New Features Guide

FortiOS 7.2.0

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

November 07, 2023
FortiOS 7.2.0 New Features Guide
01-720-770718-20231107

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-11-07	Updated Backing up and restoring configuration files in YAML format on page 244.
2023-10-24	Added Command to compute file hashes 7.2.6 on page 269.
2023-10-13	Updated Allow empty address groups on page 382.
2023-10-10	Updated Add built-in entropy source 7.2.6 on page 318.
2023-10-06	Added Add the Any and All options back for ZTNA tags in the GUI 7.2.6 on page 364.
2023-09-28	Initial release of FortiOS 7.2.6.
2023-08-09	Updated Synchronizing LDAP Active Directory users to FortiToken Cloud using the two-factor filter 7.2.1 on page 458.
2023-07-25	Updated Enhance BIOS-level signature and file integrity checking 7.2.5 on page 317. Added Real-time file system integrity checking 7.2.5 on page 318.
2023-07-19	Updated Embedded SD-WAN SLA information in ICMP probes 7.2.1 on page 134.
2023-06-08	Initial release of FortiOS 7.2.5.
2023-04-25	Added Support IPv6 dynamic addresses retrieved from Cisco ACI SDN connector 7.2.1 on page 71.
2023-04-24	Updated Support full extended IPS database for CP9 models and slim extended database for other physical models on page 404.
2023-04-21	Updated Display detailed FortiSandbox analysis and downloadable PDF report on page 24.
2023-04-13	Updated Allow application category as an option for SD-WAN rule destination on page 90.
2023-03-10	Added Support full extended IPS database for CP9 models and slim extended database for other physical models on page 404.
2023-03-08	Added Allow FortiClient EMS connectors to trust EMS server certificate renewals based on the CN field 7.2.4 on page 61.
2023-03-03	Updated Embedded SD-WAN SLA information in ICMP probes 7.2.1 on page 134.
2023-02-24	Updated System automation actions to back up, reboot, or shut down the FortiGate 7.2.1 on page 79.
2023-02-21	Updated WPA3 enhancements to support H2E only and SAE-PK 7.2.1 on page 516. Added Support for GCP ARM CPU-based T2A instance family 7.2.4 on page 633.
2023-02-13	Updated Introduce maturity firmware levels on page 247.
2023-02-02	Updated Add Fabric Overlay Orchestrator for SD-WAN overlay configurations 7.2.4 on page 158.

Date	Change Description
2023-02-01	Updated Publishing ZTNA services through the ZTNA portal 7.2.1 on page 336.
2023-01-31	Initial release of FortiOS 7.2.4.
2023-01-25	Updated Provision FortiExtender firmware upon authorization 7.2.1 on page 571.
2023-01-11	Updated SD-WAN in large scale deployments on page 108.
2022-12-30	Added FortiExtender monitoring enhancement 7.2.1 on page 566 and Provision FortiExtender firmware upon authorization 7.2.1 on page 571.
2022-12-06	Updated Publishing ZTNA services through the ZTNA portal 7.2.1 on page 336.
2022-11-15	Added Add profile support for FortiAP G-series models supporting WiFi 6E Tri-band and Dual 5 GHz modes 7.2.1 on page 509.
2022-11-01	Updated ZTNA inline CASB for SaaS application access control 7.2.1 on page 345.
2022-09-27	Added ICAP scanning with SCP and FTP on page 416.
2022-09-26	Added Update naming of FortiCare support levels 7.2.1 on page 28.
2022-09-20	Added Introduce distributed topology and security rating reports 7.2.1 on page 46.
2022-08-30	Added Support CORS protocol in explicit web proxy when using session-based, cookie-enabled, and captive portal-enabled SAML authentication 7.2.1 on page 239, Allow the YouTube channel override action to take precedence 7.2.1 on page 421, and Synchronizing LDAP Active Directory users to FortiToken Cloud using the two-factor filter 7.2.1 on page 458.
2022-08-19	Added GCP DPDK support on page 608.
2022-08-11	Added New default certificate for HTTPS administrative access 7.2.1 on page 257. Updated Configuring client certificate authentication on the LDAP server on page 446.
2022-08-10	Updated Permanent trial mode for FortiGate-VM 7.2.1 on page 620.
2022-08-09	Added Support backing up configurations with password masking 7.2.1 on page 255.
2022-08-08	Added FortiGate as FortiGate LAN extension 7.2.1 on page 207 and Configure the frequency of IGMP queries 7.2.1 on page 550.
2022-08-04	Initial release of FortiOS 7.2.1.
2022-07-27	Added Add option to disable the FortiGuard IP address rating on page 416.
2022-07-22	Updated BFD for multihop path for BGP on page 172.
2022-06-15	Updated Support Layer 3 roaming for tunnel mode on page 470.
2022-05-30	Updated Abbreviated TLS handshake after HA failover on page 271.
2022-04-21	Added Increase the number of VRFs per VDOM on page 184.
2022-04-18	Added Allow FortiExtender to be managed and used in a non-root VDOM on page 562, Support up to 30 virtual clusters on page 276, and SNMP OIDs for port block allocations IP pool statistics on page 181.

Date	Change Description
2022-04-14	Added Display LTE modem configuration on GUI of FG-40F-3G4G model on page 26, and Show the SSL VPN portal login page in the browser's language on page 435.
2022-04-13	Added Report wireless client app usage for clients connected to bridge mode SSIDs on page 477.
2022-04-12	Added Add OT asset visibility and network topology to Asset Identity Center page on page 636.
2022-04-11	Added Support 802.1X on virtual switch for certain NP6 platforms on page 179
2022-04-08	Added SD-WAN segmentation over a single overlay on page 119.
2022-04-06	Added Add new FortiSwitch Clients page on page 547. Updated Allow a LAG on a FortiLink-enabled software switch on page 536, Allow multiple managed FortiSwitch VLANs to be used in a software switch on page 535, Manage FortiSwitch units on VXLAN interfaces on page 544, Use wildcard serial numbers to pre-authorize FortiSwitch units on page 534, and Enhanced FortiSwitch Ports page and Diagnostics and Tools pane on page 544.
2022-03-31	Initial release.

Overview

This guide provides details of new features introduced in FortiOS 7.2. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable. Features are organized into the following sections:

- GUI
- Security Fabric
- Network
- System
- Policy and Objects
- Security profiles
- VPN
- User and authentication
- Secure access
- Log and report
- Cloud
- Operational Technology

For features introduced in 7.2.1 and later versions, the version number is appended to the end of the topic heading. For example, GUI support for advanced BGP options 7.2.1 on page 188 was introduced in 7.2.1. If a topic heading has no version number at the end, the feature was introduced in 7.2.0.

For a list of features organized by version number, see Index on page 643.

GUI

This section includes new features related to the FortiOS GUI:

- General usability enhancements on page 15

General usability enhancements

This section includes new features related to general usability enhancements:

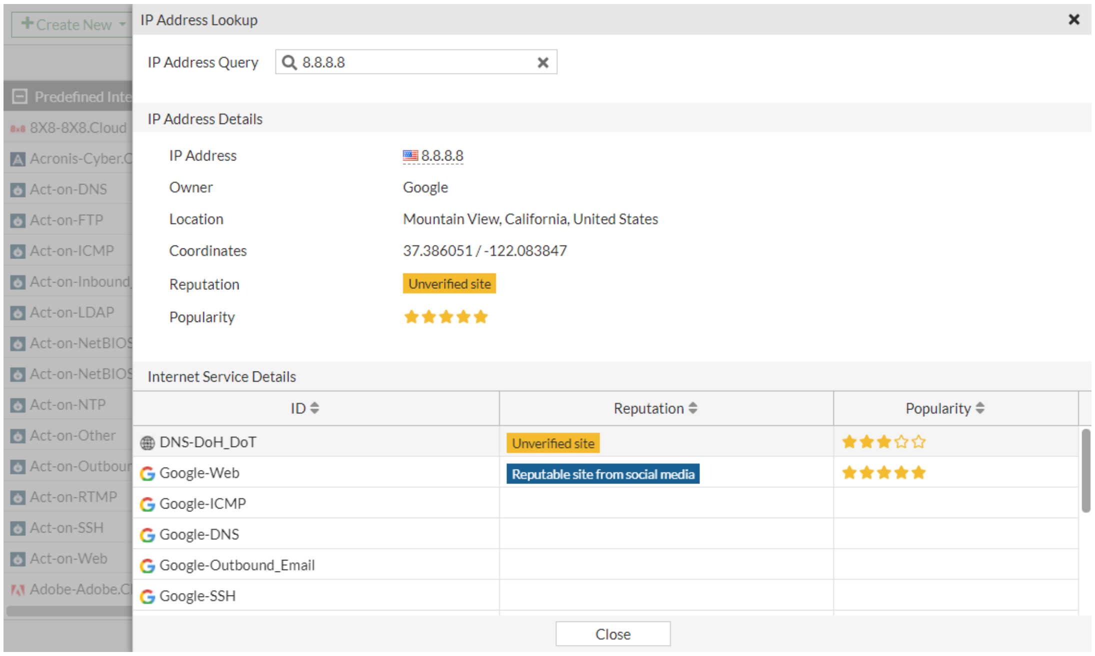
- Look up IP address information from the Internet Service Database page on page 15
- Embed real-time packet capture and analysis tool on Diagnostics page on page 16
- Embed real-time debug flow tool on Diagnostics page on page 20
- Display detailed FortiSandbox analysis and downloadable PDF report on page 24
- Display LTE modem configuration on GUI of FG-40F-3G4G model on page 26
- Update naming of FortiCare support levels 7.2.1 on page 28

Look up IP address information from the Internet Service Database page

The *IP Address Lookup* button has been added to allow users to look up IP address information from the Internet Service Database and GeoIP Database. Returned IP address information includes the reverse IP address/domain lookup, location, reputation, and other internet service information.

To look up IP address information:

1. Go to *Policy & Objects* > *Internet Service Database*.
2. Click *IP Address Lookup*. The *IP Address Lookup* pane opens.
3. In the *IP Address Query* field, enter the IP address and press `Enter`.
   Results of an IP address from the Internet Service Database:



IP Address Lookup

IP Address Query: 8.8.8.8

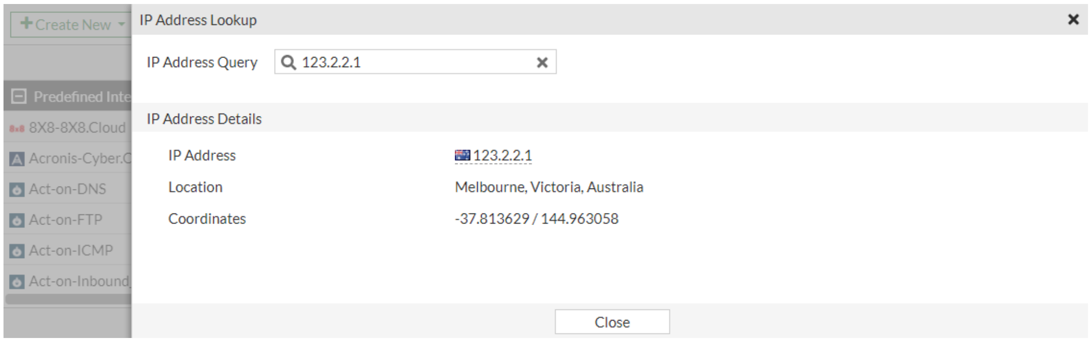
IP Address Details

IP Address	8.8.8.8
Owner	Google
Location	Mountain View, California, United States
Coordinates	37.386051 / -122.083847
Reputation	Unverified site
Popularity	★★★★★

Internet Service Details

ID	Reputation	Popularity
DNS-DoH_DoT	Unverified site	★★★☆☆
Google-Web	Reputable site from social media	★★★★★
Google-ICMP		
Google-DNS		
Google-Outbound_Email		
Google-SSH		

Results of an IP address from the GeoIP Database:



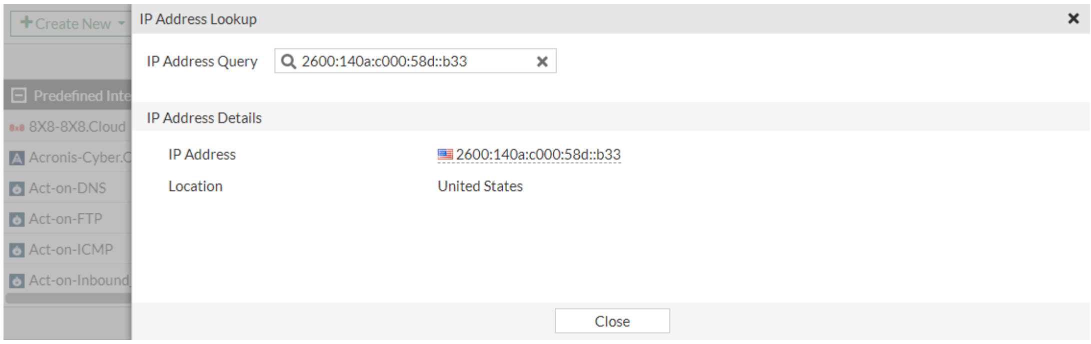
IP Address Lookup

IP Address Query: 123.2.2.1

IP Address Details

IP Address	123.2.2.1
Location	Melbourne, Victoria, Australia
Coordinates	-37.813629 / 144.963058

Results of an IPv6 address from the GeoIP Database:



IP Address Lookup

IP Address Query: 2600:140a:c000:58d::b33

IP Address Details

IP Address	2600:140a:c000:58d::b33
Location	United States

4. Click *Close*.

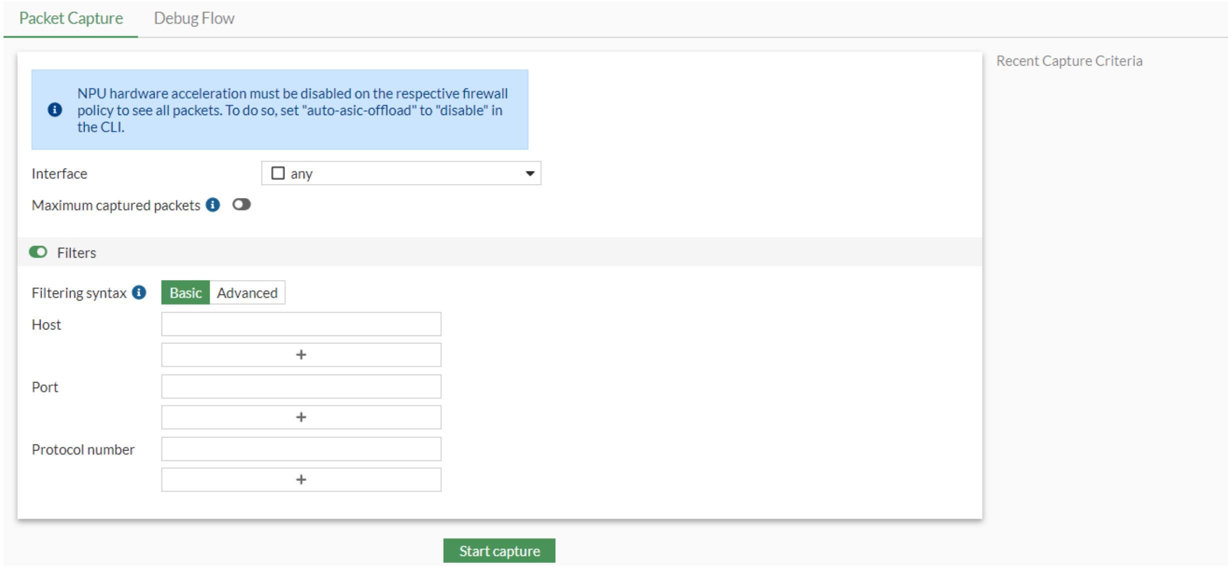
Embed real-time packet capture and analysis tool on Diagnostics page

This enhancement removes the previous *Network* > *Packet Capture* page and replaces it with the *Network* > *Diagnostics* page. The *Packet Capture* page streams the capture in real-time. It allows users to select a packet and view its header and payload information in real-time. Once completed, packets can be filtered by various fields or through the search bar. The capture can be saved as a PCAP file for further analysis.

