PNG) relevant for OCR scanning to the ICAP server, such as FortiProxy. This selective forwarding applies exclusively to responses, not web requests. This feature enhances overall system efficiency by reducing processing time and optimizing resource usage.<br>`config icap profile`<br>`edit <name>`<br>`set ocr-only enable`<br>`next`<br>`end` |
| 1055921 | The inline CASB security profile has been enhanced to support control factors such as tenant information in JSON data exchanged between a web browser and a custom SaaS application. For example, for some custom SaaS applications, the URL does not change to reflect the type or identity of the user or organization when logged in as such tenant information is exchanged using JSON data instead of through changes in the URL. With this enhancement, JSON data can be extracted using JQ filters. |
| 1068910 | Streamline IoT/OT device detection. With this new feature, there's no longer a need to apply an Application Control profile. Users can now simply enable or disable IoT or OT categories directly for device detection. If these signatures aren't excluded in any policy interfaces, a built-in application list is automatically created and applied. This ensures the relevant IoT or OT categories are active, optimizing the IPS functionality and reducing the overall configuration complexity for users.<br>`config system interface`<br>`edit <name>`<br>`set device-identification enable`<br>`set exclude-signatures {ot \| iot)`<br>`next`<br>`end` |

# System

See System in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 752946 | To enhance the security of system administrator passwords, FortiGate now uses PBKDF2 as the hashing scheme with randomized salts to hash and store the password.<br>To maintain downgrade support, a new command is introduced:<br>`config system password-policy`<br>`set login-lockout-upon-downgrade {enable \| disable}`<br>`end` |

| Feature ID | Description |
|---|---|
| 812576 | Previously, customers had to register each Fortinet device to their FortiCare account individually. This new feature simplifies the process with a one-click solution, allowing customers to register all Fortinet devices in the same security fabric group at once. It lists all unregistered fabric components (FGT, FAP, FSW) and provides a *Register All* option, saving time and effort. |
| 861843 | Support Firmware Upgrade Report. This enhancement allows users to perform sanity checks by comparing configurations and statistics before and after a firewall upgrade, thereby enhancing the upgrade process and providing detailed assurance of successful upgrades. |
| 954888 | FortiGate A-P HA cluster now supports sharing a single FortiGuard service license for both cluster units for the following models and their variants: 40F, 60F, 70F, 80F, and 100F. |
| 1053978 | Subscriptions and FortiGuard settings are now organized into separate tabs with clear distinctions between licensed, expired, and available-for-purchase subscriptions, providing customers with a more intuitive and informative layout. |
| 1061119 | This enhancement reduces ipshelper CPU usage during the database update process, optimizing system performance and ensuring smoother operations. |
| 1066694 | For the FortiGate 7000F platform, you can use the following commands to control how traffic from individual VDOMs is load balanced to FPMs. By default, traffic from any VDOM is distributed to all FPMs using the `default dp-load-distribution-method`. However, you can set up groups of FPMs (called worker groups) and send traffic from individual VDOMs to a selected worker group.<br>Use the following command to create a new worker group:<br>`config system global`<br>`  config load-balance worker-group`<br>`  edit wrk-grp-678`<br>`  set member 6 7 8`<br>`end`<br>The default worker group (named default) sends traffic to all FPMs. You cannot edit or delete this worker group. By default, each VDOM is configured to send traffic to the default worker group. You can change the worker group that a VDOM sends traffic to by editing the VDOM and using the following command to change the worker group:<br>`config vdom`<br>`  edit root`<br>`  config system settings`<br>`  set dp-load-distribution-group wrk-grp-678`<br>`end`<br>You can also configure the load distribution method used for traffic for each VDOM:<br>`config vdom`<br>`  edit root`<br>`  config system settings`<br>`  set dp-load-distribution-method {to-primary \| src-ip \|dst-ip \| src-dst-ip \| src-ip-sport \| dst-ip-dport \| src-dst-ip-sport-dport \| derived}`<br>`end` |

| Feature ID | Description |
|---|---|
| 1087866 | Added route monitoring to FGSP, enhancing network stability by detecting route prefix withdrawals. This prevents traffic loss in complex environments and improves the UTM scanning experience. |
| 1088468 | Added SNMP objects for hyperscale CGN to allow users to retrieve CGN IP pool and session information using SNMP, simplifying management and enhancing resource monitoring. |

# User & Authentication

See Authentication in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 1040375 | Introducing *Bearer Token* authentication alongside the current pre-shared secret improves security between the SCIM server and client. The new bearer tokens, generated by FortiOS, are temporary, minimizing the risk of unauthorized access and adhering to modern security standards. |
| 1057309 | Dial-up IPsec with SAML using an external browser for authentication is supported starting from FortiOS 7.6.1, FortiClient versions 7.2.5 and 7.4.1 for Mac and Windows, and FortiClient version 7.4.3 for Linux. |

# VPN

See IPsec and SSL VPN in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 969747, 1072923 | Support Post-Quantum Cryptography (PQC) for IPsec key exchange, enhancing security with algorithms that protect against quantum computer attacks. This update ensures future-proof encryption and addresses vulnerabilities in traditional methods, aligning with upcoming security standards. |
| 1073893 | When TCP traffic goes through IPSec tunnel, FortiGate reduces the TCP MSS size if it is larger than the tunnel's MTU. When a large TCP packet enters IPSec tunnel, FortiGate will fragment the packet, and uses ICMP message *ICMP_FRAG_NEEDED* to notify the sender the MTU size. Then the sender can adjust the following packet size. |

# WiFi Controller

See Wireless in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 1043784 | In FortiOS, the WiFi controller supported the MPSK feature on a WPA2-Personal SSID by applying an MPSK profile or enabling RADIUS MAC authentication. However, for a WPA3-SAE SSID, the MPSK feature was only supported through the application of an MPSK profile. This enhancement allows WPA3-SAE SSIDs to utilize RADIUS MAC authentication to implement the MPSK feature. |
| 1044322 | The FortiGate WiFi Controller now supports uploading the portal servers certificate to the FortiAP. This allows the FortiAP to use the same server certificate to secure the HTTPS POST actions. With the corresponding CA imported on users devices, authentication is smoother and free of security warnings, enhancing the user experience. |

# ZTNA

See Zero Trust Network Access in the New Features Guide for more information.

| Feature ID | Description |
|---|---|
| 998798 | A ZTNA web portal is added for accessing applications directly within the portal without requiring FortiClient to be installed on the endpoint or a client certificate check. The ZTNA portal handles authentication and authorization of traffic destined for the protected resources. It is implemented entirely in WAD.<br>`config ztna web-portal`<br>`edit <name>`<br>`set vip <vip name>`<br>`set host <Virtual host name>`<br>`set auth-portal {enable \| disable}`<br>`set vip6 <Virtual IPv6 name>`<br>`set auth-rule <rule>`<br>`next`<br>`end`<br>`config ztna web-portal-bookmark`<br>`edit <name>`<br>`set users <users>`<br>`set groups <groups>`<br>`config bookmarks`<br>`edit <name>`<br>`set apptype {ftp \| rdp \| sftp \| smb \| ssh \| telnet \| vnc \| web}`<br>`set url <string>`<br>`set host <name or IP>`<br>`set description <Description>`<br>`set port <remote port>`<br>`set sso {enable \| disable}`<br>`next`<br>`end` |

| Feature ID | Description |
| --- | --- |
| | next<br>end |
| 1069002 | Added `ztna-ems-tag-negate` to ZTNA proxy policy. |

# Upgrade information

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

| FortiGate | Upgrade option | Details |
|---|---|---|
| Individual FortiGate devices | Manual update | Use the procedure in this topic.<br>See also Upgrading individual devices in the FortiOS Administration Guide. |
| | Automatic update based on FortiGuard upgrade path | See Enabling automatic firmware updates in the FortiOS Administration Guide for details |
| Multiple FortiGate devices in a Fortinet Security Fabric | Manual, immediate or scheduled update based on FortiGuard upgrade path | See Fortinet Security Fabric upgrade on page 39 and Upgrading all devices in the FortiOS Administration Guide. |

**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 7.6.1 is verified to work with these Fortinet products. This includes:

| | |
|---|---|
| **FortiAnalyzer** | • 7.6.1 |
| **FortiManager** | • 7.6.1 |
| **FortiExtender** | • 7.4.0 and later |
| **FortiSwitch OS (FortiLink support)** | • 6.4.6 build 0470 and later |

| | |
|---|---|
| **FortiAP** | • 7.2.2 and later |
| **FortiAP-U** | • 6.2.5 and later |
| **FortiAP-W2** | • 7.2.2 and later |
| **FortiClient EMS** | • 7.0.3 build 0229 and later |
| **FortiClient Microsoft Windows** | • 7.0.3 build 0193 and later |
| **FortiClient Mac OS X** | • 7.0.3 build 0131 and later |
| **FortiClient Linux** | • 7.0.3 build 0137 and later |
| **FortiClient iOS** | • 7.0.2 build 0036 and later |
| **FortiClient Android** | • 7.0.2 build 0031 and later |
| **FortiSandbox** | • 2.3.3 and later for post-transfer scanning<br>• 4.2.0 and later for post-transfer and inline scanning |

* 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.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.6.0, use FortiClient 7.6.0.

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 FortiExtender devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.6.1. When Security Fabric is enabled in FortiOS 7.6.1, all FortiGate devices must be running FortiOS 7.6.1.

# 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*.

# FortiGate 6000 and 7000 upgrade information

Upgrade FortiGate 6000 firmware from the management board GUI or CLI. Upgrade FortiGate 7000 firmware from the primary FIM GUI or CLI. The FortiGate 6000 management board and FPCs or the FortiGate 7000 FIMs and FPMs all run the same firmware image. Upgrading the firmware copies the firmware image to all components, which then install the new firmware and restart. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

On a standalone FortiGate 6000 or 7000, or an HA cluster with `uninterruptible-upgrade` disabled, the firmware upgrade interrupts traffic because all components upgrade in one step. These firmware upgrades should be done during a quiet time because traffic can be interrupted for a few minutes during the upgrade process.

Fortinet recommends running a graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Fortinet recommends that you review the services provided by your FortiGate 6000 or 7000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

**To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.6.1:**

1. Use the following command to set the `upgrade-mode` to `uninterruptible` to support HA graceful upgrade:

   ```
   config system ha
       set uninterruptible-upgrade enable
   end
   ```

   When upgrading from FortiOS 7.4.1 to a later version, use the following command to enable uninterruptible upgrade:

   ```
   config system ha
       set upgrade-mode uninterruptible
   end
   ```

2. Download the FortiOS 7.6.1 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.
5. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

# Default setting of cp-accel-mode is changed to none on 2GB memory models

This change disables CP acceleration to lower system memory usage thus can prevent some unexpected behavior due to lack of memory.

Previous FortiOS CLI behavior:

```
config ips global
    set cp-accel-mode advanced
end
```

New FortiOS CLI behavior after upgrade:

```
config ips global
    set cp-accel-mode none
end
```

This change will cause performance impact as CPU will do the pre-match (pattern match) inside IPS (CPU) instead of hardware engine (cp module in SOC4). Some customers could expect an increase in CPU utilization as a result.