In the CLI, some options under `config firewall sniffer` have been removed.

To run a packet capture:

1. Go to *Network > Diagnostics* and select the *Packet Capture* tab.
2. Optionally, select an *Interface* (*any* is the default).
3. Optionally, enable *Filters* and select a *Filtering syntax*:
   a. *Basic*: enter criteria for the *Host*, *Port*, and *Protocol number*.



NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

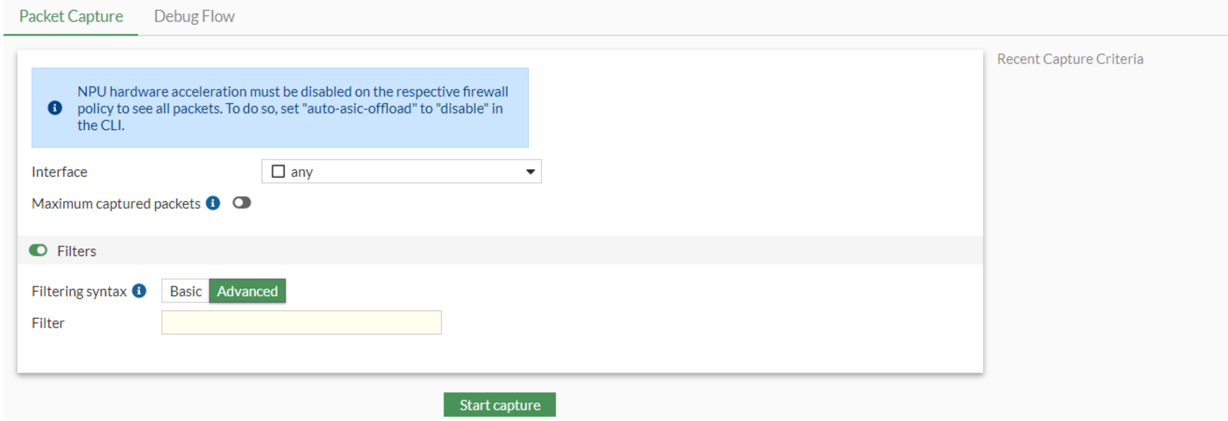
Interface: □ any

Maximum captured packets: ○

Filters: ●

Filtering syntax: Basic

   b. *Advanced*: enter a string, such as *src host 172.16.200.254 and dst host 172.16.200.1 and dst port 443*.



NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

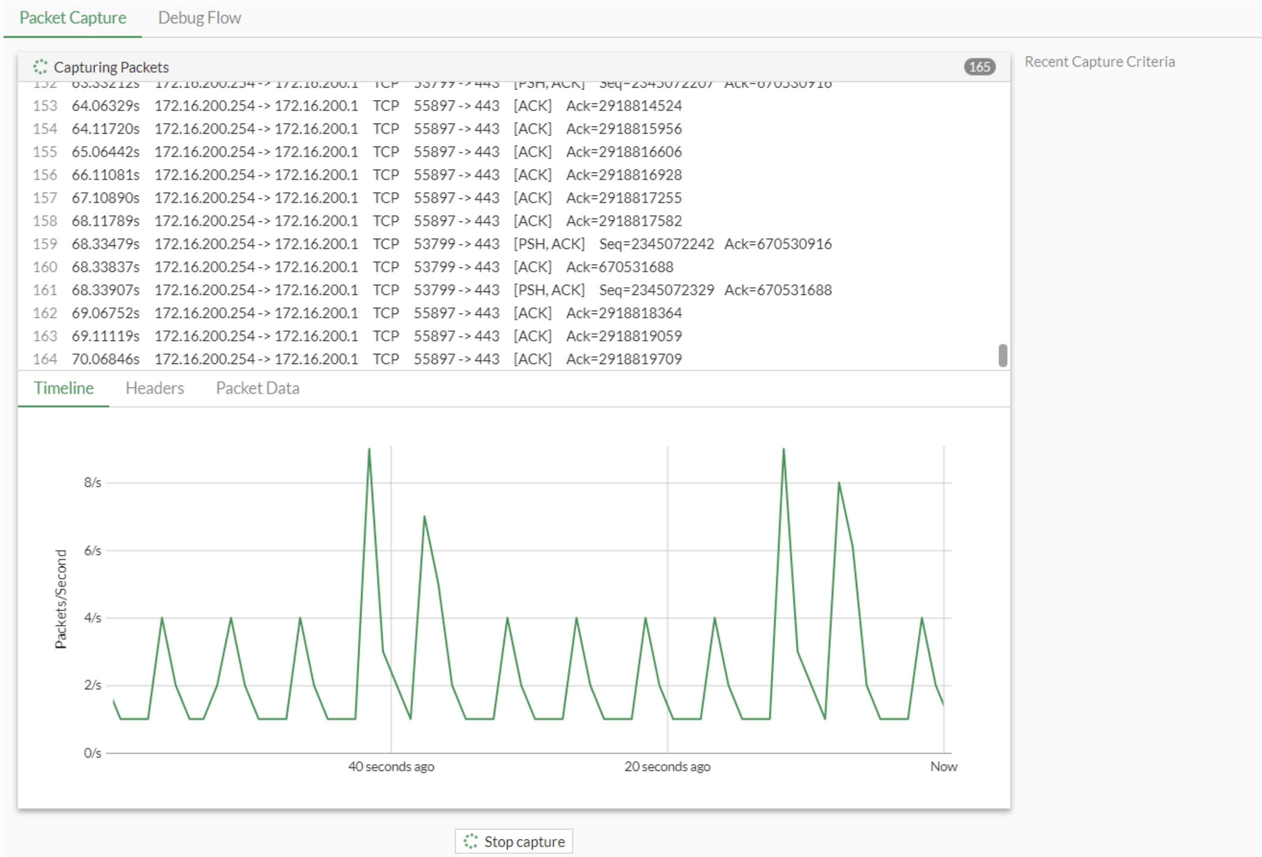
Interface: □ any

Maximum captured packets: ○

Filters: ●

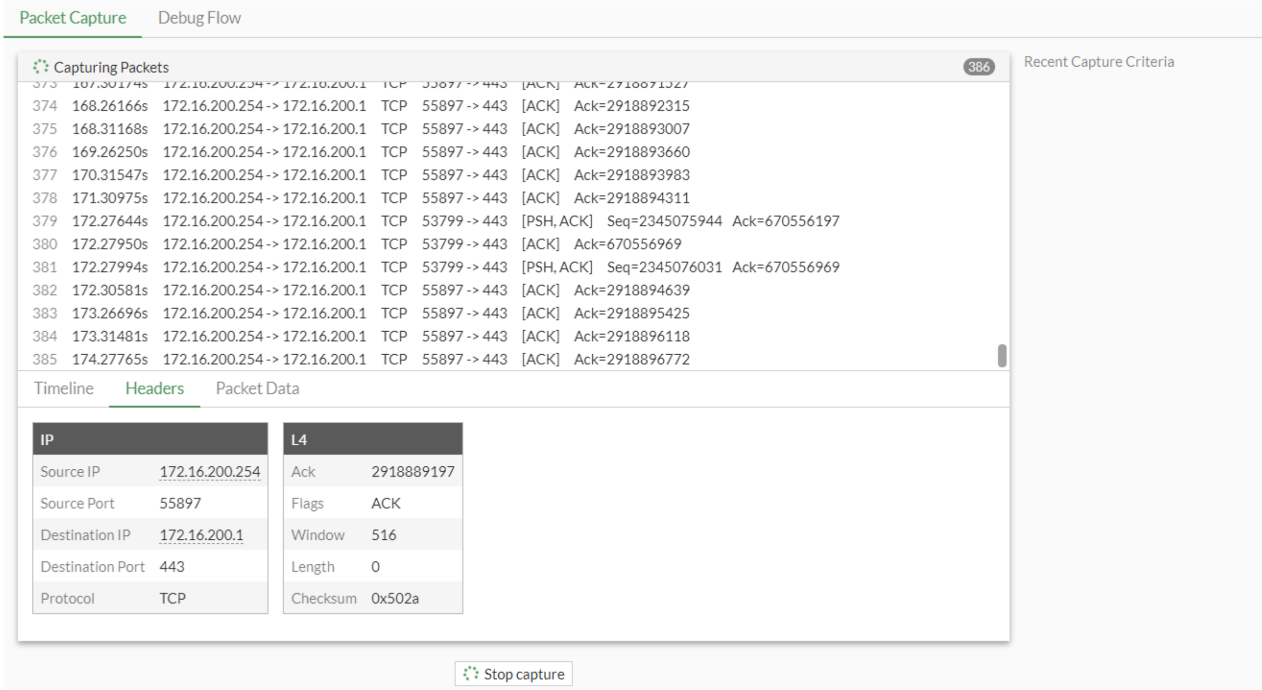
Filtering syntax: Advanced

4. Click *Start capture*. The capture is visible in real-time.



```
152  63.33212s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345072207  Ack=670530916
153  64.06329s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918814524
154  64.11720s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918815956
155  65.06442s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918816606
156  66.11081s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918816928
157  67.10890s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918817255
158  68.11789s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918817582
159  68.33479s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345072242  Ack=670530916
160  68.33837s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [ACK]  Ack=670531688
161  68.33907s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345072329  Ack=670531688
162  69.06752s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918818364
163  69.11119s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918819059
164  70.06846s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918819709
```

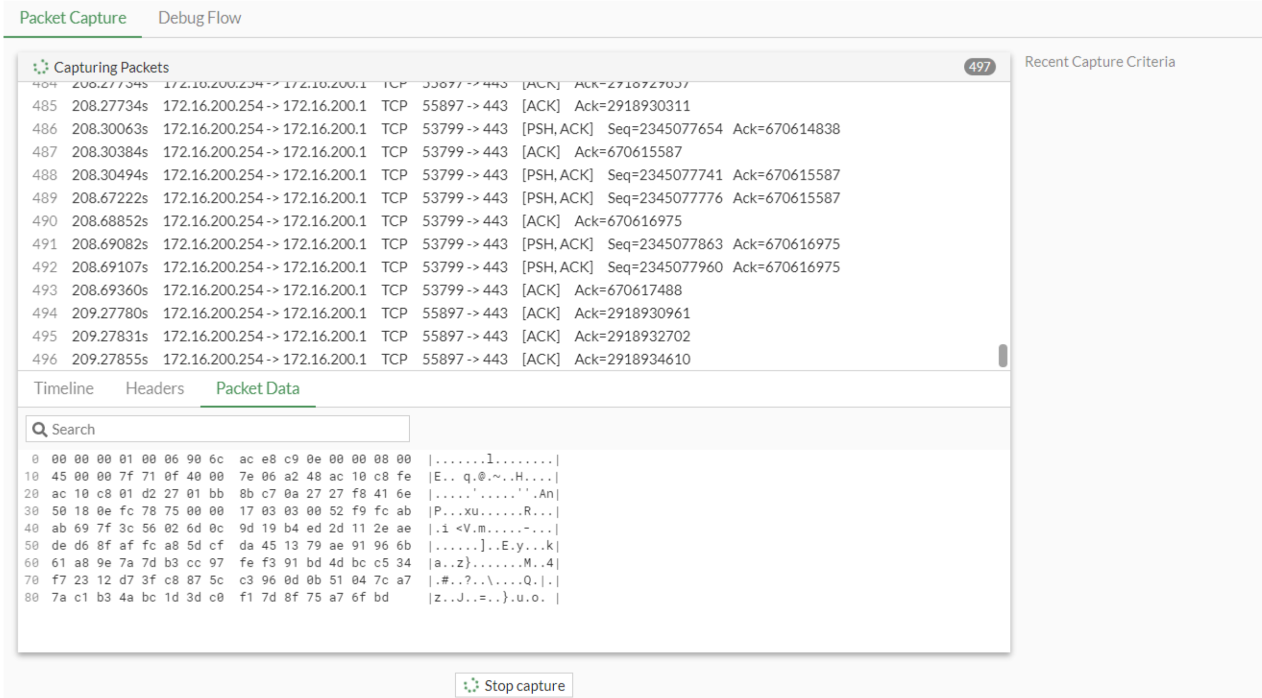
5. While the capture is running, select a packet, then click the *Headers* or *Packet Data* tabs to view more information.



```
373  167.30174s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918891527
374  168.26166s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918892315
375  168.31168s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918893007
376  169.26250s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918893660
377  170.31547s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918893983
378  171.30975s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918894311
379  172.27644s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345075944  Ack=670556197
380  172.27950s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [ACK]  Ack=670556969
381  172.27994s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345076031  Ack=670556969
382  172.30581s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918894639
383  173.26696s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918895425
384  173.31481s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918896118
385  174.27765s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918896772
```

IP	
Source IP	172.16.200.254
Source Port	55897
Destination IP	172.16.200.1
Destination Port	443
Protocol	TCP

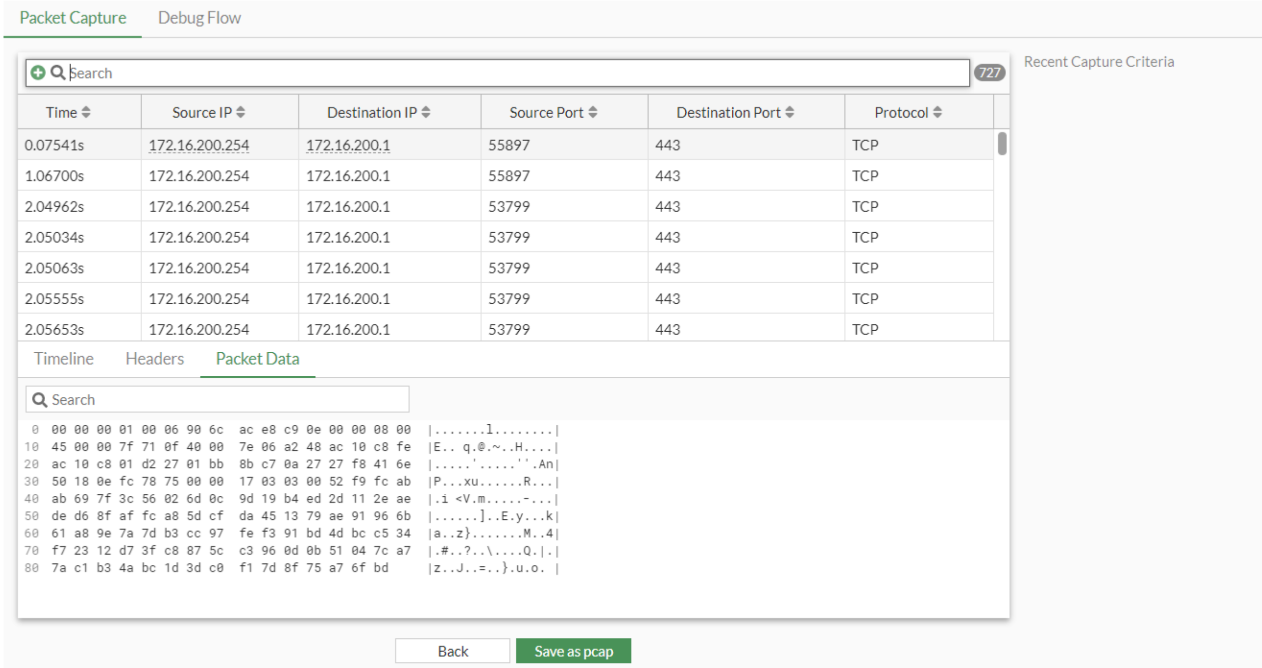
L4	
Ack	2918889197
Flags	ACK
Window	516
Length	0
Checksum	0x502a



```
484  208.27734s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918929657
485  208.27734s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918930311
486  208.30063s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345077654  Ack=670614838
487  208.30384s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [ACK]  Ack=670615587
488  208.30494s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345077741  Ack=670615587
489  208.67222s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345077776  Ack=670615587
490  208.68852s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [ACK]  Ack=670616975
491  208.69082s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345077863  Ack=670616975
492  208.69107s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345077960  Ack=670616975
493  208.69360s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [ACK]  Ack=670617488
494  209.27780s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918930961
495  209.27831s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918932702
496  209.27855s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918934610
```

```
 0  00 00 00 01 00 06 90 6c  ac e8 c9 0e 00 00 08 00  |.......l........|
10  45 00 00 7f 71 0f 40 00  7e 06 a2 48 ac 10 c8 fe  |E.. q.@.~..H....|
20  ac 10 c8 01 d2 27 01 bb  8b c7 0a 27 27 f8 41 6e  |.....'.....''.An|
30  50 18 0e fc 78 75 00 00  17 03 03 00 52 f9 fc ab  |P...xu......R...|
40  ab 69 7f 3c 56 02 6d 0c  9d 19 b4 ed 2d 11 2e ae  |.i <V.m.....-...|
50  de d6 8f af fc a8 5d cf  da 45 13 79 ae 91 96 6b  |......]..E.y...k|
60  61 a8 9e 7a 7d b3 cc 97  fe f3 91 bd 4d bc c5 34  |a..z}.......M..4|
70  f7 23 12 d7 3f c8 87 5c  c3 96 0d 0b 51 04 7c a7  |.#..?..\....Q.|.|
80  7a c1 b3 4a bc 1d 3d c0  f1 7d 8f 75 a7 6f bd     |z..J..=..}.u.o. |
```