FortiGate and FortiWiFi 4xF/6xF families are affected by this change.

# Policies that use an interface show missing or empty values after an upgrade

If local-in policy, DoS policy, interface policy, multicast policy, TTL policy, or central SNAT map used an interface in version 7.4.5, 7.6.0 GA or any previous GA version that was part of the SD-WAN zone, these policies will be deleted or show empty values after upgrading to version 7.4.6 or 7.6.1.

After upgrading to version 7.4.6 or 7.6.1 GA, users must manually recreate these policies and assign them to the appropriate SD-WAN zone.

# Managed FortiSwitch do not permit empty passwords for administrator accounts

Starting from FortiOS version 7.6.1, a managed FortiSwitch no longer permits empty passwords for the admin account. If a FortiSwitch unit was previously authorized without an admin password, the FortiGate will automatically generate a random admin password for the FortiSwitch upon upgrading to 7.6.1. This change will cause the admin to lose access.

To regain access, configure a password override on the FortiGate device using the following commands:

```
config switch-controller switch-profile
    edit default
        set login-passwd-override enable
        set login-passwd <passwd>
    next
end
```

FortiSwitch units with an existing admin password will not be affected by this change.

# Removed speed setting affects SFP+ interfaces after upgrade

Starting in FortiOS 7.6.1, the `1000auto` speed setting is removed. If a FortiGate SFP+ port speed is set to `1000auto` before upgrade, the upgrade process automatically changes the setting to `10000full`. This change can cause the interface to go down when the connecting device has a different speed setting.

**Workaround**: After upgrade, align the port settings. Edit the port and set the speed to `1000full` to restore the connection.

```
config system interface
    edit <port>
        set speed 1000full
    next
end
```

# Product integration and support

The following table lists FortiOS 7.6.1 product integration and support information:

| | |
|---|---|
| **Web browsers** | • Microsoft Edge 135<br>• Mozilla Firefox version 138<br>• Google Chrome version 136<br>Other browser versions have not been tested, but may fully function.<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **Explicit web proxy browser** | • Microsoft Edge 135<br>• Mozilla Firefox version 138<br>• Google Chrome version 136<br>Other browser versions have not been tested, but may fully function.<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **FortiController** | • 5.2.5 and later<br>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C |
| **Fortinet Single Sign-On (FSSO)** | • 5.0 build 0319 and later (needed for FSSO agent support OU in group filters)<br>  • Windows Server 2022 Standard<br>  • Windows Server 2022 Datacenter<br>  • Windows Server 2019 Standard<br>  • Windows Server 2019 Datacenter<br>  • Windows Server 2019 Core<br>  • Windows Server 2016 Datacenter<br>  • Windows Server 2016 Standard<br>  • Windows Server 2016 Core<br>  • Windows Server 2012 Standard<br>  • Windows Server 2012 R2 Standard<br>  • Windows Server 2012 Core<br>  • Novell eDirectory 8.8 |
| **AV Engine** | • 7.00034 |
| **IPS Engine** | • 7.01026 |

See also:

- Virtualization environments on page 46
- Language support on page 46
- SSL VPN support on page 47
- FortiExtender modem firmware compatibility on page 47

# Virtualization environments

The following table lists hypervisors and recommended versions.

| Hypervisor | Recommended versions |
|---|---|
| **Citrix Hypervisor** | • 8.2 Express Edition, CU1 |
| **Linux KVM** | • Ubuntu 22.04.3 LTS<br>• Red Hat Enterprise Linux release 9.4<br>• SUSE Linux Enterprise Server 12 SP3 release 12.3 |
| **Microsoft Windows Server** | • Windows Server 2022 |
| **Windows Hyper-V Server** | • Microsoft Hyper-V Server 2022 |
| **Open source XenServer** | • Version 3.4.3<br>• Version 4.1 and later |
| **VMware ESXi** | • Versions 6.5, 6.7, 7.0, and 8.0. |

# 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 138<br>Google Chrome version 136 |
| Microsoft Windows 10 (64-bit) | Microsoft Edge 135<br>Mozilla Firefox version 138<br>Google Chrome version 136 |
| Ubuntu 20.04 (64-bit) | Mozilla Firefox version 138<br>Google Chrome version 136 |
| macOS Ventura 13.1 | Apple Safari version 18<br>Mozilla Firefox version 137<br>Google Chrome version 136 |
| iOS | Apple Safari<br>Mozilla Firefox<br>Google Chrome |
| Android | Mozilla Firefox<br>Google Chrome |

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

# FortiExtender modem firmware compatibility

The following table lists the modem firmware file name and version for each FortiExtender model and its compatible geographical region.

| FortiExtender model | Modem firmware image name | Modem firmware file on Support site | Geographical region |
|---|---|---|---|
| FEX-101F-AM | FEM_EM06A-22-1-1 | FEM_EM06A-22.1.1-build0001.out | America |

| FortiExtender model | Modem firmware image name | Modem firmware file on Support site | Geographical region |
|---|---|---|---|
| FEX-101F-EA | FEM_EM06E-22-01-01 | FEM_EM06E-22.1.1-build0001.out | EU |
| | FEM_EM06E-22.2.2 | FEM_EM06E-22.2.2-build0002.out | EU |
| FEX-201E | FEM_06-19-0-0-AMEU | FEM_06-19.0.0-build0000-AMEU.out | America and EU |
| | FEM_06-19-1-0-AMEU | FEM_06-19.1.0-build0001-AMEU.out | America and EU |
| | FEM_06-22-1-1-AMEU | FEM_06-22.1.1-build0001-AMEU.out | America and EU |
| | FEM_06-22-1-2-AMEU | FEM_06-22.1.2-build0001-AMEU.out | America and EU |
| FEX-201F-AM | FEM_07A-22-1-0-AMERICA | FEM_07A-22.1.0-build0001-AMERICA.out | America |
| | FEM_07A-22-2-0-AMERICA | FEM_07A-22.2.0-build0002-AMERICA.out | America |
| FEX-201F-EA | FEM_07E-22-0-0-WRLD | FEM_07E-22.0.0-build0001-WRLD.out | World |
| | FEM_07E-22-1-1-WRLD | FEM_07E-22.1.1-build0001-WRLD.out | World |
| FEX-202F-AM | FEM_07A-22-1-0-AMERICA | FEM_07A-22.1.0-build0001-AMERICA.out | America |
| | FEM_07A-22-2-0-AMERICA | FEM_07A-22.2.0-build0002-AMERICA.out | America |
| FEX-202F-EA | FEM_07E-22-1-1-WRLD | FEM_07E-22.1.1-build0001-WRLD.out | World |
| FEX-211E | FEM_12-19-1-0-WRLD | FEM_12-19.1.0-build0001-WRLD.out | World |
| | FEM_12-19-2-0-WRLD | FEM_12-19.2.0-build0002-WRLD.out | World |
| | FEM_12-22-1-0-AMEU | FEM_12-22.0.0-build0001-AMEU.out | America and EU |
| | FEM_12-22-1-1-WRLD | FEM_12-22.1.1-build0001-WRLD.out | World |
| FEV-211F_AM | FEM_12_EM7511-22-1-2-AMERICA | FEM_12_EM7511-22.1.2-build0001-AMERICA.out | America |
| FEV-211F | FEM_12-22-1-0-AMEU | FEM_12-22.1.0-build0001-AMEU.out | World |
| FEX-211F-AM | FEM_12_EM7511-22-1-2-AMERICA | FEM_12_EM7511-22.1.2-build0001-AMERICA.out | America |
| FEX-212F | FEM_12-19-2-0-WRLD | FEM_12-19.2.0-build0002-WRLD.out | World |
| | FEM_12-22-1-1-WRLD | FEM_12-22.1.1-build0001-WRLD.out | World |

| FortiExtender model | Modem firmware image name | Modem firmware file on Support site | Geographical region |
|---|---|---|---|
| FEX-311F | FEM_EM160-22-02-03 | FEM_EM160-22.2.3-build0001.out | World |
| | FEM_EM160-22-1-2 | FEM_EM160-22.1.2-build0001.out | World |
| FEX-511F | FEM_RM502Q-21-2-2 | FEM_RM502Q-21.2.2-build0003.out | World |
| | FEM_RM502Q-22-03-03 | FEM_RM502Q-22.3.3-build0004.out | World |
| | FEM_RM502Q-22-04-04-AU | FEM_RM502Q-22.4.4-build0005_AU.out | Australia |
| | FEM_RM502Q-22-1-1 | FEM_RM502Q-22.1.1-build0001.out | World |
| | FEM_RM502Q-22-2-2 | FEM_RM502Q-22.2.2-build0002.out | World |

The modem firmware can also be uploaded manually by downloading the file from the Fortinet Customer Service & Support site. The firmware file names are listed in the third column of the table.

**To download the modem firmware:**

1. Go to https://support.fortinet.com/Download/FirmwareImages.aspx.
2. From the *Select Product* dropdown, select *FortiExtender*.
3. Select the *Download* tab.
4. Click *MODEM-Firmware*.
5. Select the FortiExtender model and image name, then download the firmware file.

# Resolved issues

The following issues have been fixed in version 7.6.1. To inquire about a particular bug, please contact Customer Service & Support.

## Anti Spam

| Bug ID | Description |
|---|---|
| 1050805 | Client termination occurs during email processing when inserting antispam tags in emails lacking body sections or delimiters, particularly with multipart base64 encoded data. |

## Anti Virus

| Bug ID | Description |
|---|---|
| 1044961 | On FortiGate, the Scanunit does not work as expected due to zlib data check issue. |
| 1055609 | Files are dropped by Quard when sending to FortiSandbox under heavy load, as new connections are established despite existing ones being active. |
| 1058701 | On FortiGate, the `av-mem-limit` does not work as expected when `set av-failopen pass` configured due to a memory usage issue. |
| 1068321 | Previous unsigned MMDB and AVAI databases are kept after upgrading FortiOS. |
| 1073326 | Entry-level FortiGate's with 2GB of memory may encounter a memory usage issue during FGD-based firmware upgrades causing the AV engine to restart. |
| 1078882 | Scanunit tries to scan with no payload, resulting in an error message from FortiNDR and generating an error on FortiGate. |
| 1070864, 1082877 | The scanunit shows error messages that do not provide enough detail when corrupt AV engine or DB events occur. |

# Application Control

| Bug ID | Description |
|---|---|
| 951150 | The Zoom meeting remote control feature is not blocked during meetings. |
| 990540 | FortiGate does not generate traffic logs for established or denied TCP sessions that lack application data. |
| 1060562 | The application control profile is missing on the GUI for FortiGate models with 2GB of memory. |
| 1064413 | Traffic fails to follow SD-WAN rules when SNAT is enabled and "snat-route-change" is activated due to session drops caused by SNAT check failures after route changes. |
| 1066078, 1066567 | Application classification fails when SSL inspection is bypassed, causing Inline IPS to miss blocking certain apps like Tencent Meeting and Facebook due to incomplete traffic processing. |

# Data Loss Prevention

| Bug ID | Description |
|---|---|
| 908279 | The DLP incorrectly detects a .pdf file as a .mpeg file and blocks the download. |
| 984784 | When a DLP profile is set to MAPI, there is a slow connection between Outlook and the Exchange server. |
| 1049719 | The DLP dictionary with a regex configuration does not deny an accent mark on FortiGate. |

# DNS Filter

| Bug ID | Description |
|---|---|
| 1058866 | DNS translation does not work as expected when a resolved IP matches the external block list entry. |
| 1086355 | DNS query logs are not logged on FortiGate when traffic uses a VIP mapped to a loopback interface hosting a DNS server. |

# Endpoint Control

| Bug ID | Description |
|---|---|
| 1055192 | Downstream FortiGates incorrectly send a REST API request to declare themselves as root to EMS, causing potential management issues in Fabric trees. |

# Explicit Proxy

| Bug ID | Description |
|---|---|
| 900911 | When `secure-web-proxy` is enabled, if the client disconnects without sending any data as soon as the TCP connection with FortiGate is established, a WAD process signal 11 error occurs. |
| 1015722 | WAD auto-tuning is not working ideally for various cases, resulting in throughput for single file downloads not reaching the ideal speed when `tcp-window-type` is set to `auto-tuning`. |
| 1056600 | FortiGate experiences a WAD process issue and produces a *wad_find_fwdsvr_by_key* error. |
| 1076642 | Unable to load pages with cloudflare protected websites with auth enabled, if Auth scheme is set to Form-Based in explicit proxy. |

# File Filter

| Bug ID | Description |
|---|---|
| 1011320 | Adding File Filter to a flow-based firewall policy may impact performance. |
| 1095866 | Clients incorrectly believe write operations succeed when WAD blocks SMB file uploads due to forwarded success responses. |

# Firewall

| Bug ID | Description |
|---|---|
| 996622 | On FortiGate, the IPv6 real server shown as DOWN by the health check but it is considered UP in the kernel. |

| Bug ID | Description |
|---|---|
| 1007029 | On FortiGate, connections are disrupted between client email exchange servers and a virtual server when HTTP2 support is enabled. |
| 1007566 | When the FortiGate has thousands of addresses and hundreds address groups, the GUI can take a few minutes to search for a specific address inside the address group dialog. |
| 1028356 | Incorrect DNAT hit counts are displayed when VIP order is changed in Central NAT. |
| 1030516 | An internet interface with egress/outbound shaping encounters a performance issue with sla after rebooting. |
| 1047208 | The FortiGate virtual server does not setup an http2 connection with a WebSocket server due to a WAD process issue. |
| 1050864 | No route is found when FTP server attempts to connect back to client in active mode due to incorrect dst inheritance from master session. |
| 1051891 | The SNMP fgIpsAnomalyDetections counter does not increase if the DoS policy is configured in a no management VDOM. |
| 1052334 | The firewall policy name length validation does not work with Korean characters. |
| 1055733 | The F5 HTTP/S monitors for the web server in FortiGate do not function as expected due to HTTP 0.9 traffic. |
| 1057080 | On the *Firewall Policy* page, search results do not display in an expanded format. |
| 1058494 | When `snat-hairpin-traffic` is enabled, SNAT is not automatically applied to hairpin traffic, causing a SNAT mismatch in `strict-dirty-session-check`. |
| 1059989 | Modifying the shaping profile, whether it is assigned to an interface or not, results in IPsec tunnels going down. |
| 1060452 | FortiGate in policy-based mode showing the incorrect policy ID in forward traffic logs. |
| 1062333 | FortiGate does not reply to an ARP request when VIP is disabled due to an iplist reference issue. |
| 1064748 | FortiGate incorrectly uses outgoing interface IP instead of configured IPPool for SNAT when HTTP multiplexing is enabled on a load balancer VIP. |
| 1068393 | Incorrect matching of zones and SD-WAN zones occurs where interfaces do not exist. |
| 1078662 | If an interface on an NP7 platform has the `set inbandwidth XXX`, `set outbandwidth XXX`, and `set egress-shaping-profile XX` settings, the following issues may occur:<br>• Fragment packet checksum is incorrect.<br>• MTU is not honored when sending packets out.<br>• QTM hangs and blocks traffic when packet size is larger than 6000 bytes.<br>**Workaround**:<br>`config system interface`<br>`edit xxx`<br>`unset egress-shaping-profile`<br>`next`<br>`end` |

| Bug ID | Description |
|---|---|
| 1079590 | Reply traffic isn't sent out of FortiGate when heavy traffic fills up the txqueue on EMAC VLAN interfaces. |
| 1081542 | Packet drops occur when high traffic causes nTurbo buffers to be reused without proper initialization under CPU-intensive conditions with ASIC offloading enabled. |
| 1088905 | The Virtual Server HTTP `healthcheck` uses the IP address as a Host even when the full URL is configured in `http-get`. |

# FortiGate 6000 and 7000 platforms

| Bug ID | Description |
|---|---|
| 986845 | On FortiOS, the *Security Fabric* widget does not display information on blade status. |
| 997161 | On FortiGate 6000 FPCs and FortiGate 7000 FPMs the node process may consume large amounts of CPU resources, possibly affecting FPC or FPM performance. (You can run the `diagnose sys top` command from an FPC or FPM CLI to view CPU usage.) This problem may be caused by security rating result submission. |
| 1016439 | Enabling or disabling a vcluster causes some backup routes (proto = 20) to be lost when a routing table has a significant amount of routes (over 10000 routes). |
| 1032573 | In an HA configuration, FortiGate does not respond to SNMP queries causing the device to display as being DOWN. |
| 1035601 | An SNMP query for policy statistics returns 0 on MBD. |
| 1037965 | When applying a script to a configuration, the updated configuration is applied to the FIM but is not fully synchronized on the FPCs. |
| 1048808 | If the secondary reboots, after it rejoins the cluster SIP sessions are not resynchronized. |
| 1050727 | MAC info packets carrying session sync data are dropped under asymmetric routing conditions with L2 connections available. |
| 1056894 | On the FortiGate 6000 platform, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed. |
| 1057499 | FIM interfaces are DOWN after restoring the root VDOM configuration due to a speed issue. |
| 1060619 | CSF is not working as expected. |
| 1086889 | FIM encounters a split-brain scenario after rebooting. |
| 1088402 | On FortiGate 6K/7K FGSP clusters, the configuration does not synchronize properly with `standalone-config-sync` enabled. |
| 1106519 | ISDB/FFDB was out-of-sync from MBD to FPCs after running `exec update-now` on 6K/7K platform. |

| Bug ID | Description |
|---|---|
| 1081015, | ISDB updates fail during FortiGate database synchronization attempts due to missing FFDB package handling and failed temporary file transfers. |
| 1086953 | FIMs can be in split-brain state when one FIM reboots, leading to incorrect master election and network instability. |

# FortiView

| Bug ID | Description |
|---|---|
| 1009287 | On the *Dashboard* > *FortiView Sessions* page, closing a large number of FortiView sessions (+100) can take longer than expected and result in a CPU usage issue. |
| 1029254 | When trying to filter by device using the *1 week* filter option, the *User device store query error (error code: -1)* error message is displayed. |
| 1077555 | On FortiGate, the *Top Threat - WAN* does not show the correct information for the IPS Logs. |

# GUI

| Bug ID | Description |
|---|---|
| 885427 | On the *Network* > *Interfaces* page, the SFP port is grayed out on the faceplate diagram even though the port is working. This is purely a GUI display issue and does not affect system operation.<br>**Workaround**: View the SFP port information and status using the `interface list` in the CLI. |
| 989512 | When the number of users in the *Firewall User* monitor exceeds 2000, the search bar, column filters, and graphs are no longer displayed due to results being lazily loaded. |
| 991573 | In the *Assets* widget preview window of the *Asset & Identities* widget, clicking the *Refresh* button does not update the data. |
| 1009143 | On FortiOS, the time displayed in the CLI and in the GUI do not match. |
| 1018682 | When creating a firewall policy, applications groups with custom application signatures cannot be saved using the GUI. |
| 1035356 | The WAN interface is accessible in the GUI under certain interface configurations even though it is not allowed in the configuration file. |
| 1044745 | On the *Dashboard* > *User & Devices* page on a VDOM, the *Address* column shows multiple devices with the FortiGate VLAN gateway instead of the Client IP. |

| Bug ID | Description |
|---|---|
| 1050865 | When updating an administrator password in the GUI, the password expiration date does not update when the new password is created. |
| 1052040 | The *IP/Netmask* column of HA management port hangs in the GUI. |
| 1052895 | GUI fails to fetch files from FortiGuard on HA secondary unit with HTTP 500 error. |
| 1056800 | On FortiOS, IPSec localid cannot be deleted using the GUI. |
| 1057628 | *Catch WebSocket* errors from *PerMessageDeflate* occur when the client abruptly closes the connection. |
| 1058473 | Expired licenses are still displayed in the GUI after 30 days. |
| 1058608 | The FortiGate Cloud status incorrectly shows as Activated after logging out using the GUI dashboard. |
| 1062753 | Incorrect percentage is displayed in the dashboard widget for "Files Uploaded Today" to Sandbox. |
| 1068202 | On low end models, the service list is empty when selecting members for a Service Group. |
| 1071907 | In the GUI, there is no setting for the type option for the *npu_vlink* interface. |
| 1081912 | When inserting a policy using the new layout, the destination information is not displayed. |
| 1087857 | On the *Policy & Objects* > *Firewall Policy* page in the GUI on the secondary FortiGate in an HA cluster, create a new address, and the page keeps loading. |
| 1092475 | On the *Policy & Objects* > *Firewall Policy* page, in the *Edit Policy* dialog, the GTP-profile do not display in the GUI when Central SNAT is enabled. |