6. When the capture is finished, click *Save as pcap*. The PCAP file is automatically downloaded.

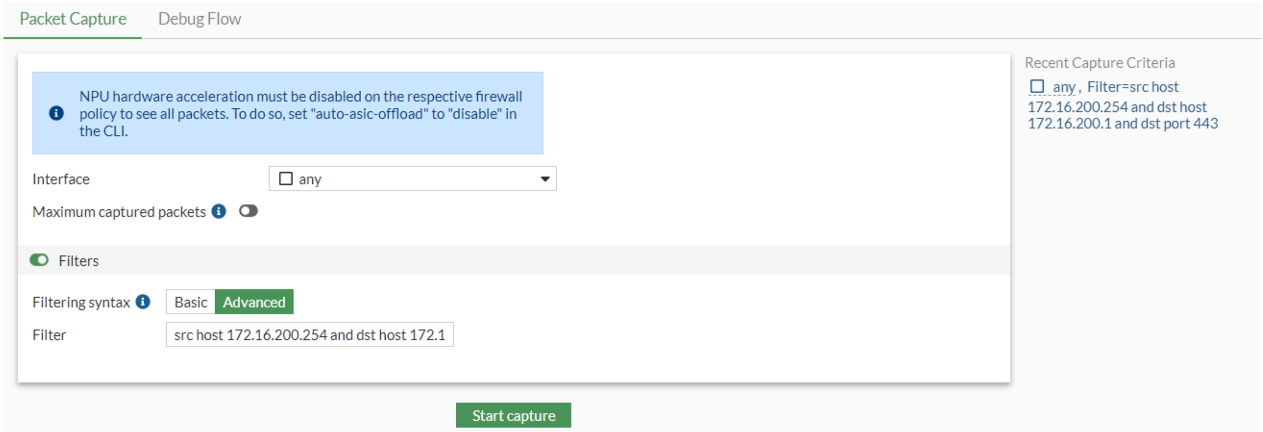


Time	Source IP	Destination IP	Source Port	Destination Port	Protocol
0.07541s	172.16.200.254	172.16.200.1	55897	443	TCP
1.06700s	172.16.200.254	172.16.200.1	55897	443	TCP
2.04962s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05034s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05063s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05555s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05653s	172.16.200.254	172.16.200.1	53799	443	TCP

```
 0  00 00 00 01 00 06 90 6c  ac e8 c9 0e 00 00 08 00  |.......l........|
10  45 00 00 7f 71 0f 40 00  7e 06 a2 48 ac 10 c8 fe  |E.. q.@.~..H....|
20  ac 10 c8 01 d2 27 01 bb  8b c7 0a 27 27 f8 41 6e  |.....'.....''.An|
30  50 18 0e fc 78 75 00 00  17 03 03 00 52 f9 fc ab  |P...xu......R...|
40  ab 69 7f 3c 56 02 6d 0c  9d 19 b4 ed 2d 11 2e ae  |.i <V.m.....-...|
50  de d6 8f af fc a8 5d cf  da 45 13 79 ae 91 96 6b  |......]..E.y...k|
60  61 a8 9e 7a 7d b3 cc 97  fe f3 91 bd 4d bc c5 34  |a..z}.......M..4|
70  f7 23 12 d7 3f c8 87 5c  c3 96 0d 0b 51 04 7c a7  |.#..?..\....Q.|.|
80  7a c1 b3 4a bc 1d 3d c0  f1 7d 8f 75 a7 6f bd     |z..J..=..}.u.o. |
```

7. Optionally, use the *Search* bar or the column headers to filter the results further.

   The packet capture history is listed under *Recent Capture Criteria* in the right-side of the screen. Clicking the hyperlink will take you back to the main page with the interface and filter settings already populated.



NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Interface: □ any

Maximum captured packets

Filters

Filtering syntax: Basic **Advanced**

Filter: src host 172.16.200.254 and dst host 172.1

Recent Capture Criteria
□ any, Filter=src host 172.16.200.254 and dst host 172.16.200.1 and dst port 443

For more granular sniffer output with various verbose settings, use `diagnose sniffer packet <interface> <'filter'> <verbose> <count> <tsformat>`. See Performing a sniffer trace in the FortiOS Administration Guide for more details.

Summary of CLI changes

The following options have been removed from `config firewall sniffer`:

```
config firewall sniffer
    edit <id>
        set ipv6 {enable | disable}
        set non-ip {enable | disable}
        set host <string>
        set port <string>
        set protocol <string>
        set vlan <string>
        set max-packet-count <integer>
    next
end
```

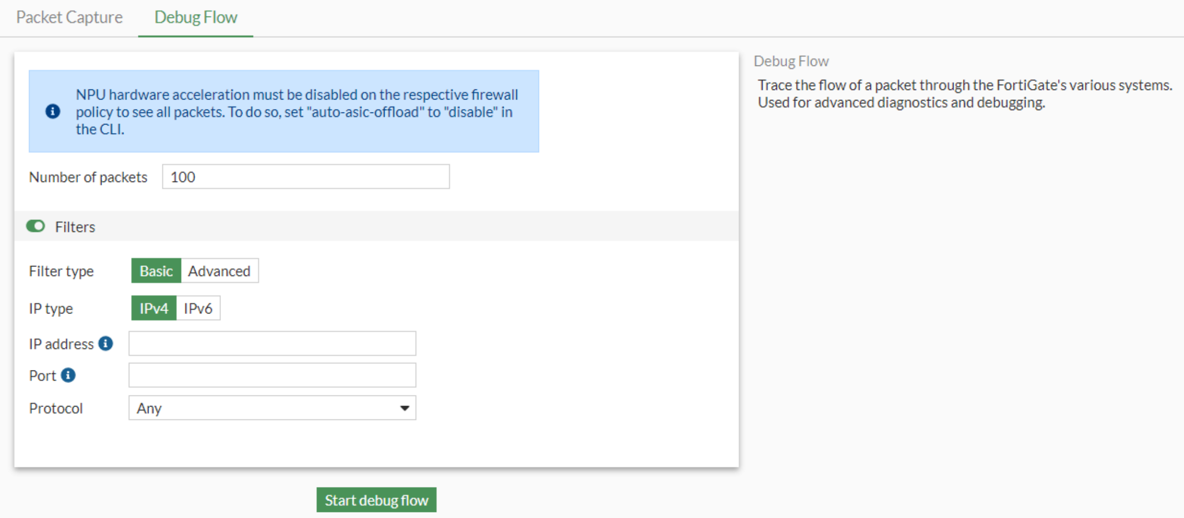
Embed real-time debug flow tool on Diagnostics page

Debug flows can now be executed from the GUI using the *Network > Diagnostics > Debug Flow* page. Debug flow output is displayed in real-time until it is stopped. The completed output can be filtered by time, message, or function. The output can be exported as a CSV file.

To run a debug flow:

1. Go to *Network > Diagnostics* and select the *Debug Flow* tab.
2. Optionally, enable *Filters* and select a *Filter type*:
   a. *Basic*: filter by *IP address*, *Port*, and *Protocol*, which is the equivalent of:
      - `# diagnose debug flow filter addr <addr/range>`
      - `# diagnose debug flow filter port <port/range>`

- `# diagnose debug flow filter proto <protocol>`



NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

Filter type: Basic (selected) | Advanced

IP type: IPv4 (selected) | IPv6

IP address:

Port:

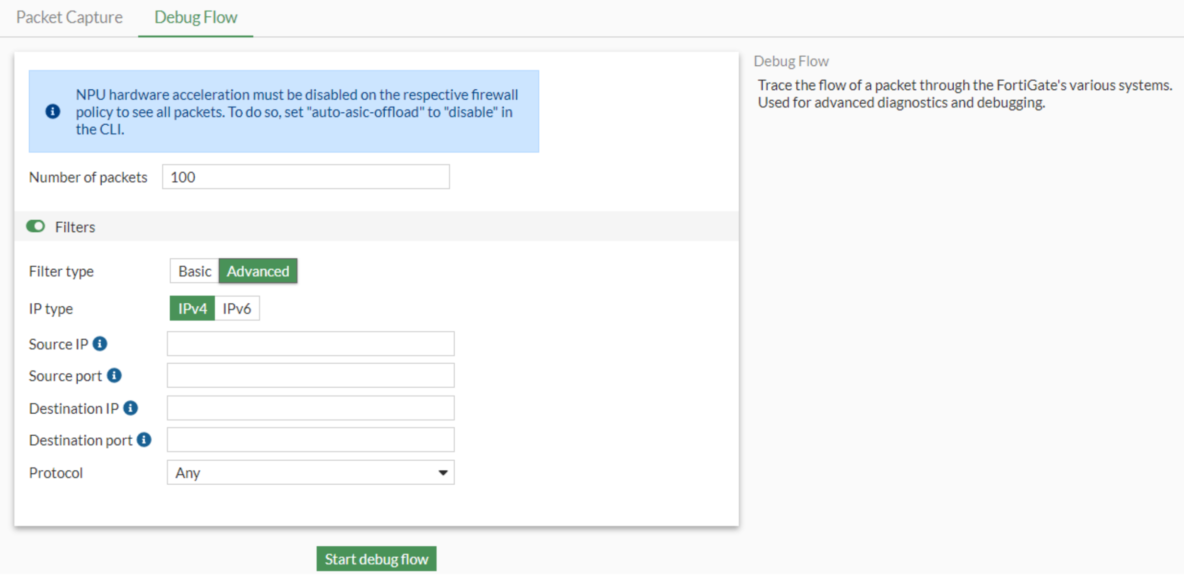
Protocol: Any

Debug Flow

Trace the flow of a packet through the FortiGate's various systems. Used for advanced diagnostics and debugging.

b. *Advanced*: filter by *Source IP*, *Source port*, *Destination IP*, *Destination port*, and *Protocol*, which is the equivalent of:

- `# diagnose debug flow filter saddr <addr/range>`
- `# diagnose debug flow filter sport <port/range>`
- `# diagnose debug flow filter daddr <addr/range>`
- `# diagnose debug flow filter dport <port/range>`
- `# diagnose debug flow filter proto <protocol>`



NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

Filter type: Basic | Advanced (selected)

IP type: IPv4 (selected) | IPv6

Source IP:

Source port:

Destination IP:

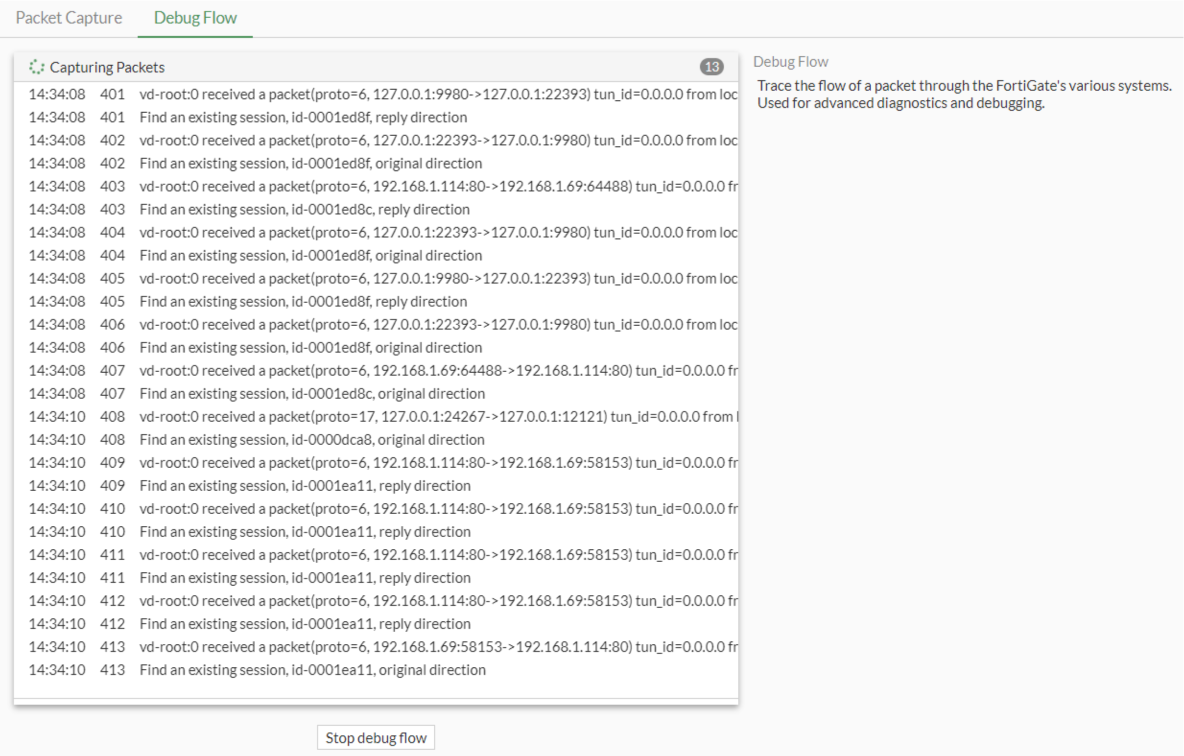
Destination port:

Protocol: Any

Debug Flow

Trace the flow of a packet through the FortiGate's various systems. Used for advanced diagnostics and debugging.