# HA

| Bug ID | Description |
|---|---|
| 824651 | Certificate upload causes HA checksum mismatch. |
| 965217 | In an HA configuration, FortiGate may experience intermittent heartbeat loss causing unexpected failover to the secondary unit. |
| 1007516 | Rx_dropped counters increase on ha1 and ha2 interfaces, causing them to flap and resulting in FGSP member loss during high session and CPU usage spikes. |
| 1009939 | When bandwidth is low, the *tftp backup* command on the secondary unit does not work as expected when it should be able to reach the server. |
| 1026794 | The HA secondary FortiGate logical topology page shows the *FAZ* connected interface as *FortiAnalyzer*. |
| 1036139 | FortiGate encounters a memory usage issue caused by cmdbsvr and hasync. |

| Bug ID | Description |
|---|---|
| 1047094 | The HA Secondary unit cannot communicate with FortiGate Cloud when it uses *standalone-mgmt-vdom* using the HA Primary unit. |
| 1052320 | In a vCluster configuration, traffic stops after a VDOM failover. |
| 1052532 | Newly created VDOM is not synchronized for a while after secondary reboots. |
| 1054041 | On FortiGate's in an HA environment, DHCP clients can not get an IPv4 address from the server with vcluster. |
| 1055336 | Using the *Test User Credentials* button from the Radius Server in the GUI does not honor the custom `nas-id-type`. |
| 1056138 | On FortiGate 120G and 121G models in an HA cluster, if the `ha` or `mgmt` interface is used as the heartbeat interface, the HA cluster may not synchronize and the GUI HA page may not load.<br>**Workaround**: Do not use `ha` or `mgmt` interface as heartbeat interface.<br>Or:<br>Review the upgrade path when upgrading FGT-120G/FGT-121G in HA cluster from 7.0.x to 7.2.11 build 1740 or later. When 7.2.10 build 1706 is a part of the upgrade path, exclude 7.2.10 build 1706 from the upgrade path, and upgrading directly to 7.2.11 build 17140 or later to form HA cluster successfully without issues. |
| 1056651 | Static routes configured under the secondary unit's `standalone-mgmt-vdom` do not take effect. |
| 1060006 | Rebooting a member in an FGSP cluster with standalone-config-sync enabled may cause desynchronization due to port_ha communication failure. |
| 1060023 | High CPU load occurs due to recursive session syncs between primary and secondary HA nodes during URL category ID updates. |
| 1061492 | The HA secondary device sends GARP with the wrong MAC address after the vcluster is removed. |
| 1064728 | UDP single-packet sessions cause a race condition during expiration, leading to inconsistent synchronization between primary and secondary FGCP clusters, resulting in an imbalance of session counts across units. |
| 1067274 | Reply packets fail to reach the session owner instance in FortiOS asymmetric L3 FGSP deployments, causing network loops and preventing TCP connections from forming. |
| 1070745 | Sessions may not fail back to the original FGSP peer that owns the session if either the interface name for the `monitor-interface` or `pingsvr-monitor-interface` is 7 characters or longer. |
| 1070901 | The `fgsp_route_health` status is incorrect when configuring a `monitor-interface` or `link-monitor-interface` with a long interface name. |
| 1084662 | Inconsistent FFDB signed statuses occur on secondary blades when a signature file fails to synchronize during HA database sync events. |
| 1085371 | SNMP v3 times out in FortiGate Azure/AWS in HA setup. |
| 1092547 | FortiGate in an HA configuration keeps rebooting continuously during a firmware upgrade. |

# Hyperscale

| Bug ID | Description |
|---|---|
| 1042512 | On FortiGate, the *CGN Resource Quota* field allows an invalid value to be set. |
| 1047362 | Decoding errors occur when Netflow data packets contain certain values for each NPU but lack corresponding templates for proper interpretation. |
| 1075915 | NP gets stuck during extended traffic with specific DoS anomalies due to MSE hash table issues from depfail. |
| 1090234 | The system crashes due to a null pointer dereference when the hairpin session query function accesses uninitialized pointers after ICMP rate control functions were incorrectly added. |

# ICAP

| Bug ID | Description |
|---|---|
| 1072282 | HTTP 400 errors occur due to missing space after status code in converted HTTP responses. |

# Intrusion Prevention

| Bug ID | Description |
|---|---|
| 891295 | FortiGate experiences a performance issue with geography-type addresses matching in NGFW policy mode. |
| 1001860 | On the *Security Profiles* > *Intrusion Prevention* page, when a new IPS filter is created with no filter selected, the *Details* column of the IPS Signatures and Filters table is blank instead of *All Attributes*. |
| 1016531 | FortiGate encounters a memory usage issue in the IPSengine when `av-failopen` is set to `pass`. |
| 1040783 | FortiGate encounters CPU usage issue due to IPSEngine utilization when using an `app-ctrl utm` profile. |
| 1061119 | This enhancement reduces ipshelper CPU usage during the database update process, optimizing system performance and ensuring smoother operations. |
| 1066151 | Forticron runs `diagnose ips debug disable all` and `diagnose ips ssl debug none` constantly due to a processing issue. |
| 1086789 | High CPU usage due to an uninitialized return value in the load balance comparison function when SD-WAN load balancing is enabled. |
| 1090134 | IPS engine re-initialization after receiving a threat feed update from an external resource. |

# IPsec VPN

| Bug ID | Description |
|---|---|
| 1002345 | IKE daemon randomly does not operate as expected during phase1 rekeying depending on soft rekey margin, timing, and packet ordering. |
| 1018749 | IPsec inserted SA's are not deleted successfully after flushing all tunnels. |
| 1020690 | The *IPsec Aggregate* interface displays as DOWN on the *Network* > *Interfaces* and the *Policy & Objects* > *Firewall Policy* pages when the member including the Dialup VPN is actually UP. This is purely a GUI display issue and does affect system operation. The correct status is shown on the *VPN* > *IPsec Tunnels* page. |
| 1023871 | IPSec IKEv2 with SAML cannot match the Entra ID group during EAP due to a buffer size issue. |
| 1024558 | IPsec interfaces created on `802.1ad + 802.3ad` interfaces with NP offloading enable do not work as expected after a firmware upgrade. |
| 1027537 | On the SOC4 platform, L2TP & ETHERIP traffic does not traverse through an IPSec tunnel with NP offload enabled. |
| 1031963 | On the *Policy & Objects* > *Firewall Policy* page, the firewall `hit` and `bytes` counts display values of *0* in a policy-based VPN. |
| 1039988 | When performing a SAML authentication, authd gets stuck in a loop due to a CPU usage issue. |
| 1041019 | When QKD dialup is enabled, IKE SA cannot establish a connection and generates an error. |
| 1042324 | The Phase1 monitor BGP remains active when the tunnel is DOWN. |
| 1049015 | IPsec performance issue on Intel-based platforms occurs due to FOS not enabling all available IPsec drivers. |
| 1050646 | FortiGate does not always send the full Server Certificate Chain causing disconnections with IKEv2 VPN using the native Windows client. |
| 1054953 | If *IKEv2* is selected during the VPN FortiClient Remote Access wizard setup in the GUI, the Extensible Authentication Protocol (EAP) configuration cannot be selected using the GUI. |
| 1057165 | The IPsec tunnel with QKD experiences flapping each time a DHCP configuration/interface update occurs. |
| 1058691 | The IPsec VPN tunnel on the branch unit does not terminate even when the remote gateway IP address becomes unavailable. |
| 1059778 | IPsec does not work as expected when the traffic path is from spoke dial-up to hub1, and then from hub1 to another site using a site-to-site tunnel. |
| 1060048 | Throughput is limited in Site to Site VPN connections between the FW1kF and the FWVM Google Cloud platform. |
| 1061925 | IPsec tunnels are flushed when unrelated changes are made in the system. |

| Bug ID | Description |
|---|---|
| 1064078 | Egress shaper fails to enforce bandwidth limits on VPN ID with IPIP encapsulation IPsec interfaces due to incorrect handling of traffic forwarding across multiple network processing units. |
| 1073995 | Authentication for native iOS IPsec VPN user with FortiToken 2FA does not work as expected. |
| 1075112 | FortiGate enters into conserve mode due to IKED encountering a memory usage issue. |
| 1076636 | Unexpected behavior in IKED occurs when a peer attempts to negotiate with two different gateway profiles simultaneously. |
| 1077122 | The Phase2 SA is present in the kernel but there is no IKE Phase1 SA after an HA upgrade. |
| 1080164 | Tcp-MSS settings are not applied to IPv6 traffic when configured on egress interfaces. |
| 1080420 | Tunnel fails when DPD is enabled because FortiGate does not increment its receive message ID after processing an unexpected payload, causing out-of-sync message IDs and ignoring subsequent DPD requests. |
| 1081951 | FortiGate encounters a steadily increasing IKED memory usage issue after upgrading to version 7.4.5. |
| 1082624 | EAP authentication fails for local users specified directly in firewall policies, while RADIUS users authenticate successfully. |
| 1126436 | The IKE TCP port is exposed on all IP addresses and interfaces when no local-in firewall policy regulates the traffic. |

# Log & Report

| Bug ID | Description |
|---|---|
| 979200 | In a Policy-Based NGFW, if there is no rule hit in `central-snat` and session never gets established, there will be no traffic log. |
| 1001583 | On the *Log & Report* > *Forward Traffic* page, the GUI experiences a performance issue and reverts to the last input when multiple ports are added to a filter for destination ports. |
| 1024570 | The SSH deep-inspection with `unsupported-version bypass > log information` is not showing. |
| 1024990 | Local-out traffic logs appear when FortiGate initiates internal processes like certificate probes or FGD queries, causing policyid=0 and srcintf="root" entries in kernel-level logs. |
| 1031342 | On the *Security Traffic Log* > *Security* tab, the *Details* page displays data with a *1/500 log fetched* prompt. |
| 1034824 | On the *Log & Report* > *Forward Traffic* page, application icons may not display in the *Application Name* column. |

| Bug ID | Description |
|---|---|
| 1044092 | When filtering forward traffic logs using FortiAnalyzer as a source, data takes longer than expected to load and generates a memory error message. |
| 1045253 | Log items cannot be created and sent to FortiGate Cloud log server when confirm queue becomes full. |
| 1050071 | The `unset pac-file-data` from pac-policy does not generate a system event log and the pac-file-data is deleted. |
| 1053334 | The `appcat` log field is not included in the IoT signature logs. |
| 1053412 | Alert email displays an error for *FDS-license-expiring*. |
| 1060204 | When the threat feed download times out, a system event log is not generated. |
| 1060316 | Event logs are generated with *CLEAR TEXT PASSWORD* when using the `diagnose test authserver tacacs*...` command. |
| 1074236 | FortiGate cannot connect to FortiAnalyzer due to a hostname resolution issue. |
| 1083537 | Serial numbers are lost in FortiAnalyzer when high availability information packets lack serial number data, causing cached entries to expire and be removed. |
| 1086191 | An error condition is observed in the `fgtlod` daemon when FortiCloud uses FortiAnalyzer-Cloud for backend logging. |
| 1087067 | On the *Log Viewer* page in *Log & Report* > *Forward Traffic*, the UTM log *Matching log* page keeps loading under the *Log Details* > *Security* tab. |
| 1088385 | FortiGate intermittently loses the FortiAnalyzer serial number and is required to verify again the FortiAnalyzer serial number and certificate. |
| 1091064 | Missing poluuid and policyname fields occur in Forward Traffic logs when HA failover happens in FGCP clusters. |