3. Click *Start debug flow*. The debug messages are visible in real-time.

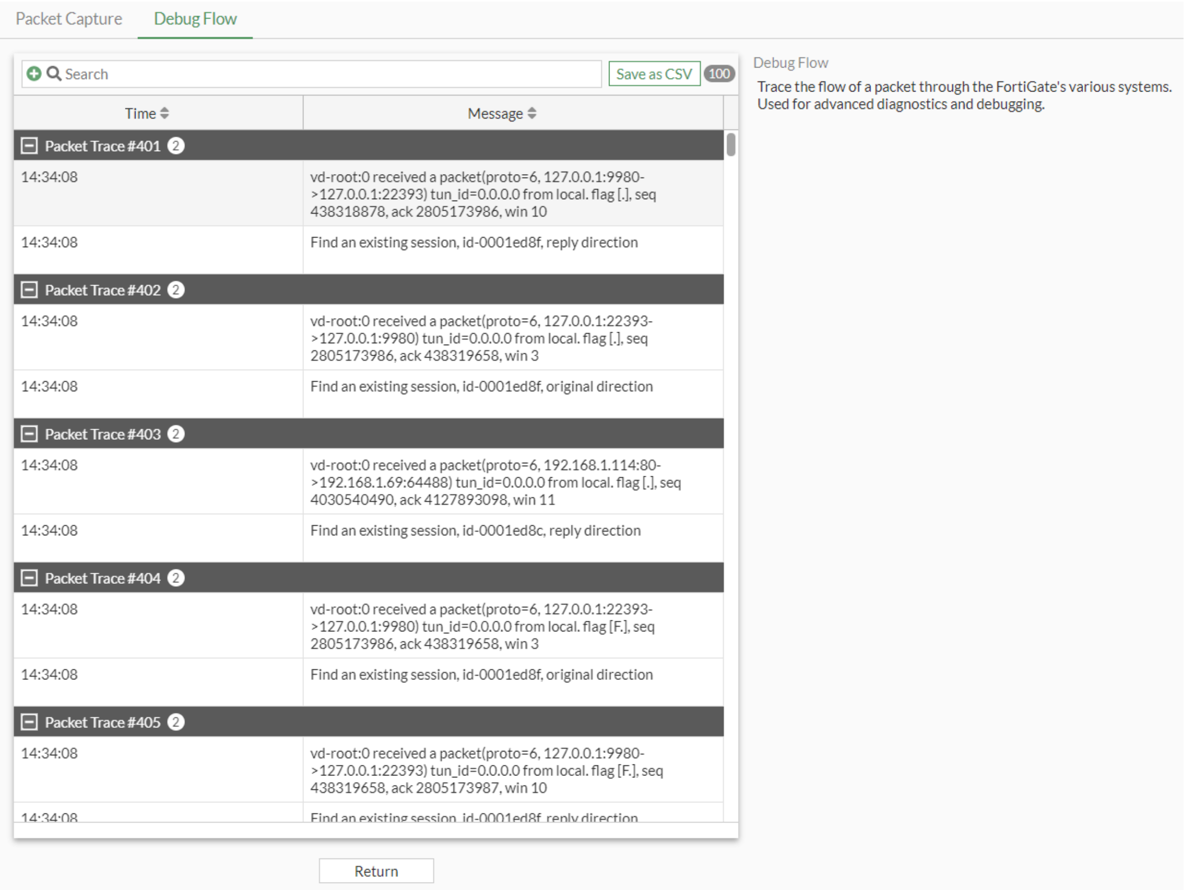


```
14:34:08   401   vd-root:0 received a packet(proto=6, 127.0.0.1:9980->127.0.0.1:22393) tun_id=0.0.0.0 from loc
14:34:08   401   Find an existing session, id-0001ed8f, reply direction
14:34:08   402   vd-root:0 received a packet(proto=6, 127.0.0.1:22393->127.0.0.1:9980) tun_id=0.0.0.0 from loc
14:34:08   402   Find an existing session, id-0001ed8f, original direction
14:34:08   403   vd-root:0 received a packet(proto=6, 192.168.1.114:80->192.168.1.69:64488) tun_id=0.0.0.0 fr
14:34:08   403   Find an existing session, id-0001ed8c, reply direction
14:34:08   404   vd-root:0 received a packet(proto=6, 127.0.0.1:22393->127.0.0.1:9980) tun_id=0.0.0.0 from loc
14:34:08   404   Find an existing session, id-0001ed8f, original direction
14:34:08   405   vd-root:0 received a packet(proto=6, 127.0.0.1:9980->127.0.0.1:22393) tun_id=0.0.0.0 from loc
14:34:08   405   Find an existing session, id-0001ed8f, reply direction
14:34:08   406   vd-root:0 received a packet(proto=6, 127.0.0.1:22393->127.0.0.1:9980) tun_id=0.0.0.0 from loc
14:34:08   406   Find an existing session, id-0001ed8f, original direction
14:34:08   407   vd-root:0 received a packet(proto=6, 192.168.1.69:64488->192.168.1.114:80) tun_id=0.0.0.0 fr
14:34:08   407   Find an existing session, id-0001ed8c, original direction
14:34:10   408   vd-root:0 received a packet(proto=17, 127.0.0.1:24267->127.0.0.1:12121) tun_id=0.0.0.0 from l
14:34:10   408   Find an existing session, id-0000dca8, original direction
14:34:10   409   vd-root:0 received a packet(proto=6, 192.168.1.114:80->192.168.1.69:58153) tun_id=0.0.0.0 fr
14:34:10   409   Find an existing session, id-0001ea11, reply direction
14:34:10   410   vd-root:0 received a packet(proto=6, 192.168.1.114:80->192.168.1.69:58153) tun_id=0.0.0.0 fr
14:34:10   410   Find an existing session, id-0001ea11, reply direction
14:34:10   411   vd-root:0 received a packet(proto=6, 192.168.1.114:80->192.168.1.69:58153) tun_id=0.0.0.0 fr
14:34:10   411   Find an existing session, id-0001ea11, reply direction
14:34:10   412   vd-root:0 received a packet(proto=6, 192.168.1.114:80->192.168.1.69:58153) tun_id=0.0.0.0 fr
14:34:10   412   Find an existing session, id-0001ea11, reply direction
14:34:10   413   vd-root:0 received a packet(proto=6, 192.168.1.69:58153->192.168.1.114:80) tun_id=0.0.0.0 fr
14:34:10   413   Find an existing session, id-0001ea11, original direction
```

Debug Flow

Trace the flow of a packet through the FortiGate's various systems. Used for advanced diagnostics and debugging.

4. When the debug flow is finished (or the user clicks *Stop debug flow*), click *Save as CSV*. The CSV file is automatically downloaded.



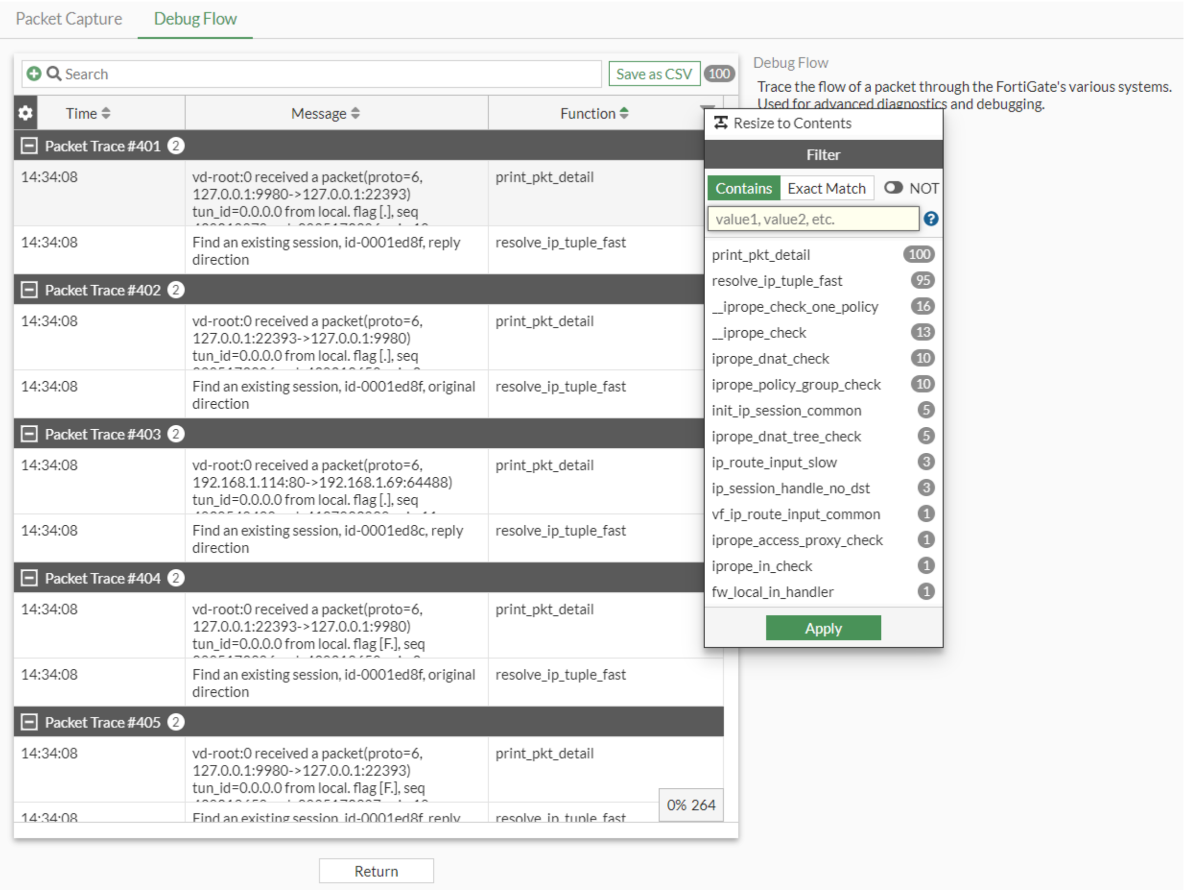
Debug Flow

Trace the flow of a packet through the FortiGate's various systems. Used for advanced diagnostics and debugging.

Time	Message
Packet Trace #401 2	
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:9980->127.0.0.1:22393) tun_id=0.0.0.0 from local. flag [.], seq 438318878, ack 2805173986, win 10
14:34:08	Find an existing session, id-0001ed8f, reply direction
Packet Trace #402 2	
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:22393->127.0.0.1:9980) tun_id=0.0.0.0 from local. flag [.], seq 2805173986, ack 438319658, win 3
14:34:08	Find an existing session, id-0001ed8f, original direction
Packet Trace #403 2	
14:34:08	vd-root:0 received a packet(proto=6, 192.168.1.114:80->192.168.1.69:64488) tun_id=0.0.0.0 from local. flag [.], seq 4030540490, ack 4127893098, win 11
14:34:08	Find an existing session, id-0001ed8c, reply direction
Packet Trace #404 2	
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:22393->127.0.0.1:9980) tun_id=0.0.0.0 from local. flag [F.], seq 2805173986, ack 438319658, win 3
14:34:08	Find an existing session, id-0001ed8f, original direction
Packet Trace #405 2	
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:9980->127.0.0.1:22393) tun_id=0.0.0.0 from local. flag [F.], seq 438319658, ack 2805173987, win 10
14:34:08	Find an existing session, id-0001ed8f, reply direction

The current output can be filtered by *Time* and *Message*. The *Function* field can be added.

5. Hover over the table header and click the gear icon (*Configure Table*).
6. Select *Function* and click *Apply*. The *Function* column is displayed and can be used to filter the output for further analysis.



Debug Flow

Trace the flow of a packet through the FortiGate's various systems. Used for advanced diagnostics and debugging.

Time	Message	Function
Packet Trace #401 2		
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:9980->127.0.0.1:22393) tun_id=0.0.0.0 from local. flag [.], seq	print_pkt_detail
14:34:08	Find an existing session, id-0001ed8f, reply direction	resolve_ip_tuple_fast
Packet Trace #402 2		
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:22393->127.0.0.1:9980) tun_id=0.0.0.0 from local. flag [.], seq	print_pkt_detail
14:34:08	Find an existing session, id-0001ed8f, original direction	resolve_ip_tuple_fast
Packet Trace #403 2		
14:34:08	vd-root:0 received a packet(proto=6, 192.168.1.114:80->192.168.1.69:64488) tun_id=0.0.0.0 from local. flag [.], seq	print_pkt_detail
14:34:08	Find an existing session, id-0001ed8c, reply direction	resolve_ip_tuple_fast
Packet Trace #404 2		
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:22393->127.0.0.1:9980) tun_id=0.0.0.0 from local. flag [F.], seq	print_pkt_detail
14:34:08	Find an existing session, id-0001ed8f, original direction	resolve_ip_tuple_fast
Packet Trace #405 2		
14:34:08	vd-root:0 received a packet(proto=6, 127.0.0.1:9980->127.0.0.1:22393) tun_id=0.0.0.0 from local. flag [F.], seq	print_pkt_detail
14:34:08	Find an existing session, id-0001ed8f, reply	resolve_ip_tuple_fast

print_pkt_detail	100
resolve_ip_tuple_fast	95
__iprope_check_one_policy	16
__iprope_check	13
iprope_dnat_check	10
iprope_policy_group_check	10
init_ip_session_common	5
iprope_dnat_tree_check	5
ip_route_input_slow	3
ip_session_handle_no_dst	3
vf_ip_route_input_common	1
iprope_access_proxy_check	1
iprope_in_check	1
fw_local_in_handler	1

Display detailed FortiSandbox analysis and downloadable PDF report

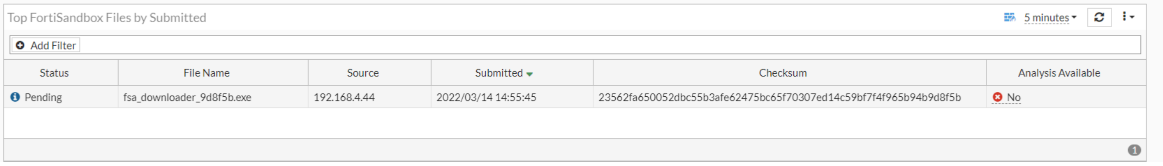
In the *Top FortiSandbox Files* FortiView monitor, users can select a submitted file and drill down to view its static and dynamic file analysis. The full FortiSandbox report can be downloaded in PDF format. This feature works with FortiGate Cloud Sandbox, FortiSandbox Cloud, and FortiSandbox appliance. FortiSandbox must be running version 3.2.1 and later.

Prerequisites:

1. Add FortiSandbox to the Security Fabric (see Sandboxing in the FortiOS Administration Guide).
2. Configure an AV profile with *Send files to FortiSandbox for inspection* enabled (see Using FortiSandbox with antivirus in the FortiOS Administration Guide).
3. Configure a firewall policy with the AV profile that allows traffic to the internet.
4. Add the *Top FortiSandbox Files* FortiView monitor (see Adding FortiView monitors in the FortiOS Administration Guide).
5. On a client PC, attempt to download a suspicious file.

To view the FortiSandbox analysis and download the PDF:

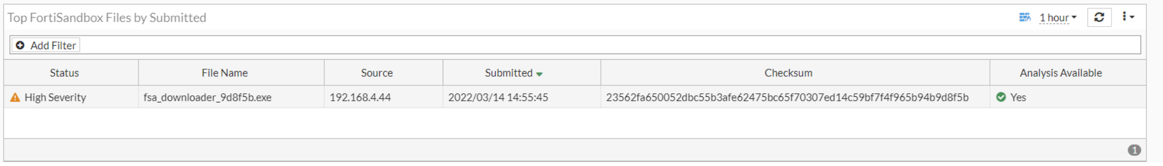
1. Go to *Dashboard > Top FortiSandbox Files*. The entry appears in the table, but the analysis is not available yet.



Top FortiSandbox Files by Submitted

Status	File Name	Source	Submitted	Checksum	Analysis Available
Pending	fsa_downloader_9d8f5b.exe	192.168.4.44	2022/03/14 14:55:45	23562fa650052dbc55b3afe62475bc65f70307ed14c59bf7f4f965b94b9d8f5b	No

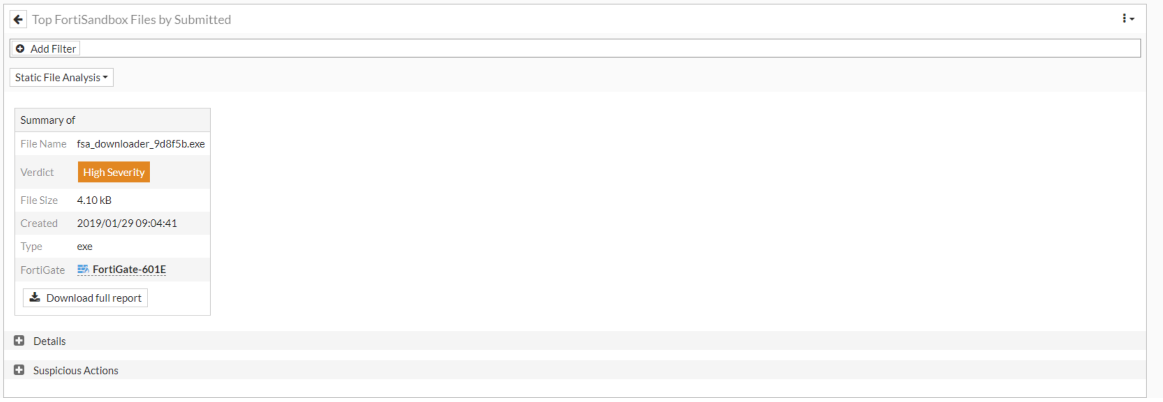
2. After about five to ten minutes, refresh the table. The analysis is available.



Top FortiSandbox Files by Submitted

Status	File Name	Source	Submitted	Checksum	Analysis Available
High Severity	fsa_downloader_9d8f5b.exe	192.168.4.44	2022/03/14 14:55:45	23562fa650052dbc55b3afe62475bc65f70307ed14c59bf7f4f965b94b9d8f5b	Yes

3. Select the entry, then right-click and select *Drill Down to Details*.
4. In the dropdown, select *Static File Analysis* to view the static file analysis.

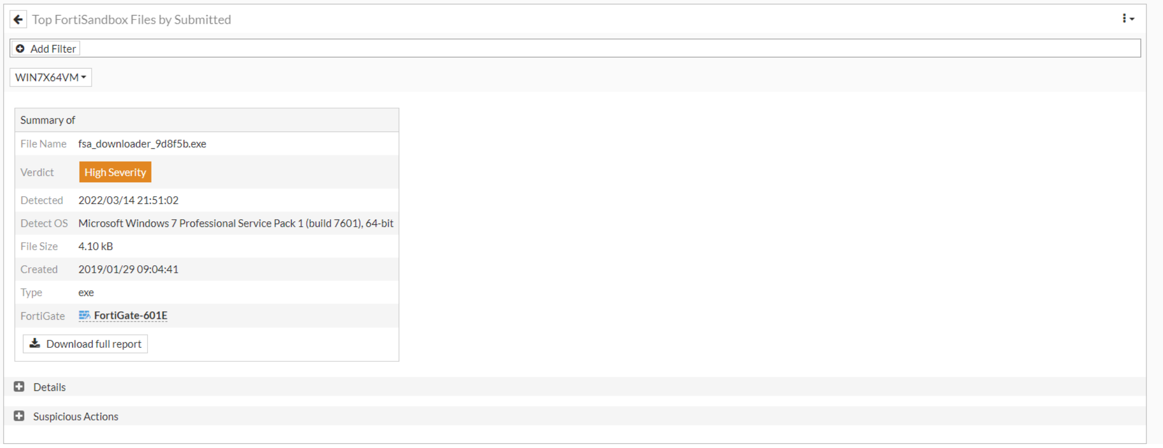


Top FortiSandbox Files by Submitted

Summary of

File Name	fsa_downloader_9d8f5b.exe
Verdict	High Severity
File Size	4.10 kB
Created	2019/01/29 09:04:41
Type	exe
FortiGate	FortiGate-601E

5. In the dropdown, select the client device to view the dynamic file analysis.



Top FortiSandbox Files by Submitted

Summary of

File Name	fsa_downloader_9d8f5b.exe
Verdict	High Severity
Detected	2022/03/14 21:51:02
Detect OS	Microsoft Windows 7 Professional Service Pack 1 (build 7601), 64-bit
File Size	4.10 kB
Created	2019/01/29 09:04:41
Type	exe
FortiGate	FortiGate-601E

6. Click *Download full report* to download the detailed PDF report. The reports contains FortiSandbox job information, detailed file information, static analysis results, and dynamic analysis results.

Starting in FortiOS 7.2.4, PDF reports are downloaded on-demand and only 10 are kept in memory by default. PDFs are deleted from memory after 24 hours.

To change the maximum number of PDFs kept in memory:

```
# diagnose test analytics-pdf-report max <integer>
```

The range is 1 - 10, and the default is 10. After the FortiGate is restarted, this value will revert to the default.

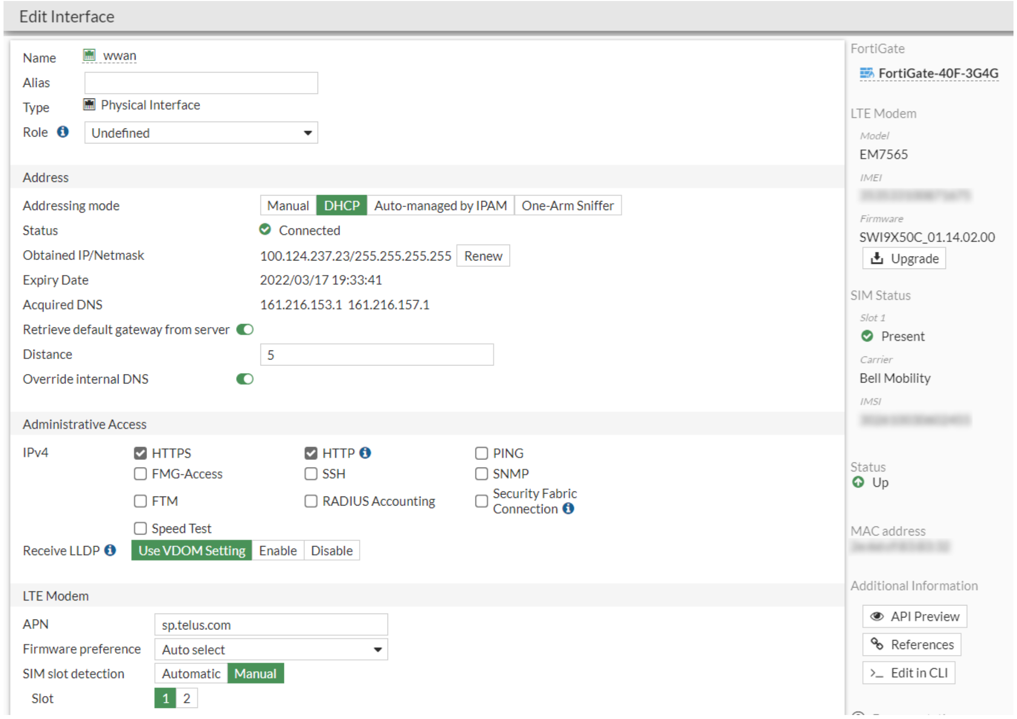
Display LTE modem configuration on GUI of FG-40F-3G4G model

Administrators can view the LTE modem configuration for the FortiGate 40F-3G4G model on the *Network* > *Interfaces* page. The LTE modem interface appears as *wwan* in the GUI.

In the right-side banner, you can also upgrade the firmware or primary rate interface (PRI) and view modem details and SIM status.

To access the LTE modem configuration in the GUI:

1. Go to *Network* > *Interfaces*.
2. Select the *wwan* interface, and click *Edit*. The right-side banner displays details about the modem and the *Upgrade* button for firmware and PRI.
   In the right-side banner, the *LTE modem* area displays the model, International Mobile Equipment Identity (IMEI) number, and firmware version of the modem. The *SIM status* area displays the working SIM slot number, the carrier name, and the International Mobile Subscriber Identity (IMSI) for the modem.



Edit Interface

Name: wwan
Alias:
Type: Physical Interface
Role: Undefined

Address
Addressing mode: Manual [✓ DHCP] Auto-managed by IPAM One-Arm Sniffer
Status: Connected
Obtained IP/Netmask: 100.124.237.23/255.255.255.255 Renew
Expiry Date: 2022/03/17 19:33:41
Acquired DNS: 161.216.153.1 161.216.157.1
Retrieve default gateway from server: ●
Distance: 5
Override internal DNS: ●

Administrative Access
IPv4: ☑ HTTPS ☑ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection □ Speed Test
Receive LLDP: [✓ Use VDOM Setting] Enable Disable

LTE Modem
APN: sp.telus.com
Firmware preference: Auto select
SIM slot detection: Automatic [✓ Manual]
Slot: [✓ 1] 2

FortiGate
FortiGate-40F-3G4G

LTE Modem
Model: EM7565
IMEI: [redacted]
Firmware: SWI9X50C_01.14.02.00
Upgrade

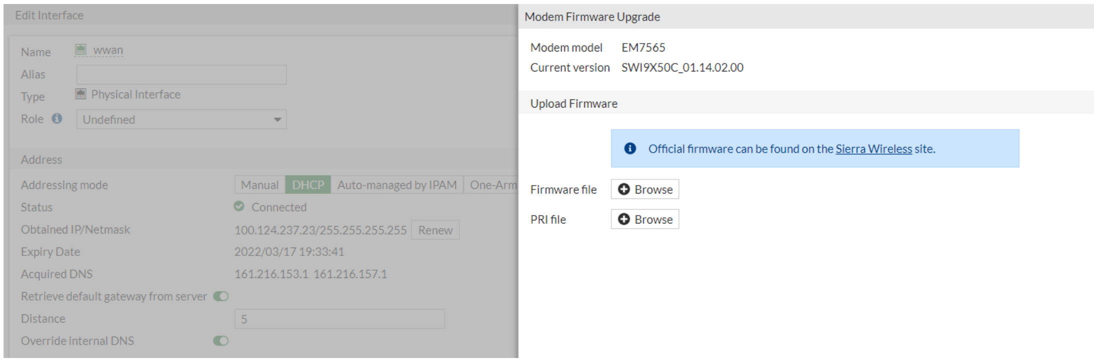
SIM Status
Slot 1: Present
Carrier: Bell Mobility
IMSI: [redacted]

Status: Up

MAC address: [redacted]

Additional Information

3. Optionally set the following fields under *LTE Modem*:
   - Set *APN* to the access point name for the SIM card.
   - Set *SIM slot detection* to *Automatic* or *Manual*. When set to *Manual*, select a slot.
4. In the right-side banner, click *Upgrade* to upgrade the modem firmware or PRI. The *Modem Firmware Upgrade* pane is displayed.



Edit Interface

Name: wwan
Alias:
Type: Physical Interface
Role: Undefined

Address

Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm
Status: Connected
Obtained IP/Netmask: 100.124.237.23/255.255.255.255
Expiry Date: 2022/03/17 19:33:41
Acquired DNS: 161.216.153.1 161.216.157.1
Retrieve default gateway from server
Distance: 5
Override internal DNS

Modem Firmware Upgrade

Modem model: EM7565
Current version: SWI9X50C_01.14.02.00

Upload Firmware

Official firmware can be found on the Sierra Wireless site.

Firmware file: Browse
PRI file: Browse

5. Click *Browse* to select the firmware file or PRI file, and upgrade the modem.

To configure the LTE modem in the CLI:

```
config system lte-modem
    set apn "sp.telus.com"
    set auto-connect enable
    set gps-service enable
    set override-gateway enable
    set sim-hot-swap disable
end
```

To check LTE modem status in the CLI:

```
# diagnose sys lte-modem modem-details
LTE Modem detailed information:
Modem detected:       Yes
Manufacturer:         Sierra Wireless, Incorporated
Model:                EM7565
Revision:             SWI9X50C_01.14.02.00 2e210b jenkins 2020/08/19 14:18:39
MSISDN:               <number>
ESN:                  0
IMEI:                 <number>
MEID:
Hardware revision:    1.0
Software revision:    S.AT.2.5.1-00666-9655_GEN_PACK-1
SKU:
FSN:                  UF01037177021047
PRL version:          0x0000
Modem FW version:     01.14.02.00
PRI version:          002.035_003
Carrier Abbr:         GENERIC
Modem Operation mode:      QMI_DMS_OPERATING_MODE_ONLINE
```

To upgrade LTE modem firmware in the CLI:

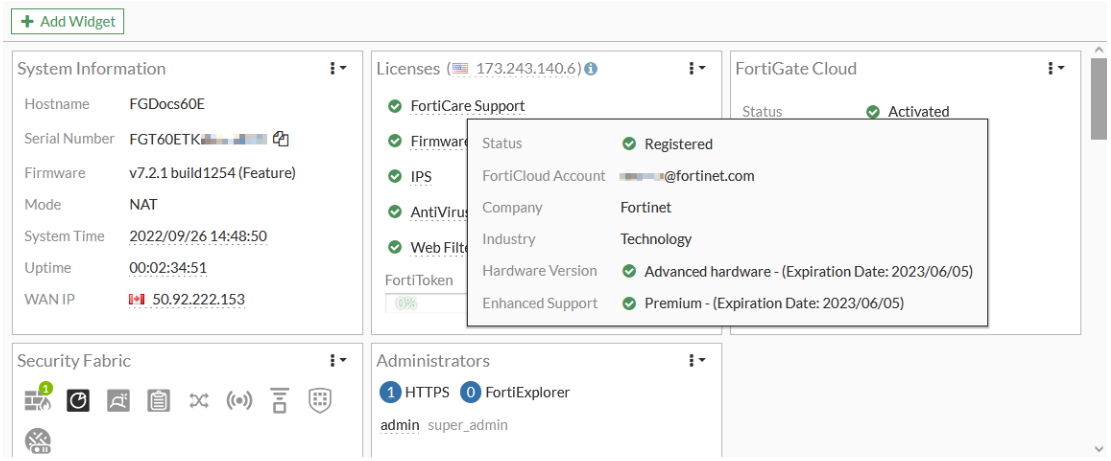
```
# execute lte-modem get-modem-firmware ftp SWI9X50C_01.09.04.00.cwe 192.168.1.73 anonymous
asd
Please wait...

Connect to ftp server 192.168.1.73 ...
Get image from ftp server OK.
```

```
# execute lte-modem get-pri-firmware ftp SWI9X50C_01.09.04.00_DOCOMO_002.015_002.nvu
192.168.1.73 anonymous asd
Please wait...

Connect to ftp server 192.168.1.73 ...
Get image from ftp server OK.

# execute lte-modem start-upgrade
You are going to burn the following images into your LTE modem.
---------------------------------------------------------
Modem image:            SWI9X50C_01.09.04.00.cwe
PRI image:              SWI9X50C_01.09.04.00_DOCOMO_002.015_002.nvu
---------------------------------------------------------
The original images on your LTE Modem will be replaced!
Do you want to continue? (y/n)y

Starting LTE Modem firmware upgrade, please don't power off your device
until the whole process is done!
LTE Modem firmware upgrade routine will run in the background.

.Image information from the modem:
Modem image count ==> 2
Image type ==> 0
Modem firmware version ==> 01.09.04.00
PRI firmware version ==> 002.015_002
Carrier abbr ==> DOCOMO
Image type ==> 1
Modem firmware version ==> 01.09.04.00
PRI firmware version ==> 002.015_002
Carrier abbr ==> DOCOMO
Modem name ==> EM7565

Information from the image file
Image model name = SWI9X50C
Image modem firmware version = 01.09.04.00
Image carrier name = DOCOMO
Image carrier PRI version = 002.015
Image carrier pack version = 002
.
EM7565 Modem Firmware Upgrade Process succeeded!

Restart the LTE daemon.
```

Update naming of FortiCare support levels - 7.2.1

In the *Licenses* widget on the *Dashboard* > *Status* page, the *FortiCare Support* tooltip displays the corresponding support level associated with the account: *Essential*, *Premium*, or *Elite* in the *Enhanced Support* field.