# Proxy

| Bug ID | Description |
|---|---|
| 916178 | FortiGate encounters an issue with the WAD daemon when deep inspection and SSL exemption are enabled while visiting a server with an expired certificate. |
| 979502 | On FortiGate, when the `waps` file is broken, the WAD process does not start. |
| 1018780 | FortiGate encounters a memory usage issue caused by the WAD process after an upgrade. |
| 1020828 | An HTTP2 stream issue causes an error condition in the WAD. |
| 1023127 | WAD crashes on the FGTs with signal 11. |

| Bug ID | Description |
|---|---|
| 1042055 | On FortiGate, an interruption occurs in the WAD process when in proxy-mode causing the unit to go into memory conserve mode. |
| 1043423 | Unexpected behavior is observed in the WAD user info history daemon due to erroneous memory allocation. |
| 1047441 | On FortiGate, the WAD process may not work as expected with H2 traffic when creating UTM logs. |
| 1048296 | FortiGate experiences an HTTP2 framing error when accessing websites using proxy mode with deep inspection configured due to a frame sizing issue in the WAD process. |
| 1054052 | The WAD process does not load a self-sign certificate when `set admin-server-cert self-sign` is configured in an explicit proxy. |
| 1054835 | HTTP/2 large file transfers are slow when IPS, APP, or SSL inspect-all is enabled due to excessive buffering during traffic forwarding. |
| 1056127 | An error condition occurs in the WAD process due to a rare error case during the SSL handshake. |
| 1057442 | On FortiGate, erroneous memory allocation is observed in the WAD process. |
| 1057488 | On FortiGate, unexpected behavior is observed in the WAD process during the HTTP session freeing. |
| 1060812 | Botnet detection fails in transparent proxy setups caused by implementation error. |
| 1062516 | The WAD process does not work as expected when FortiGate is configured as a HTTP load balancer with an HTTP session and changes are made to the virtual server live. |
| 1064758 | The *Protocol* option tcp window size in a proxy policy does not work as expected. |
| 1067014 | All wad-workers encounter a gradual memory usage issue, `/proc/pid/maps` shows increasing symbolic links to `/tmp/casb_shm`. |
| 1067942 | An error occurs in the WAD process when DoH traffic is sent to a transparent proxy after enabling HTTP policy redirect, and without having a transparent proxy configured. |
| 1068747 | WAD process fails to boot up and crashes if waps file is broken. |
| 1069896 | A wad-worker experiences a memory usage issue increase over several days. |
| 1078385 | FortiGate experiences a memory usage issue in the WAD process when sending AVDBs updates from the config daemon to workers. |

# REST API

| Bug ID | Description |
|---|---|
| 989677 | Update JavaScripts to the latest Long Term Support version. |

| Bug ID | Description |
|---|---|
| 1057999 | REST API returns an HTTP 500 error when `ssl-static-key-ciphers` is enabled under `config system global`. |
| 1074529 | Renaming an address object using the cmdb API in workspace mode transactions creates a new object instead of updating the existing one. |

# Routing

| Bug ID | Description |
|---|---|
| 969992 | On FortiGate, SCTP traffic does not follow the routing table. |
| 981876 | VRRP master stops sending advertisement messages for three seconds randomly during HA cluster operations in multi-VLAN environments. |
| 1003756 | When creating a rule on the *Network* > *Routing Objects* page, the *Prefix-list* is set to *0.0.0.0 0.0.0.0* when an incorrect format is entered in the *Prefix* field. |
| 1006753 | When renewing the LTE WWAN IP, some packets are sent using the old IP address causing traffic to drop. |
| 1011816 | The BGP neighbor range with a space in the name is ignored. |
| 1023109 | On the *Network* > *Interfaces* page, the vlan interface and IPSec tunnel interface are not displayed in the GUI after an upgrade. This is a cosmetic issue and does not affect functionality. |
| 1027847 | FortiGate does not include the `ecmp-max-paths` setting in the configuration. |
| 1029460 | Creating a BGP IPv4 network prefix or neighbor in the GUI unintentionally creates an empty IPv6 network prefix. |
| 1041812 | In a hub and spoke HA configuration, *SD-WAN* pages take longer than expected to load in the GUI when there are a large number of spokes (~350) configured. |
| 1042909 | When creating a new static route on the *Network* > *Static Routes* page, the *Priority* field still displays when the *Destination* is switched from *Subnet* to *Internet Service*. |
| 1046169 | On FortiGate, outgoing traffic goes through the wrong interface for local-in traffic coming on an SDWAN interface. |
| 1048338 | Unexpected SD-WAN event logs are generated on HA passive devices indicating no role match or selected. |
| 1049721 | When BGP enables local-as-replace-as and there is a network loop condition, the NLRI's as-path is increased indefinitely. |
| 1051709 | On FortiOS, the *Routes* widget does not list out IPv6 routes with non-zero VRF's. |
| 1057135 | The gateway/offload value of offloaded one-way UDP sessions is reset when unrelated routing changes are made. |

| Bug ID | Description |
|---|---|
| 1057474 | FortiGate does not generate a PIM register after stopping and starting a multicast stream. |
| 1057504 | PIM-SM fails to update the failback neighbor when a higher-priority DR becomes available in VRRP environments, causing incorrect routing decisions. |
| 1058616 | The SD-WAN Rules GUI page does not load on HA secondary FortiGates due to restricted access to the virtual-wan/health-check monitor API. |
| 1060456 | When hovering over a vlan interface on the *SD-WAN Rules* tab on the *Network* > *SD-WAN* page, the interface shows as disabled in the SD-WAN rule even though it is active. |
| 1061899 | Packet are duplicated if the latency between SD-WAN channels differs by more than 250ms. |
| 1065805 | A malformed payload error occurs when an ADVPN-2.0 shortcut-reply message has a msg id of 0 and is fragmented, bypassing proper reassembly in FortiOS. |
| 1069060 | Routes are not displayed correctly when the BGP configuration is in a specific order. |
| 1071662 | Shortcut creation fails when using ADVPN 2.0 with BGP on Loopback interfaces for segregated transports due to depublication errors caused by incorrect VRF handling in specific FortiOS versions. |
| 1078608 | The SD-WAN `probe-timeout` value is reset to 60000 after rebooting. |
| 1085271 | An IGMP membership report with a `0.0.0.0` source does not work as expected in kernel 4.19.13. |
| 1085897 | VPNv4 routes are lost on restarting side when PE VRF exits graceful-restart prematurely before CE VRFs finish. |
| 1086828 | SD-WAN logs show the parent interface instead of the shortcut interface. |
| 1091628 | Interface IP addresses are incorrectly added and removed from the kernel before their interfaces are properly generated, causing secondary IPs to be deleted from other VDOMs during new VDOM creation. |

# Security Fabric

| Bug ID | Description |
|---|---|
| 873222 | The automation email does not show the output of some commands. |
| 948322 | After deauthorizing a downstream FortiGate from the *System* > *Firmware & Registration* page, the page may appear to be stuck to loading.<br>**Workaround**: perform a full page refresh to allow the page to load again. |
| 987531 | Threat Feed connectors in different VDOMs cannot use the source IP when using internal interfaces. |
| 1007607 | When creating a new IPv6 address, SDN connectors cannot be added for dynamic addresses. |

| Bug ID | Description |
|---|---|
| 1019284 | When optimizing a security rating, resolving an alert for one rating causes another alert to appear for another rating and the alerts cycle between both ratings continuously. |
| 1040700 | The external connector only allows users to specify the interface in the root vdom and not the vdom it is configured in. |
| 1042972 | On the *Security Fabric* > *Automation* page, users cannot test an automation stitch that uses the *Schedule* trigger from the GUI. |
| 1054407 | The Security Rating report does not show test results for downstream FortiGates when the *All FortiGates* view is selected. |
| 1055616 | External resources are not loaded immediately on devices without a disk after a reboot due to delayed forticron checks, causing a 30-minute delay before WAD reloads them. |
| 1056262 | With a FortiGate configured with a `root-vdom` and a `mgmt-vdom`, when an automation stitch is configured for a compromised host with IP-Ban action, the IP is banned from the `mgmt-vdom`. |
| 1057862 | On the *Security Fabric* > *Automation* page, webhook requests use the same `Content-Type: application/json` in HTTP headers for all requests, even if it has a custom header. |
| 1058589 | On the *Security Fabric* > *Automation* page, webhook requests use the same `Content-Type: application/json` in HTTP headers for all requests, even if it has a custom header. |
| 1068310 | The system rejects IP addresses in the reserved range when attempting DHCP allocation, causing configuration errors. |
| 1075080 | On the *Security Fabric* > *Automation* page, the *Duplicate Firewall Objects* security rating does not work as expected, even it should be passed. |
| 1082980 | The AZURE type dynamic firewall address takes longer than normal to resolve itself, even with the correct filter value in the robot test bed. |
| 1088000 | The `fsvrd` listens on port 8013 and provides a certificate with `set allowaccess fabric`. |

# SSL VPN

| Bug ID | Description |
|---|---|
| 943971 | On the *VPN* > *SSL-VPN Settings* page, when renaming a selected *Restrict Access Host* object, the object is deselected. |
| 998219 | Internet services cannot be used (IPv4 and IPv6) as destination in SSL VPN policies with dual stack enabled. |
| 1026775 | Remove SSL VPN from FGT 9xG. |
| 1042457 | Duplicate log entries are created for SSL VPN when the tunnel is up or down. |
| 1046374 | An unauthenticated user mismatch occurs with the user. |

| Bug ID | Description |
|---|---|
| 1047705 | SAML login from a Windows FortiClient is blocked when `sslvpn-webmode` is disabled in the `config system global` command. |
| 1061165 | SSL VPN encounters a signal 11 interruption and does not work as expected due to a word-length heap memory issue. |
| 1063777 | Login fails for local remote TAC+ users with FortiToken when waiting for token response. |
| 1066564 | SMB bookmarks become inaccessible through SSL-VPN web portal mode due to incorrect DNS server path definitions. |
| 1078149 | Blocked internal resource access occurs when FCT reestablishes a TLS tunnel using the same DHCP IP after a brief link downtime, due to improper handling of the previous tunnel's AP session and tun dev index. |
| 1079185 | Incorrect maximum values present in CLI schema files. |
| 1082427 | The SSL VPN OS checklist in FortiOS does not include minor versions of macOS 13 and 14, nor macOS Sequoia 15.0. |
| 1082696 | When FCT reestablishes a TLS tunnel quickly after a network disruption, SSL VPN attempts an IP association with the same IP, causing a duplication and no value assigned to the tun dev index. |
| 1094825 | Unexpected behavior caused by SSL VPN when multiple routes are configured with the same address. |

# Switch Controller

| Bug ID | Description |
|---|---|
| 1034470 | FortiGate GUI shows multiple entries for the same FortiSwitch when exporting it to be used by several VDOMs. |
| 1035823 | When trying to start and stop the FortiSwitch LED blink using the Security Fabric, the GUI shows a *Failed to send command* error. |
| 1038646 | On the *System* > *Firmware & Registration* page, the FortiSwitch registration status changes from *Not registered* to *Failed to fetch status* when it is deauthorized and then authorized. |
| 1042390 | On the *WiFi & Switch Controller* > *SSID* page, NAC policies using a Wildcard MAC Address cannot be saved using the GUI.<br>**Workaround**: use the CLI to perform the operation. |
| 1044150 | Firmware installation fails when upgrading FortiSwitch devices through FGT GUI. |
| 1052908 | When the name of the FortiSwitch does not match its serial number, it shows up as *not registered* on the *System* > *Firmware & Registration* and *Security Fabric* > *Fabric Connectors* pages. |
| 1054445 | When editing a dynamic port policy, saved changes are not shown in the GUI. |

| Bug ID | Description |
|---|---|
| 1055052 | The NAC policy is not visible in the GUI due to switch-fortilink not set in the NAC policy. |
| 1064814 | Random CPU spikes and for cu_acd process. |
| 1069164 | The managed switch incorrectly reverts to the default time zone after reboot due to improper handling of zero-minute GMT values in the configuration. |
| 1071594 | Users cannot de-select all values from Allowed VLANs and related policies due to a GUI malfunction. |
| 1073340 | On the *Firmware* page, the *Registration Status* shows a *Failed to fetch status* error for an online FortiSwitch. The CLI shows that its registered. |
| 1074981 | The FortiSwitch port configuration GUI under FortiOS 7.6.0 no longer allows users to de-select all values for Allowed VLANs, Security Policy, or QOS Policy. |
| 1077496 | High CPU utilization occurs when flpold/flcfgd processes mishandle socket messages during WAD operations due to incomplete or corrupted data. |
| 1092043 | The dynamic VLAN is not visible in the GUI. |