Sample premium support level:



+ Add Widget

System Information

Hostname	FGDocs60E
Serial Number	FGT60ETK[redacted]
Firmware	v7.2.1 build1254 (Feature)
Mode	NAT
System Time	2022/09/26 14:48:50
Uptime	00:02:34:51
WAN IP	50.92.222.153

Licenses (173.243.140.6)

- FortiCare Support
- Firmware
- IPS
- AntiViru
- Web Filt

FortiToken 0%

Status	✓ Registered
FortiCloud Account	[redacted]@fortinet.com
Company	Fortinet
Industry	Technology
Hardware Version	✓ Advanced hardware - (Expiration Date: 2023/06/05)
Enhanced Support	✓ Premium - (Expiration Date: 2023/06/05)

FortiGate Cloud

Status ✓ Activated

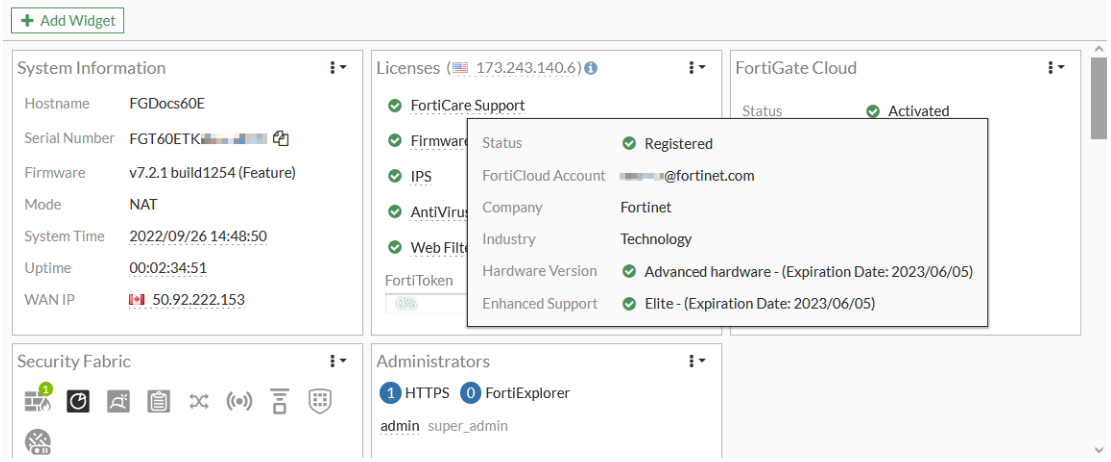
Security Fabric

Administrators

1 HTTPS 0 FortiExplorer

admin super_admin

Sample elite support level:



+ Add Widget

System Information

Hostname	FGDocs60E
Serial Number	FGT60ETK[redacted]
Firmware	v7.2.1 build1254 (Feature)
Mode	NAT
System Time	2022/09/26 14:48:50
Uptime	00:02:34:51
WAN IP	50.92.222.153

Licenses (173.243.140.6)

- FortiCare Support
- Firmware
- IPS
- AntiViru
- Web Filt

FortiToken 0%

Status	✓ Registered
FortiCloud Account	[redacted]@fortinet.com
Company	Fortinet
Industry	Technology
Hardware Version	✓ Advanced hardware - (Expiration Date: 2023/06/05)
Enhanced Support	✓ Elite - (Expiration Date: 2023/06/05)

FortiGate Cloud

Status ✓ Activated

Security Fabric

Administrators

1 HTTPS 0 FortiExplorer

admin super_admin

Security Fabric

This section includes information about Security Fabric new features:

- Fabric settings on page 30
- External connectors on page 63
- Automation stitches on page 73
- Security ratings on page 86

Fabric settings

This section includes information about Security Fabric settings related new features:

- Automatic regional discovery for FortiSandbox Cloud on page 30
- Follow the upgrade path in a federated update on page 31
- Rename FortiAI to FortiNDR on page 34
- Register all HA members to FortiCare from the primary unit on page 37
- Remove support for Security Fabric loose pairing on page 40
- Allow FortiSwitch and FortiAP upgrade when the Security Fabric is disabled on page 40
- Add support for multitenant FortiClient EMS deployments 7.2.1 on page 42
- Add IoT devices to Asset Identity Center page 7.2.1 on page 45
- Introduce distributed topology and security rating reports 7.2.1 on page 46
- Add IoT vulnerabilities to the asset identity list and FortiGuard IoT security rating checks 7.2.4 on page 47
- Enhance the Fabric Connectors page 7.2.4 on page 50
- Add FortiPolicy as Security Fabric device 7.2.4 on page 56
- Allow FortiClient EMS connectors to trust EMS server certificate renewals based on the CN field 7.2.4 on page 61

Automatic regional discovery for FortiSandbox Cloud

The FortiGate will automatically connect to fortisandboxcloud.com, and then discover the specific region and server to connect to based on which region the customer selected to deploy their FortiSandbox Cloud instance. FortiSandbox Cloud 4.0.0 (or later) is required for this functionality. The FortiGate must have a FortiCloud premium account license and a FortiSandbox Cloud VM license.

To verify the automatic FortiSandbox Cloud regional discovery:

1. Configure FortiSandbox Cloud:
   - In the GUI:
     i. Go to *Security Fabric > Fabric Connectors* and double-click the *Cloud Sandbox* card.
     ii. Set *Status* to *Enable*.
     iii. For *Type*, select *FortiSandbox Cloud*.
     iv. Click *OK*.

- In the CLI, enter the following:

  ```
  config system fortisandbox
      set status enable
      set forticloud enable
      set server "fortisandboxcloud.com"
  end
  ```

2. Verify the quarantine daemon debug output. Currently, the FortiGate connects to fortisandboxcloud.com:

   ```
   # diagnose debug application quarantine -1
       ...
       __quar_start_connection()-961: start server fortisandbox-fsb1-66.35.19.98 in vdom-3
       __quar_oftp_get_oif()-930: dev fortisandbox-fsb1 get oif 0
       ...
   ```

3. Once the FortiGate connects to the FortiSandbox controller, it receives the region information and attempts to connect to the specific regional server (ca-west-1):

   ```
   # diagnose debug application quarantine -1
       ...
       __quar_remote_connect()-806: oftp_connect region server: ca-west-
   1.fortisandboxcloud.com.
       __quar_start_connection()-962: start server fortisandbox-fsb1-66.35.19.98 in vdom-0
       ...
   ```

4. Verify that the connection is established to the new region (ca-west-1):

   ```
   # diagnose test application quarantined 1
   forticloud-fsb is disabled.
   fortisandbox-fsb1(ca-west-1.fortisandboxcloud.com) is enabled: analytics, realtime=yes,
   taskfull=no
       addr=66.35.19.98/514, source-ip=0.0.0.0, keep-alive=no.
       ssl_opt=3, hmac_alg=0
       intf_sel=auto() oif=0
   ```

Follow the upgrade path in a federated update

When performing a Fabric upgrade or non-Fabric upgrade under *System* > *Fabric Management* and choosing a firmware that requires multiple builds in the upgrade path, the FortiGate can follow the upgrade path to complete the upgrade automatically. This can be performed immediately or during a scheduled time.

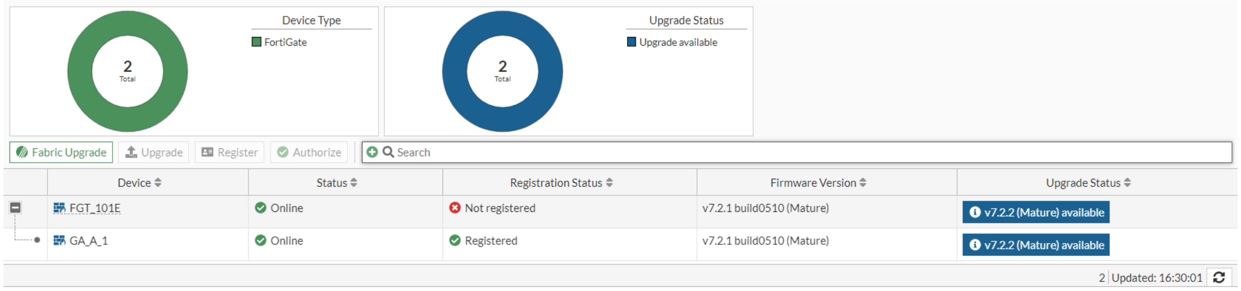
The *System* > *Firmware* page in the tree menu has been removed. The *System* > *Firmware* shortcut in the top-right dropdown (username menu) has also been removed. It was replaced with a shortcut to the *Fabric Management* page.

To demonstrate the functionality of this feature, this example uses FortiGates that are running and upgrading to fictitious build numbers.

FortiAPs and FortiSwitches currently cannot follow the upgrade path. They upgrade directly to the target version.

Example

In this example, the Security Fabric consists of a root FortiGate (FGT_101E) and a downstream FortiGate (GA_A_1). The FortiGates are currently running FortiOS 7.2.1 (build 0510). The administrator wants to upgrade the firmware to version 7.4.0 (build 0810). When upgrading the firmware on the *Fabric Management* page, the FortiGate is able to display the upgrade path, 7.2.1 > 7.2.2 > 7.4.0, and perform all of the upgrades in sequence (with multiple reboots).

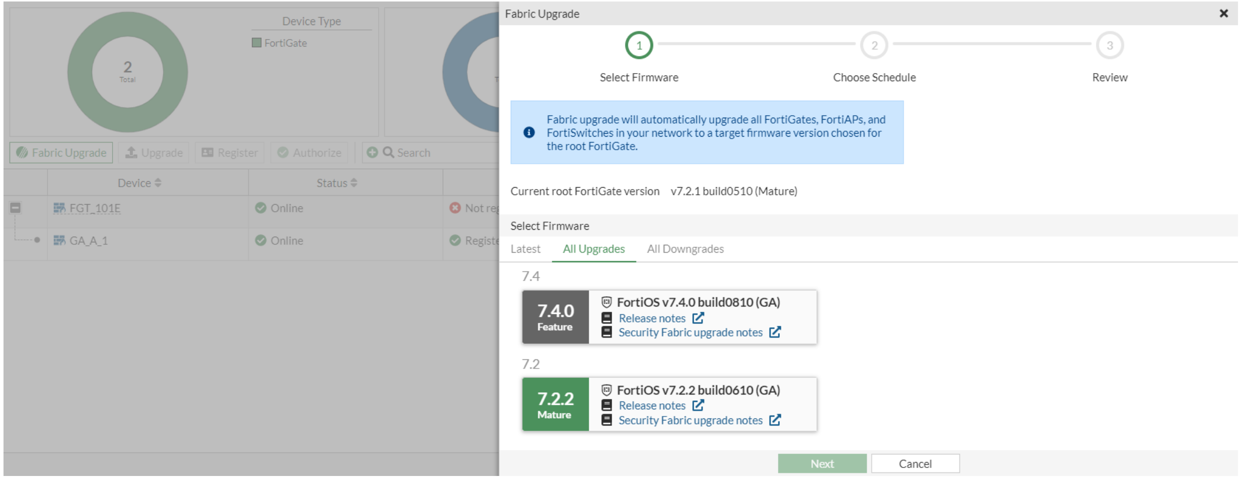


Device	Status	Registration Status	Firmware Version	Upgrade Status
FGT_101E	Online	Not registered	v7.2.1 build0510 (Mature)	v7.2.2 (Mature) available
GA_A_1	Online	Registered	v7.2.1 build0510 (Mature)	v7.2.2 (Mature) available

2 Updated: 16:30:01

To upgrade the FortiGate firmware:

1. Go to *System > Fabric Management* and click *Fabric Upgrade*. The *Fabric Upgrade* pane opens.
2. In the *Select Firmware* section, select *All Upgrades*.



Fabric upgrade will automatically upgrade all FortiGates, FortiAPs, and FortiSwitches in your network to a target firmware version chosen for the root FortiGate.

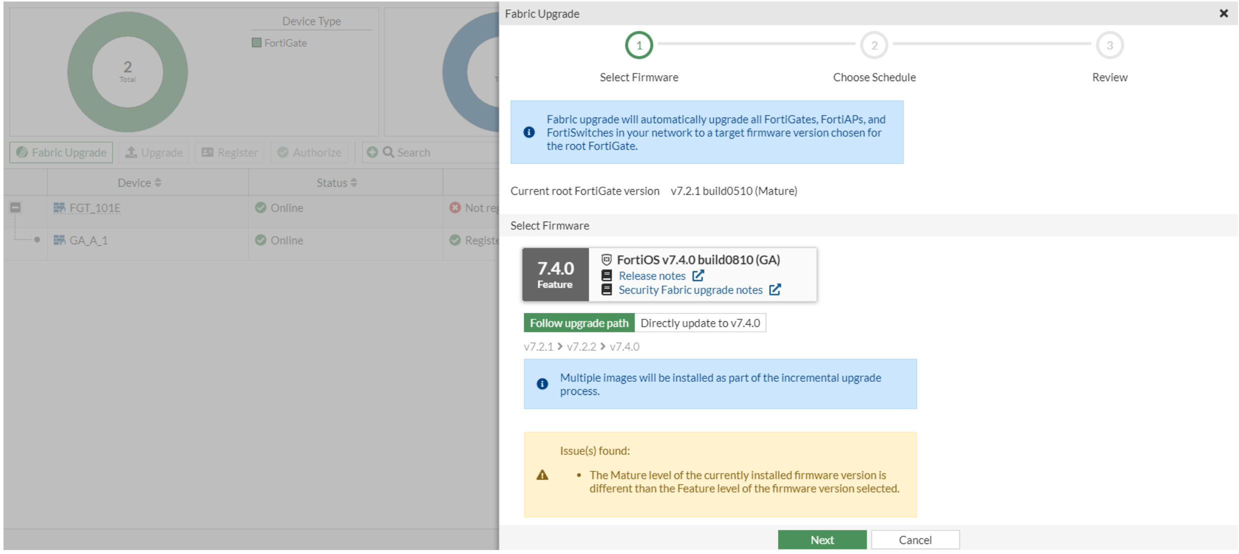
Current root FortiGate version v7.2.1 build0510 (Mature)

Select Firmware

FortiOS v7.4.0 build0810 (GA)
Release notes
Security Fabric upgrade notes

FortiOS v7.2.2 build0610 (GA)
Release notes
Security Fabric upgrade notes

3. Select the 7.4.0 version. Upgrade options appear.
4. Select *Follow upgrade path*. The upgrade path is displayed: *v7.2.1 > v7.2.2 > v7.4.0*.



Fabric upgrade will automatically upgrade all FortiGates, FortiAPs, and FortiSwitches in your network to a target firmware version chosen for the root FortiGate.

Current root FortiGate version v7.2.1 build0510 (Mature)

Select Firmware

FortiOS v7.4.0 build0810 (GA)
Release notes
Security Fabric upgrade notes

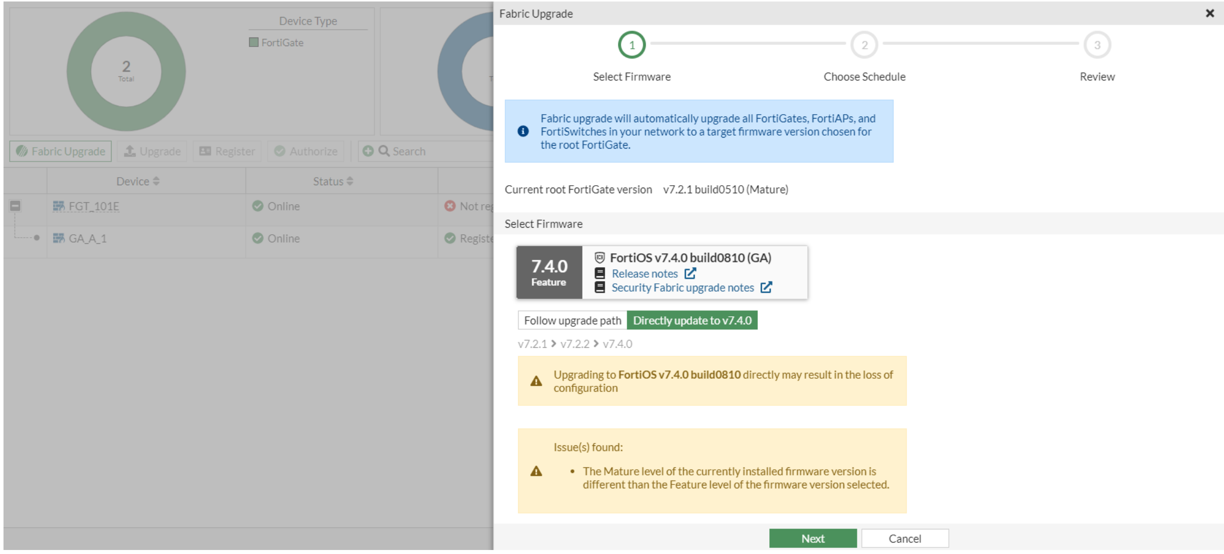
v7.2.1 > v7.2.2 > v7.4.0

Multiple images will be installed as part of the incremental upgrade process.

Issue(s) found:

- The Mature level of the currently installed firmware version is different than the Feature level of the firmware version selected.

- If *Directly upgrade to v7.4.0* is selected, a warning message appears that this may result in the loss of configuration.



Fabric Upgrade

1 Select Firmware — 2 Choose Schedule — 3 Review

Fabric upgrade will automatically upgrade all FortiGates, FortiAPs, and FortiSwitches in your network to a target firmware version chosen for the root FortiGate.

Current root FortiGate version v7.2.1 build0510 (Mature)

Select Firmware

7.4.0 Feature — FortiOS v7.4.0 build0810 (GA)
Release notes
Security Fabric upgrade notes

Follow upgrade path | Directly update to v7.4.0

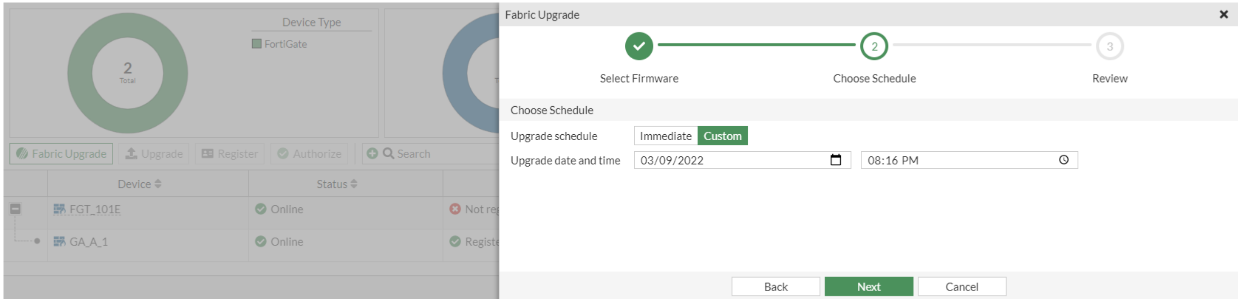
v7.2.1 > v7.2.2 > v7.4.0

Upgrading to **FortiOS v7.4.0 build0810** directly may result in the loss of configuration

Issue(s) found:

- The Mature level of the currently installed firmware version is different than the Feature level of the firmware version selected.

5. Click *Next*.
6. Select an upgrade schedule, either *Immediate* or *Custom*. If using *Custom*, enter an upgrade date and time (*Custom* is used in this example).



Fabric Upgrade

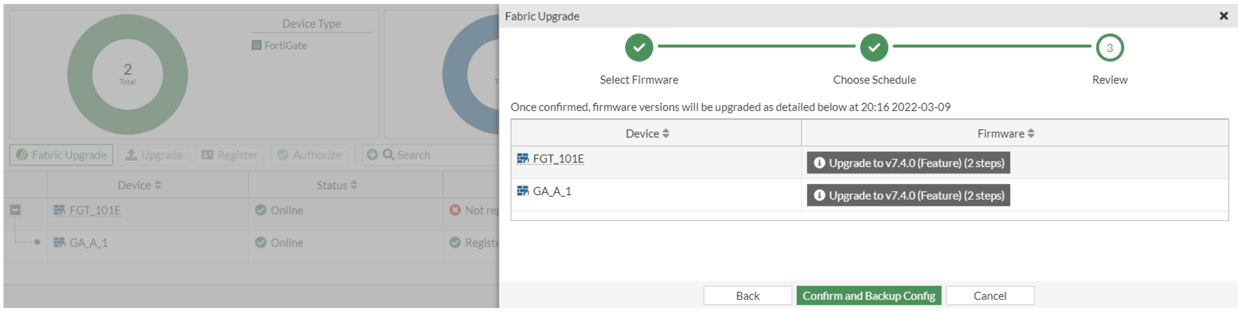
Select Firmware — 2 Choose Schedule — 3 Review

Choose Schedule

Upgrade schedule: Immediate | Custom

Upgrade date and time: 03/09/2022 08:16 PM

7. Click *Next* and review the update schedule.
8. Click *Confirm and Backup Config*.



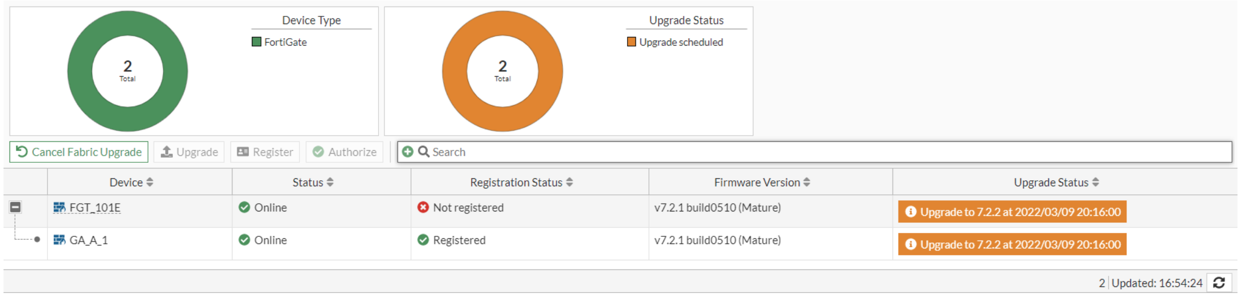
Fabric Upgrade

Select Firmware — Choose Schedule — 3 Review

Once confirmed, firmware versions will be upgraded as detailed below at 20:16 2022-03-09

Device	Firmware
FGT_101E	Upgrade to v7.4.0 (Feature) (2 steps)
GA_A_1	Upgrade to v7.4.0 (Feature) (2 steps)

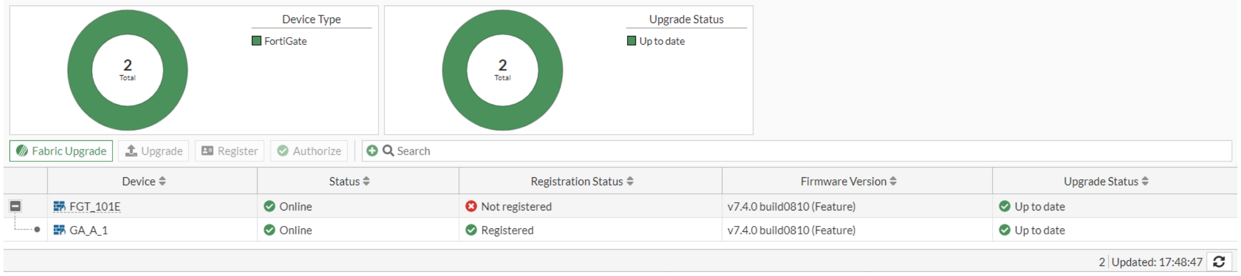
The *Upgrade Status* for both FortiGates indicated when the scheduled upgrade will take place. In this example, the first upgrade in the path is to version 7.2.2. The FortiGates will reboot and then upgrade to 7.4.0 as per the upgrade path.



Device	Status	Registration Status	Firmware Version	Upgrade Status
FGT_101E	✓ Online	✗ Not registered	v7.2.1 build0510 (Mature)	Upgrade to 7.2.2 at 2022/03/09 20:16:00
GA_A_1	✓ Online	✓ Registered	v7.2.1 build0510 (Mature)	Upgrade to 7.2.2 at 2022/03/09 20:16:00

2 Updated: 16:54:24

Once the upgrades are complete and both FortiGates are running the desired firmware (7.4.0), the *Upgrade Status* changes to *Up to date*.



Device	Status	Registration Status	Firmware Version	Upgrade Status
FGT_101E	✓ Online	✗ Not registered	v7.4.0 build0810 (Feature)	✓ Up to date
GA_A_1	✓ Online	✓ Registered	v7.4.0 build0810 (Feature)	✓ Up to date

2 Updated: 17:48:47

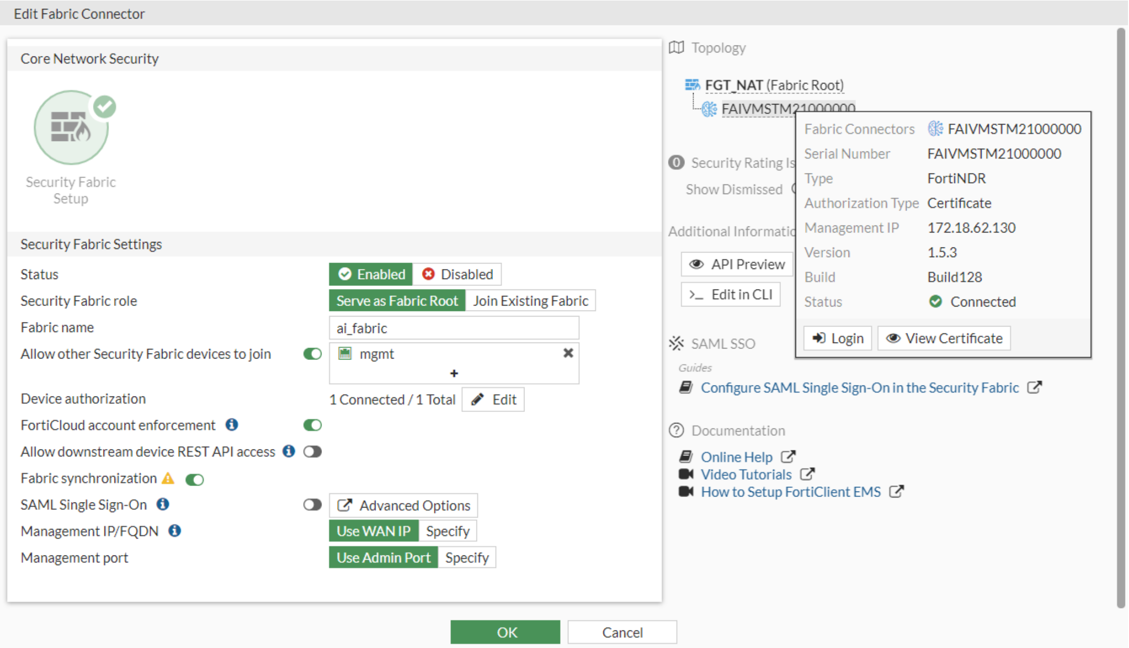
Rename FortiAI to FortiNDR

FortiAI has been renamed FortiNDR in the GUI and CLI to align with the FortiNDR rebranding. Previous CLI-only settings for sending files to FortiNDR for inspection can be configured from the *AntiVirus profile Page* in the GUI.

FortiNDR is still referred to as `fai` or `FAI` in debug traces from `diagnose sys scanunit debug all`.

Summary of GUI changes

The Fabric connector *Type* has been updated to *FortiNDR*, which is visible in the connector tooltip. In this example, the connector is running version 1.5.3, so the connector name still begins with *FAI*.



Edit Fabric Connector

Core Network Security

Security Fabric Setup

Security Fabric Settings

Status	● Enabled ✖ Disabled
Security Fabric role	Serve as Fabric Root Join Existing Fabric
Fabric name	ai_fabric
Allow other Security Fabric devices to join	● mgmt ✖ +
Device authorization	1 Connected / 1 Total Edit
FortiCloud account enforcement	●
Allow downstream device REST API access	○
Fabric synchronization ⚠	●
SAML Single Sign-On	○ Advanced Options
Management IP/FQDN	Use WAN IP Specify
Management port	Use Admin Port Specify

Topology

FGT_NAT (Fabric Root)
FAIVMSTM21000000

Fabric Connectors	FAIVMSTM21000000
Serial Number	FAIVMSTM21000000
Type	FortiNDR
Authorization Type	Certificate
Management IP	172.18.62.130
Version	1.5.3
Build	Build128
Status	✓ Connected

Login View Certificate

Security Rating Is
Show Dismissed
Additional Informatio

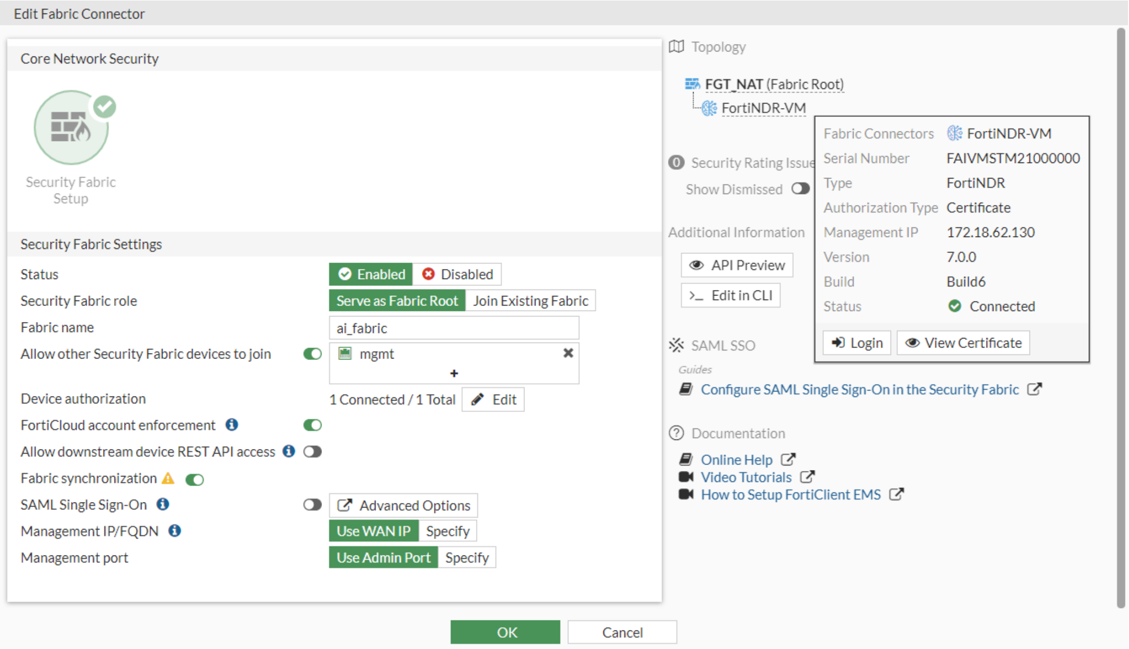
API Preview
Edit in CLI

SAML SSO
Guides
Configure SAML Single Sign-On in the Security Fabric

Documentation
Online Help
Video Tutorials
How to Setup FortiClient EMS

OK Cancel

In this example, the connector is running version 7.0.0, so the connector name has changed to *FortiNDR-VM*.