# System

| Bug ID | Description |
|---|---|
| 776290 | VLAN sub interface event logs for interface status changes are inaccurate. |
| 894966 | ACME certificates cannot be renewed manually before their expiration date. |
| 901621 | On the NP7 platform, setting the interface configuration using set inbandwidth <x> or set outbandwidth <x> commands stops traffic flow.<br>**Workaround**: Change the NP7 `default-qos-type` setting from `shaping` to `policing`. This requires a restart of the device for the configuration to take effect:<br>`config system npu`<br>`  set default-qos-type policing`<br>`end` |
| 907752 | On FortiGate 1000D models, the SFP 1G port randomly experiences flapping during operation. |
| 920320 | FortiGate encounters increasing `Rx_CRC_Errors` on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices. |
| 952104 | FortiGate experiences packet loss when using an internal hardware switch. |
| 960707 | Egress shaping does not work on NP when applied on the WAN interface. |
| 976314 | After upgrading FortiGate and not changing any configuration details, the output of `s_duplex in get hardware nic port` command displays `Half` instead of `Full`. This is purely a display issue and does not affect system operation. |

| Bug ID | Description |
|---|---|
| 978290 | FortiGate cannot communicate with ACME client and cannot generate certificate. |
| 983467 | FortiGate 60F and 61F models may experience a memory usage issue during a FortiGuard update due to the ips-helper process. This can cause the FortiGate to go into conserve mode if there is not enough free memory. |
| 999816 | FortiGate 100 models may become unresponsive and prevent access to the GUI, requiring a reboot to regain access due to an issue with the SOC3. |
| 1006685 | FortiGate enters a loop cycle and generates a large number of LCAP packets when FortiGate does not receive LCAP packets from a peer device. |
| 1008022 | After a restarting FortiGate from the GUI, the `auto-nego` SFP port settings are not reflected in FortiGate. |
| 1011696 | When a SIM card is ejected from a FortiGate using dual SIM cards, the log message does not indicate the slot number FortiOS is switching to. |
| 1018843 | When FortiGate experiences a memory usage issue and enters into conserve mode, the system file integrity check may not work as expected and cause the device to shutdown. |
| 1020602 | After configuring a virtual wire pair (VWP) setting, it is not present in FortiGate after a reboot. |
| 1020921 | When configuring an SNMP trusted host that matches the management *Admin* trusted host subnet, the GUI may give an incorrect warning that the current SNMP trusted host does not match. This is purely a GUI display issue and does not impact the actual SNMP traffic. |
| 1022935 | FortiGate experiences a CPU usage issue when `dedicated-management-cpu` is enabled. |
| 1025114 | Insufficient free memory on entry-level Fortigate devices with 2 GB RAM may cause unexpected behavior in the IPS engine. |
| 1029353 | The SNMP trap is not sent out when a virus is detected on the antivirus scanner. |
| 1029447 | FortiGate encounters increasing `Rx_CRC_Errors` on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices. |
| 1032018 | The SFP+ port LED does not illuminate and displays a speed 10Mbps even though the link status up and speed is set to 1000Mbps. |
| 1032602 | FortiGate encounters a memory usage issue on DNS proxy, resulting in FortiGate going into conserve mode. |
| 1034286 | FortiGate does not auto negotiate to `Full duplex` when connecting to FortiSwitch due to a duplication error. |
| 1034821 | On FortiGate, NP7 offloaded traffic does not use the updated MAC address from the ARP table to forward traffic using a GRE tunnel. |
| 1039264 | The DNS proxy does not forward the response after upgrading FortiGate. |
| 1039564 | When the configuration changes using the SSH, a *backup failed* alert is generated. |
| 1044178 | No ICMP error messages are sent when oversized packets are received by IPv6 tunnels with fragmentation disabled. |

| Bug ID | Description |
|---|---|
| 1045301 | Config revision files are incomplete during restores after firmware updates due to background save timeouts. |
| 1047996 | FortiGate 4800F model split ports do not work as expected causing issues with LACP and MRU on split ports. |
| 1048496 | On FortiGate, the `snmp` daemon does not work as expected resulting in the SNMP queries timing out. |
| 1049119 | FortiGate encounters an interruption in the kernel due to a NULL pointer issue. |
| 1050883 | Backing up a configuration using SFTP with the domain username does not work when characters @ and \ are in the username. |
| 1050908 | In some scenarios, when FortiGate as a DHCP client sends out `DHCP-REQUEST` packets, the SRC IP address is set in the IP header. |
| 1051961 | On FortiGate, IP addresses cannot be assigned within a configured IP range due to a DHCP server issue. |
| 1053536 | On FortiGate, the console displays error messages when adding Pre and Post-login banners due to a rare error condition. |
| 1054294 | FortiGate reboots after a connected HA heartbeat cable is connected, or running the `diag hardware deviceinfo nic ha` command. |
| 1055029 | FortiGate cannot get updates from the public FortiGuard servers in FIPS-CC mode. |
| 1055392 | The traffic shaper does not take effect on the firewall policy when traffic is offloaded to NP7 due to a traffic management issue. |
| 1055805 | Duplicate SNMP traps are sent to `ha-direct` enabled trap servers when two `ha-mgmt-intf` are configured. |
| 1056166 | Error messages appear during bootup when FortiOS devices that support CGNAT lack a valid hyperscale license. |
| 1056174 | FortiOS processes packets on a non-active port of a redundant link. |
| 1056578 | The DNS server does not operate as expected with `forward-only` mode enabled. |
| 1056580 | Lack of speed options occurs when configuring network interfaces on FGT91G/121G devices, limiting available settings. |
| 1057098 | The "dsl" test appears in hardware tests for non-DSL models where it should not be enabled. |
| 1057131 | A FortiGuard update can cause the system to not operate as expected if the FortiGate is already in conserve mode. Users may need to reboot the FortiGate. |
| 1057625 | FortiGate does not work as expected due to an interruption in the kernel. |
| 1058397 | On FortiGate 900 models, when the baudrate is configured, the changes are not applied and is set to 9600. |
| 1059398 | The `ptp` server does not work on the vlan interface. |

| Bug ID | Description |
|---|---|
| 1060729 | IPsec tunnels become unreachable on FortiGates with np7lite hardware when "vpn-id-ipip" is configured due to missing support for VPN ID IP/IP offloading in NPU processing. |
| 1061155 | Error messages are printed when assigning a transparent vdom to a vdom link interface. |
| 1061334 | FortiGate returns a string with a *%* sign for the OID *1.3.6.1.4.1.12356.101.4.8.2.1.8* (*fgLinkMonitorPacketLoss*). |
| 1061413 | `EXPIRE` dates are not displayed properly when executing the `get sys fortiguard-service status` command due to a formatting issue. |
| 1061796 | Inaccurate traffic counters display for EMAC-VLAN interfaces when VLAN ID is set to 0 and traffic is offloaded to the NPU. |
| 1062698 | DNSproxy CPU is running high. |
| 1064241 | FortiGate 100E series models sometimes get unresponsive. |
| 1065047 | An error is observed in the dnsproxy caused by the use of secondary dns-database zones. |
| 1065553 | An incorrect /8 connected route is advertised by FortiGate 80F-DSL when configured with a LANTIQ-based DSL modem. |
| 1065969 | FortiGate does not boot up after restoring a configuration file containing an invalid string format. |
| 1066296 | snmpwalk receives "No Session Data" response of fgFwPolLastUsed OID while the background traffic keeps running. |
| 1066622 | The source IP is not replaced as per the `set fmg-source-ip` after adding the device directly. |
| 1066655 | FortiGate 60F and 40F models become stuck after entering conserve mode and hbdev and console access is lost. |
| 1068150 | The DHCP relay uses the wrong interface to send DHCP offer packets to the client. |
| 1069554 | Upgrading directly from 7.2.4 or earlier versions to 7.2.9, or directly from 7.0.11 or earlier to 7.2.9 is not supported. Users must upgrade following the recommended upgrade path to avoid system hanging. |
| 1071749 | Write permission violation log observed in FortiGate in a rare case caused by the host check plugin used in FortiClient/browser side. |
| 1072320 | Link/Activity LEDs of MGMT and HA ports remain lit after executing 'exec shutdown' in FortiOS v7.4.2 and later. |
| 1072437 | FortiWiFi 61F models experience a memory usage issue caused by the WAD daemon. |
| 1072787 | IPv6 connections fail when iPhones access test sites via IPoE due to improper handling of NA messages using link-local addresses. |
| 1075032 | NP7 offloaded traffic continues to use old gateway's MAC address when receiving packets with TTL=1 after a gateway change. |
| 1075116 | Admin user gets logged out when entering an 'unset sdns-server-ip' command in FortiOS CLI during configuration through a tool with specific command timing and sequence. |

| Bug ID | Description |
|---|---|
| 1075585 | Shared copper WAN1 and WAN2 ports remain down when the interface speed is set to `100full`. |
| 1079021 | A CPU usage issue in the Softirq space on 40/160 CPU cores causes packets to drop. |
| 1082838 | System unresponsive triggered by CPU profiling across all cores. |
| 1084819 | LACP/shared ports wan1 and wan2 are down after an upgrade or reboot due to hardware shared-port medium changes. |
| 1085736 | FortiGate cannot restore the configuration file in the following sequence.<br>1. `private-data-encryption` enabled with random key, and configuration is backed up.<br>2. `private-data-encryption` disabled.<br>3. `private-data-encryption` enabled again, with new random key.<br>4. Restore configuration file in step 1. |
| 1085990 | CRC errors occur on NP6 platform SFP port when connected to Cisco ISR 4431 with fiber transceiver. |
| 1087109 | After a reboot, FortiGate shows the wrong date if the date was set manually prior to the reboot. |
| 1089397 | Frequent kernel panics occur due to dynamic update of EMS IP/MAC addresses in multiple vdom, causing the device to freeze and require a reboot. |
| 1091551 | Hardware limitation on the NP7 platform causes the following QTM related issues:<br>• Incorrect checksum for fragments after QTM. The workaround is to not parse Layer4 after QTM.<br>• Packets longer than 6000 bytes cause QTM unresponsiveness.<br>• Refresh issue causes QTM unresponsiveness. The workaround is to use one refresh list.<br>• MTU is not honored after QTM, so packets are not fragmented. |
| 1092021 | FortiGate logs out when deleting the secondary IP configured on an interface in work space mode. |
| 1093042 | High memory consumption occurs when multiple SNMP child processes are created due to frequent queries, as they fail to terminate properly and accumulate in memory. |

# Upgrade

| Bug ID | Description |
|---|---|
| 1056126 | FortiGate does not boot up properly after an upgrade when it has a large number (500+) of VDOMs configured. |

# User & Authentication

| Bug ID | Description |
|---|---|
| 940989 | Page fails to reload after successful FTM push authentication for remote LDAP users in firewall policies. |
| 1003373 | FortiGate experiences a gradual memory usage issue in the fnbamd process. |
| 1004258 | The Strict-SNI SSL Profile might block TCP connections if the SNI cannot be verified due to an active probe failure. |
| 1008709 | EST HTTP passwords are not encrypted in the config file during certificate enrollment with EST. |
| 1009884 | FortiGate encounters a CPU usage issue in the `authd` process after a firmware upgrade. |
| 1036265 | The `reply-to` option under `config system alertmail` is removed even for `custom mail-servers` with 2-factor authentication after an upgrade. |
| 1039663 | The TACACS+ connection times out, irrespective of the `remoteauthtimeout` setting, due to an issue with the `ldapconntimeout` setting, after upgrading to version 7.4.4. |
| 1039771 | FortiOS may reply to an FTM push message using a different egress interface instead of the original interface. |
| 1042326 | Admin access to GUI remains valid despite exceeding the two-factor-email-expiry timeout. |
| 1042987 | NTLM authentication does not work as expected after an upgrade. |
| 1043222 | CMPv2 IR does not work as expected due to server certification validation error conditions. |
| 1044084 | On the *Dashboard* > *Firewall User Monitor* page, the *Search* field does not display in the GUI when there are a large number (+1000) FSSO user logos. |
| 1045753 | An ACME certificate enrollment error is generated without detailed error message information. |
| 1050942 | The Active Firewall-Authentication for 2FA FAC RADIUS users using PAP method does not work as expected after upgrading to version 7.4.4. |
| 1060009 | On FortiGate, RADSEC sent incorrect accounting packets due to a hashing issue. |
| 1066264 | RADIUS message authenticator checking is not optional under TLS. |
| 1070560 | Admin authentication bypass when configuring TACACS server. |
| 1070743 | FortiToken activation-code emails fail to send when using the shortcut method due to missing recipient email addresses in the logs after an upgrade. |
| 1072870 | FortiGate initiates LDAPS sessions that do not respect the `ssl-min-proto-version` option set under the `config system global` command. |
| 1080234 | For FortiGate (versions 7.2.10 and 7.4.5 and later) and FortiNAC (versions 9.2.8 and 9.4.6 and prior) integration, when testing connectivity/user credentials against FortiNAC that acts as a RADIUS server, the FortiGate GUI and CLI returns an *invalid secret for the server* error. |

| Bug ID | Description |
|---|---|
| | This error is expected when the FortiGate acts as the direct RADIUS client to the FortiNAC RADIUS server due to a change in how FortiGate handles RADIUS protocol in these versions. However, the end-to-end integration for the clients behind the FortiGate and FortiNAC is not impacted. |
| 1080510 | SCEP certificate auto-renewal fails to trigger when forticron experiences excessive pending DNS requests due to server unavailability. |
| 1086643 | FortiGate Captive Portal does not send the full *Server Certificate Chain*. |
| 1112718 | When RADIUS server has the require-message-authenticator setting disabled, The GUI RADIUS server dialogs *Test connectivity* and *Test user credentials* still check for the message-authenticator value and incorrectly fail the test with *missing authenticator* error message.<br>`config user radius`<br>`edit <radius server>`<br>`set require-message-authenticator disable`<br>`next`<br>`end`<br>This is only a GUI display issue and the end-to-end integration with RADIUS server should still work. |

# VM

| Bug ID | Description |
|---|---|
| 953526 | The FortiGate-VM OCI may not detect an extra port attached. |
| 972520 | The FortiGate-AWS HA secondary `awsd debug` result prints raw HTML content. |
| 1012927 | When FortiGate returns an *ICMP TTL-EXCEEDED* message, the `geneve` option field header is missing. |
| 1046696 | A FortiGate VM HA in Azure Cloud may intermittently go out of synchronization due to an issue in the daemon process. |
| 1054244 | FortiToken does not work as expected after moving a FortiGate-VM license to a new VM with the same serial number. |
| 1058355 | FortiGate VM Azure does not work as expected and enters into conserve mode in vWAN setup. |
| 1061669 | FGT_KVM console cannot be accessed using serial tools under a trial license when configured with multiple virtio interfaces and queues. |
| 1066138 | FortiGate VM performance drops when traffic passes through an inter-vdom link. |
| 1067046 | Dynamic firewall address list entries are deleted when AWS STS tokens expire prematurely. |
| 1070910 | FortiFlex license fails to install consistently during Day0 configuration when using Port2 for Internet access, as injection occurs before connectivity is established. |

| Bug ID | Description |
|---|---|
| 1072695 | The VLAN interface is not reachable on a FortiGate VM running KVM with Intel 10G NIC (10Gb ethernet card). |
| 1073016 | The OCI SDN connector cannot call the API to the Oracle service when an IAM role is enabled. |
| 1074600 | Inadvertent traffic disruption observed on FortiGate-VM64 caused by a deadlock in the `newcli` process. |
| 1082197 | VLAN traffic fails to pass through E810-XXV NIC with SFP28 transceiver and 25G speed after enabling DPDK. |
| 1083073 | Security rules with port range can be pushed to the Azure VWAN SLB successfully, but the SLB doesn't allow the specified port range. |
| 1093458 | The FGVM console becomes unresponsive after a hard reboot in OpenStack environments running on Redhat Enterprise Linux 9.2 when using USB keyboards. |
| 1094274 | FortiOS becomes unresponsive when sending IPv6 traffic over MLX5 network adapters due to incorrect WQE handling. |

# VoIP

| Bug ID | Description |
|---|---|
| 1070320 | The SIP ALG does not create the expected session for SIP OPTIONS traffic. |

# Web Application Firewall

| Bug ID | Description |
|---|---|
| 1067320 | The Web Application Firewall marks http/s traffic as a malformed constraint. |
| 1071022 | A matched pattern in the HTTP body cannot be blocked with a `waf` profile for some content types. |

# Web Filter

| Bug ID | Description |
|---|---|
| 537134 | When a webfilter time-based quota is configured, once quota is reached, long sessions are not terminated. |

| Bug ID | Description |
|---|---|
| 1026023 | The webfilter and traffic logs show the incorrect realserver IP address due to a WAD process issue. |
| 1045884 | When enabling the *log all search keywords* in the web filter profile and VDOM mode is disabled, the *Key Word* column is not populated with data. |
| 1093624 | URLs fail to match intended regex patterns when special characters are escaped with backslashes. |

# WiFi Controller

| Bug ID | Description |
|---|---|
| 1013290 | WIDS data is not removed from the CLI. |
| 1028181 | Wi-Fi devices would encounter service delay when roaming over captive-portal SSID with MAC-address authentication. |
| 1033483 | Secondary AC wpad_ac memory usage increases during stress tests with simulators in HA setups. |
| 1048928 | Cannot retrieve DHCP IP's from the assigned VLAN when connecting Bridge SSID with RADIUS-based MAC authentication. |
| 1049471 | On FortiGate 90G and 120G models, traffic is dropped due to the MAC address of the VAP interface being updated with the old MAC address when HA is enabled. |
| 1050915 | On the *WiFi & Switch Controller* > *Managed FortiAPs* page, when upgrading more than 30 managed FortiAPs at the same time using the *Managed FortiAP* page, the GUI may become slow and unresponsive when selecting the firmware. |
| 1059964 | RADIUS authentication in a WPA2-Enterprise SSID does not use `ha-mgmt-interface` when `ha-direct` is enabled. |
| 1062560 | Duplicate IP detection logs are generated on both FortiGates during HA active- passive setups when they share the same IP and MAC address. |
| 1062730 | On FortiGate, the `set max-clients` feature does not work as expected and allows more clients to connect than the maximum value configured. |
| 1071329 | Change the region/SKU assignment of the following nine countries: BB, BZ, CO, DO, GD, GY, HN, FM, and PA to A (from K model) or N (G & Older model). |
| 1073390 | Duplicated WiFi event logs occur when acd-process-count is set for multi-core processing in FortiGate. |
| 1073588 | Users cannot make any changes to `wtp-profile` due to an issue with the REST API connection to the cmdbsvr. |
| 1075138 | An unknown source IP appears in client-authentication logs when laptops connect to wireless networks at specific sites. |

| Bug ID | Description |
|---|---|
| 1076738 | Group name fails to display in station list after local authentication with 2FA for Enterprise+User-group SSID connections. |
| 1089563 | The VLAN ID is lost during roaming with WPA-PSK and Fast BSS Transition enabled, causing connectivity issues as the client loses its network segmentation. |

# ZTNA

| Bug ID | Description |
|---|---|
| 1035072 | FortiClient access to TCP-FWD with saml authentication does not redirect the loop if `set ztna vip` and `saml SP` use the same IP address. |
| 1053309 | An interruption occurs in the WAD when accessing ZTNA TCP-forwarding service through a proxy-policy with a SAML user group and `h2-support` is disabled on the `firewall vip`. |
| 1056179 | PPPoE encounters a performance issue after an upgrade. |
| 1075532 | Long sessions without any authentications terminate after 5 hours. |

# Common Vulnerabilities and Exposures

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

| Bug ID | CVE references |
|---|---|
| 1031370 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2023-51385 |
| 1051974 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2025-25250 |
| 1052413 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-54021 |
| 1052903 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-46666 |
| 1054998 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-3596 |
| 1060886 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-48884 |
| 1062139 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference: |

| Bug ID | CVE references |
|---|---|
| | • CVE-2024-40591 |
| 1063464 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-46669 |
| 1066080 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2025-22251 |
| 1072334 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-46670 |
| 1074487 | FortiOS 7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-46665 |
| 1077059 | FortiOS7.6.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-52963 |

# Known issues

Known issues are organized into the following categories:

- New known issues on page 78
- Existing known issues on page 79

To inquire about a particular bug or report a bug, please contact Customer Service & Support.

# New known issues

The following issues have been identified in version 7.6.1.

## FortiGate 6000 and 7000 platforms

| Bug ID | Description |
|---|---|
| 1149405 | The image upgrade fails when performing a non-graceful update due to an ISIZE mismatch during verification. |

## Hyperscale

| Bug ID | Description |
|---|---|
| 1013892 | Unexpected behavior observed in NPD when the threat feed object attempted to update manually in the HA pair. |
| 1089281 | For FG-480xF/FFW-480xF, using `npu-group` other than `0` with log2host around ~1M CPS could result in NP chip getting stuck. |

## Intrusion Prevention

| Bug ID | Description |
|---|---|
| 1076213 | FortiGate's with 4GB memory might enter conserve mode during the FortiGuard update when IPS or APP control is enabled.<br>**Workaround**: Disable the `proxy-inline-ips` option under `config ips settings`. |

## IPsec VPN

| Bug ID | Description |
|---|---|
| 1103754 | Failed HTTP sessions occur when passing through nTurbo due to improper handling of fragmented packets. |

## Switch Controller

| Bug ID | Description |
|---|---|
| 1113304 | FortiSwitch units are offline after FortiGate is upgraded from 7.4.6 or 7.6.0 to 7.6.1 or later when LLDP configuration is set to vdom/disable under the FortiLink interface.<br>**Workaround**: In LLDP configuration, enable `lldp-reception` and `lldp-transmission` under the FortiLink interface, or rebuild the FortiLink interface. |

## System

| Bug ID | Description |
|---|---|
| 1103146 | Duplicated RADIUS packets are captured by the sniffer when performing firewall authentication with a RADIUS server. |
| 1103617 | Integrating an interface does not work when adding a new member into an existing interface or creating a new interface. |
| 1112376 | Unexpected behavior observed in the newcli daemon due to inconsistencies in node registration between cmdbsvr and other daemons. |

## Upgrade

| Bug ID | Description |
|---|---|
| 1106072 | The image file transfer between FortiManager and FortiGate may not work as expected when transferred by the FGFM tunnel. |

# Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.1.

# Endpoint Control

| Bug ID | Description |
|---|---|
| 1019658 | On FortiGate, not all registered endpoint EMS tags are displayed in the GUI. |
| 1038004 | FortiGate may not display the correct user information for some FortiClient instances. |

# Firewall

| Bug ID | Description |
|---|---|
| 959065 | On the *Policy & Objects* > *Traffic Shaping* page, when deleting or creating a shaper, the counters for the other shapers are cleared. |
| 990528 | When searching for an IP address on the *Firewall Policy* page, the search/filter functionality does not return the expected results. |
| 994986 | The *By Sequence* view in the Firewall policy list may incorrectly show a duplicate implicit deny policy in the middle of the list. This is purely a GUI display issue and does not impact policy operation.<br>The *Interface Pair View* and *Sequence Grouping View* do not have this issue. |
| 1117165 | Leaving the `apn` field empty in a GTP APN traffic shaping policy means that the policy will not match any traffic. Consequently, APN traffic shaping can only be applied to specific APNs.<br>To configure GTP APN traffic shaping:<br>`config gtp apn-shaper`<br>`edit <policy-id>`<br>`set apn [<apn-name> <apngrp-name> ...]`<br>`set rate-limit <limit>`<br>`set action {drop \| reject}`<br>`set back-off-time <time>`<br>`next`<br>`end` |

# FortiGate 6000 and 7000 platforms

| Bug ID | Description |
|---|---|
| 653335 | SSL VPN user status does not display on the FortiManager GUI. |
| 790464 | After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond. |
| 936320 | When there is a heavy traffic load, there are no results displayed on any *FortiView* pages in the GUI. |
| 950983 | *Feature Visibility* options are visible in the GUI on a `mgmt-vdom`. |

| Bug ID | Description |
|---|---|
| 994241 | On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7. |
| 998615 | When doing a GUI-packet capture on FortiGate, the through-traffic packets are not captured. |
| 1006759 | After an HA failover, there is no IPsec route in the kernel.<br>**Workaround**: Bring down and bring up the tunnel. |
| 1014826 | SLBC does not function as expected with IPsec over TCP enabled. |

# FortiView

| Bug ID | Description |
|---|---|
| 1034148 | The *Application Bandwidth* widget on the *Dashboard* > *Status* page does not display some external applications bandwidth data. |

# GUI

| Bug ID | Description |
|---|---|
| 853352 | When viewing entries in slide-out window of the *Policy & Objects* > *Internet Service Database* page, users cannot scroll down to the end if there are over 100000 entries. |
| 1047146 | After a firmware upgrade, a VLAN interface used in IPsec, SSL VPN, or SD-WAN is not displayed on the interface list or the SD-WAN page and cannot be configured in the GUI. |
| 1047963 | High Node.js memory usage when building FortiManager in Report Runner fails. Occurs when FortiManager has a slow connection, is unreachable from the FortiGate (because FMG is behind NAT), or the IP is incorrect. |

# HA

| Bug ID | Description |
|---|---|
| 851743 | When running the `diag sys ha checksum cluster` command, a previous line result is added further down in the output instead of new line result when a FortiGate is configured with several VDOMs . |
| 1137565 | vSN support added in 7.2.9, 7.4.6, and 7.6.1. FG-100F/101F do not yet support vSN and logical-sn.<br>No workaround until the devices support vSN. |

# Hyperscale

| Bug ID | Description |
|---|---|
| 1042011 | On FortiGate, an login error message displays in the event log after completing an automation. |
| 1093287 | Using fixed-allocation IP Pools may cause NP7 NSS/PRP modules to become stuck, potentially disrupting traffic. Other PBA IP pools do not have this issue. |

# Intrusion Prevention

| Bug ID | Description |
|---|---|
| 1117043 | After upgrade, event log shows `logdesc="IPSA driver update failed" msg="Fail to update IPSA driver status!"`.<br>This issue only affects physical FortiGate models with the following IPS engine versions:<br>• IPS Engine version: 7.550 - 7.567<br>• IPS Engine version: 7.1019 - 7.1039<br>To determine the IPS Engine versions, use the command:<br>`get sys fortiguard-service status \| grep 'IPS/FlowAV Engine'`<br>**Workaround**: Power off the FortiGate. Wait 30 seconds, and then power on the FortiGate.<br>**Note**: Reboot using the CLI is not an effective workaround and requires additional steps. After executing `exec shutdown`, unplug the power to the FortiGate. Wait one minute, and the power on the FortiGate. |

# IPsec VPN

| Bug ID | Description |
|---|---|
| 735398 | On FortiGate, the IKE anti-replay does not log duplicate ESP packets when SA is offloaded in the event log. |
| 944600 | CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink. |
| 995912 | After a firmware upgrade, some VPN tunnels experience intermittent signal disruptions causing traffic to be re-routed. |
| 1012615 | IPsec VPN traffic is dropped after upgrading to version 7.4.3. |
| 1042371 | RADIUS authentication with EAP-TLS does not work as expected through IPsec tunnels. |

# Log & Report

| Bug ID | Description |
|---|---|
| 611460 | On FortiOS, the *Log & Report* > *Forward Traffic* page does not completely load the entire log when the log exceeds 200MB. |

# Proxy

| Bug ID | Description |
|---|---|
| 1023054 | After an upgrade on a 2GB FortiGate device, the firewall policy does not switch from *Proxy-based* to *Flow-based* in the *Inspection mode* field. |
| 1035490 | The firewall policy works with proxy-based inspection mode on FortiGate models with 2GB RAM after an upgrade.<br>*Workaround*: After an upgrade, reboot the FortiGate. |

# REST API

| Bug ID | Description |
|---|---|
| 938349 | Unsuccessful API user login attempts do not get reset within the time specified in `admin-lockout-threshold`. |
| 993345 | The router API does not include all ECMP routes for SD-WAN included in the `get router info routing-table` command. |

# Security Fabric

| Bug ID | Description |
|---|---|
| 903922 | Physical and logical topology is slow to load when there are a lot of managed FortiAP devices (over 50). This issue does not impact FortiAP management and operation. |
| 1011833 | FortiGate experiences a CPU usage issue in the `Node.js` daemon when there multiple administrator sessions running simultaneously. |
| 1019844 | In an HA configuration, when the primary FortiGate unit fails over to a downstream unit, the previous primary unit displays as being permanently disconnected. |
| 1040058 | The Security Rating topology and results does not display non-FortiGate devices. |

# Switch Controller

| Bug ID | Description |
|---|---|
| 961142 | An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver. |

# System

| Bug ID | Description |
|---|---|
| 932077 | Connection issue between SOC4 platform and third-party switches because SOC4 doesn't support certain carrier extension signals. |
| 947982 | On NP7 platforms, DSW packets are missing resulting in VOIP experiencing performance issues during peak times. |
| 1041726 | Traffic flow speed is reduced or interrupted when the traffic shaper is enabled. |
| 1046484 | After shutting down FortiGate using the `execute shutdown` command, the system automatically boots up again. |
| 1047085 | The FortiOS GUI is unresponsive due to a CPU usage issue with the `csfd` and `node` processes. |
| 1058256 | On FortiGate, interfaces with DAC cables remain down after upgrading to version 7.4.4. |
| 1069208 | If the DHCP offer contains padding when DHCP relay is used, the DHCP relay deletes the padding before relaying the packet. |

# Upgrade

| Bug ID | Description |
|---|---|
| 1043815 | Upgrading the firmware for a large number (100+) of FortiSwitch or FortiAP devices at the same time may cause performance issues with the GUI and some devices may not upgrade.<br>**Workaround**: pace out the upgrade schedule and upgrade devices in smaller batches. |
| 1104649 | In 7.6.1 and 7.6.2, if a local-in policy, local-in-policy6, DoS policy, interface policy, multicast policy, TTL policy, or central SNAT map is used in an interface in version 7.4.5, 7.6.0, or any previous GA version that was part of the SD-WAN zone, these policies will be deleted or show empty values after upgrading to version 7.6.1 or 7.6.2.<br>**Workaround**: After upgrading to 7.6.1 or 7.6.2, users must manually recreate these policies and assign them to the appropriate SD-WAN zone. |

# User & Authentication

| Bug ID | Description |
|---|---|
| 1021719 | On the *System* > *Certificates* page, the *Create Certificate* pane does not function as expected after creating a new certificate. |
| 1082800 | When performing LDAP user searches from the GUI against LDAP servers with a large number of users (more than 100000), FortiGate may experience a performance issue and not operate as expected due to the HTTPSD process consuming too much memory. User may need to stop the HTTPSD process or perform a reboot to recover.<br>**Workaround**: Perform an LDAP user search using the CLI. |

# VM

| Bug ID | Description |
|---|---|
| 1146370 | AWS bootstrap is unable to parse IAM role profile properly due to the length. |

# Web Filter

| Bug ID | Description |
|---|---|
| 1040147 | Options set in `ftgd-wf` cannot be undone for a web filter configuration. |
| 1058007 | Web filter custom replacement messages in group configurations cannot be edited in FortiGate. |

# WiFi Controller

| Bug ID | Description |
|---|---|
| 1083395 | In an HA environment with FortiAPs managed by primary FortiGate, the secondary FortiGate GUI *Managed FortiAP* page may show the FortiAP status as offline if the FortiAP traffic is not routed through the secondary FortiGate.<br>This is only a GUI issue and does not impact FortiAP operation. |

# Built-in AV Engine

AV Engine 7.00034 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

# Built-in IPS Engine

IPS Engine 7.001026 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