Edit Fabric Connector

Core Network Security

Security Fabric Setup

Security Fabric Settings

Status	● Enabled ✖ Disabled
Security Fabric role	Serve as Fabric Root Join Existing Fabric
Fabric name	ai_fabric
Allow other Security Fabric devices to join	● mgmt ✖ +
Device authorization	1 Connected / 1 Total Edit
FortiCloud account enforcement	●
Allow downstream device REST API access	○
Fabric synchronization ⚠	●
SAML Single Sign-On	○ Advanced Options
Management IP/FQDN	Use WAN IP Specify
Management port	Use Admin Port Specify

Topology

FGT_NAT (Fabric Root)
FortiNDR-VM

Fabric Connectors	FortiNDR-VM
Serial Number	FAIVMSTM21000000
Type	FortiNDR
Authorization Type	Certificate
Management IP	172.18.62.130
Version	7.0.0
Build	Build6
Status	✓ Connected

Login View Certificate

Security Rating Issue
Show Dismissed ○
Additional Information

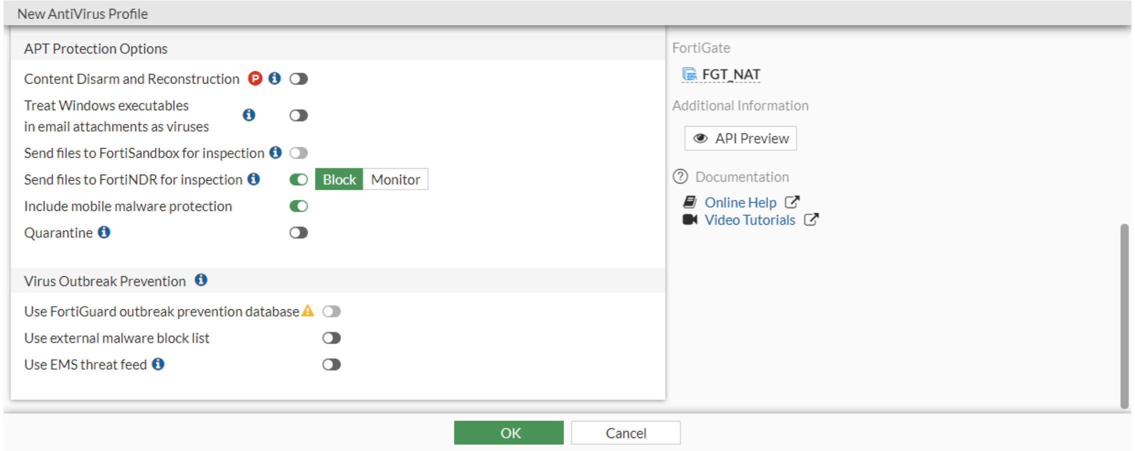
API Preview
Edit in CLI

SAML SSO
Guides
Configure SAML Single Sign-On in the Security Fabric

Documentation
Online Help
Video Tutorials
How to Setup FortiClient EMS

OK Cancel

When creating or editing an antivirus profile, there is an option in the *ATP Protection Options* section to *Send files to FortiNDR for inspection*. FortiNDR must be configured and inspecting at least one protocol to enable this option.



New AntiVirus Profile

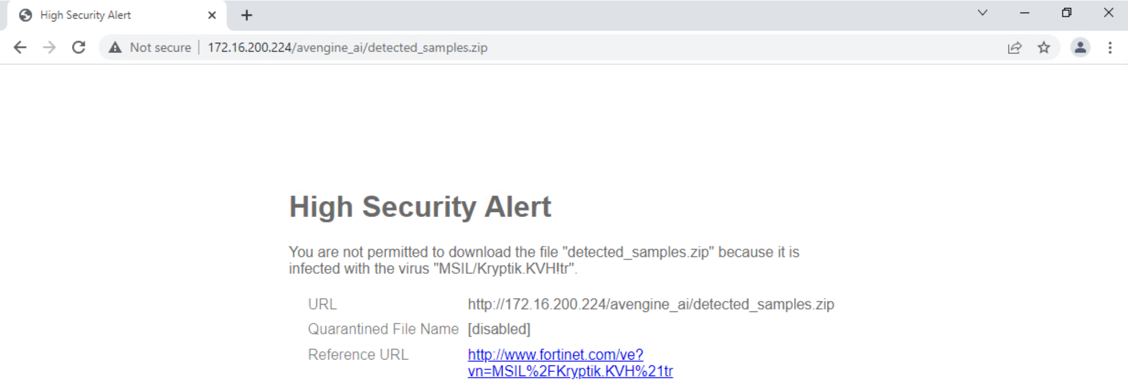
APT Protection Options

- Content Disarm and Reconstruction ○
- Treat Windows executables in email attachments as viruses ○
- Send files to FortiSandbox for inspection ○
- Send files to FortiNDR for inspection ● [✓ Block] Monitor
- Include mobile malware protection ●
- Quarantine ○

Virus Outbreak Prevention

- Use FortiGuard outbreak prevention database ○
- Use external malware block list ○
- Use EMS threat feed ○

The replacement message for blocked files by FortiNDR follows the *Virus Block Page* format (antivirus scan).



High Security Alert

You are not permitted to download the file "detected_samples.zip" because it is infected with the virus "MSIL/Kryptik.KVHltr".

URL	http://172.16.200.224/avengine_ai/detected_samples.zip
Quarantined File Name	[disabled]
Reference URL	http://www.fortinet.com/ve?vn=MSIL%2FKryptik.KVH%21tr

Summary of CLI changes

To enable FortiNDR:

```
config system fortindr
    set status {enable | disable}
end
```

To configure FortiNDR settings in an antivirus profile:

```
config antivirus profile
    edit <name>
        set feature-set proxy
        config {http | ftp | imap | pop3 | smtp | mapi | nntp | cifs | ssh}
            set fortindr {disable | block | monitor}
        end
        set fortindr-error-action {ignore | log-only | block}
        set fortindr-timeout-action {ignore | log-only | block}
    next
end
```

Summary of log changes

The `eventtype`, `msg`, `dtype`, `faiaction`, `faiseverity`, `faiconfidence`, `faifileid`, and `faifiletype` fields have been updated to reference FortiNDR.

Sample log

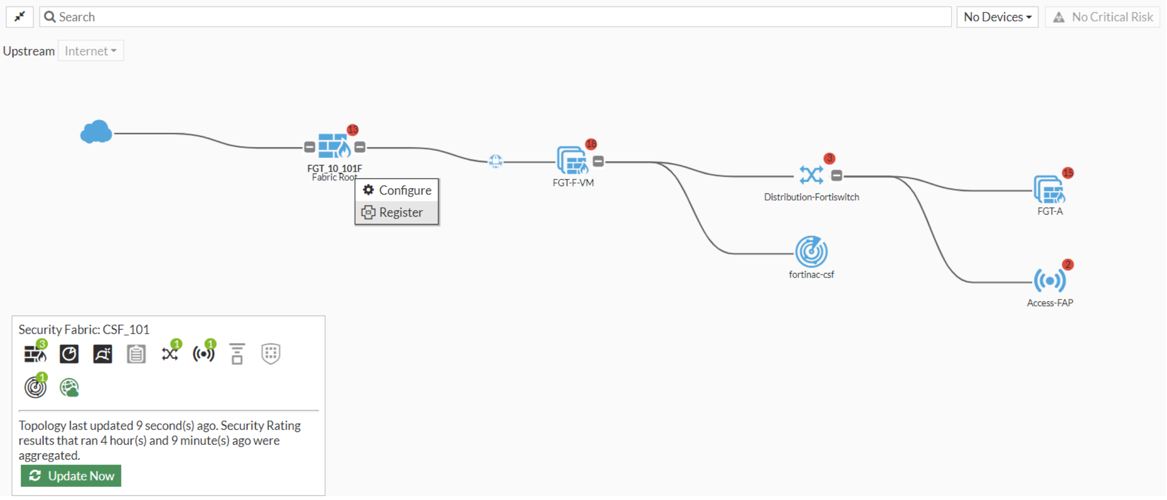
```
1: date=2022-03-14 time=11:22:43 eventtime=1647282163586828798 tz="-0700" logid="0209008220"
type="utm" subtype="virus" eventtype="fortindr" level="warning" vd="vdom1" policyid=1
poluuid="d2dc90d4-a011-51ec-2248-f6a8174bc745" policytype="policy" msg="Blocked by
FortiNDR." action="blocked" service="HTTP" sessionid=115020 srcip=10.1.100.221
dstip=172.16.200.224 srcport=57396 dstport=80 srccountry="Reserved" dstcountry="Reserved"
srcintf="port2" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined"
srcuuid="9a84ed44-a011-51ec-2550-75ae29f786ce" dstuuid="9a84ed44-a011-51ec-2550-
75ae29f786ce" proto=6 direction="incoming" filename="detected_samples.zip"
quarskip="Quarantine-disabled" virus="MSIL/Kryptik.KVH!tr" viruscat="Trojan"
dtype="fortindr" ref="http://www.fortinet.com/ve?vn=MSIL%2FKryptik.KVH%21tr" virusid=0
url="http://172.16.200.224/avengine_ai/detected_samples.zip" profile="av"
agent="curl/7.68.0" httpmethod="GET" analyticssubmit="false" fndraction="deny"
fndrseverity="high" fndrconfidence="high" fndrfileid=155804 fndrfiletype="ZIP" crscore=50
craction=2 crlevel="critical"
```

Register all HA members to FortiCare from the primary unit

Primary and secondary HA members can be registered to FortiCare at the same time from the primary unit. The secondary unit will register through the HA proxy.

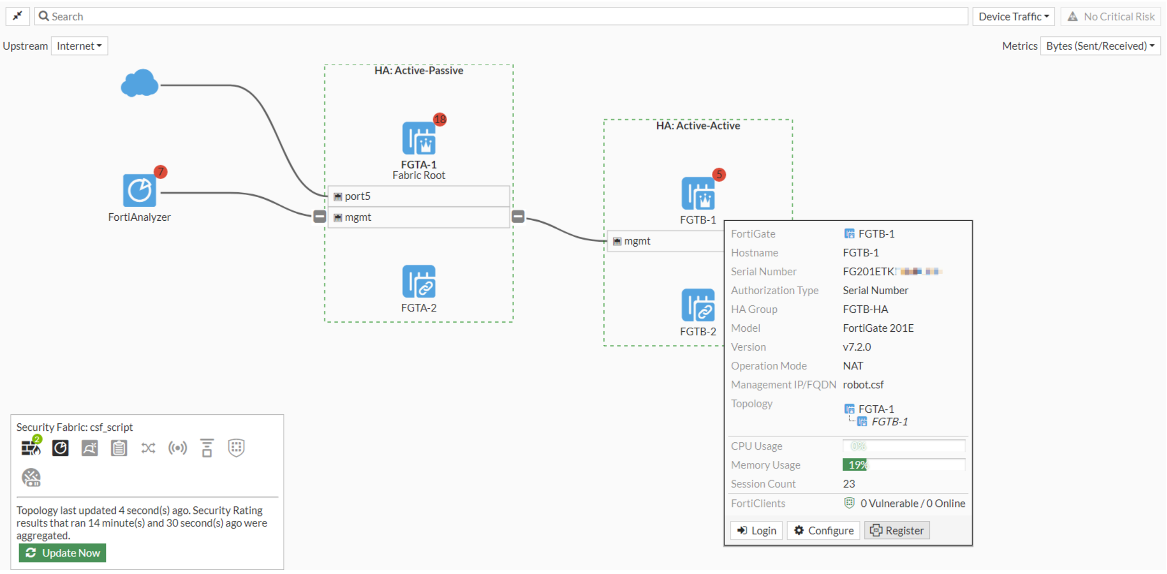
A new FortiCare *Register* button is displayed in various Fabric related pages and widgets. There are two methods to access the *Register* button:

- Right-click on a device in a topology.
  Security Fabric > Physical Topology page:



Topology last updated 9 second(s) ago. Security Rating results that ran 4 hour(s) and 9 minute(s) ago were aggregated.

- Hover over a device to display the tooltip.
  Security Fabric > Logical Topology page:



FortiGate	FGTB-1
Hostname	FGTB-1
Serial Number	FG201ETK[redacted]
Authorization Type	Serial Number
HA Group	FGTB-HA
Model	FortiGate 201E
Version	v7.2.0
Operation Mode	NAT
Management IP/FQDN	robot.csf
Topology	FGTA-1 *FGTB-1*
CPU Usage	0%
Memory Usage	19%
Session Count	23
FortiClients	0 Vulnerable / 0 Online

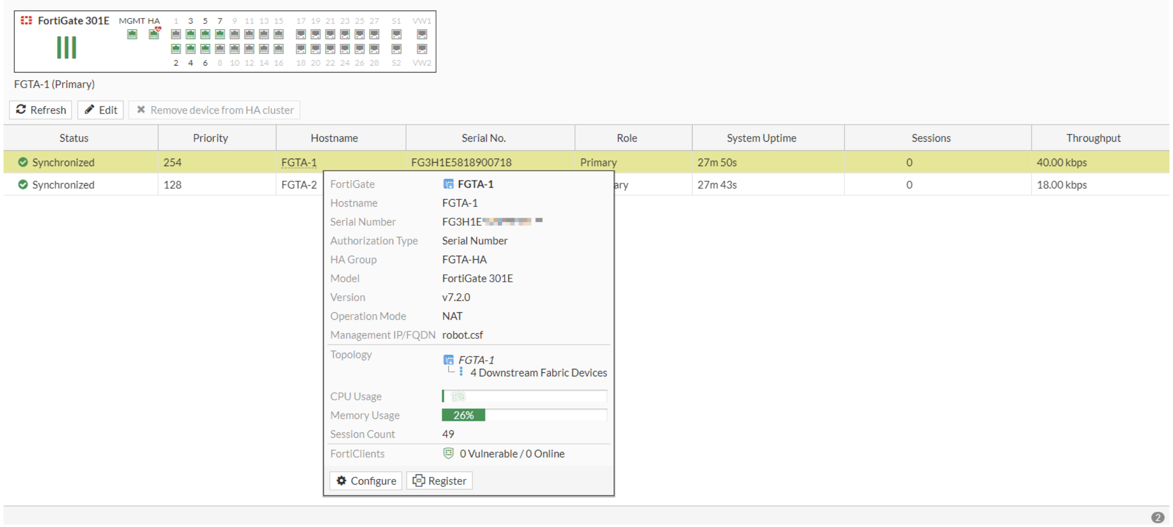
Login | Configure | Register

Security Fabric: csf_script

Topology last updated 4 second(s) ago. Security Rating results that ran 14 minute(s) and 30 second(s) ago were aggregated.

Update Now

System > *HA* page:


FortiGate 301E
MGMT HA
1 3 5 7 9 11 13 15 17 19 21 23 25 27 S1 VW1
2 4 6 8 10 12 14 16 18 20 22 24 26 28 S2 VW2
Refresh
Edit
Remove device from HA cluster

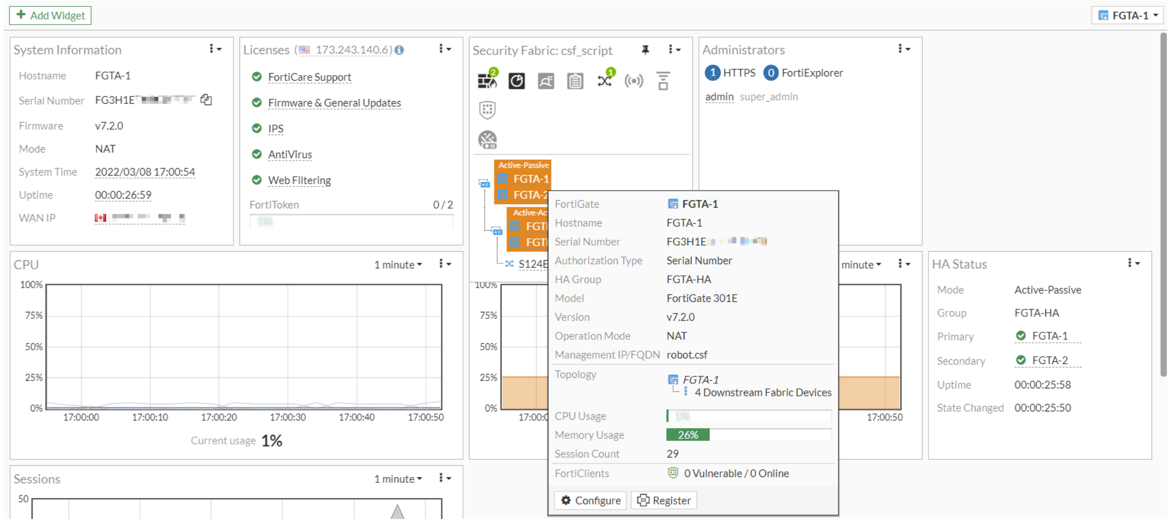
FGTA-1 (Primary)

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	254	FGTA-1	FG3H1E5818900718	Primary	27m 50s	0	40.00 kbps
Synchronized	128	FGTA-2		ary	27m 43s	0	18.00 kbps

FortiGate	FGTA-1
Hostname	FGTA-1
Serial Number	FG3H1E[redacted]
Authorization Type	Serial Number
HA Group	FGTA-HA
Model	FortiGate 301E
Version	v7.2.0
Operation Mode	NAT
Management IP/FQDN	robot.csf
Topology	*FGTA-1* 4 Downstream Fabric Devices
CPU Usage	1%
Memory Usage	26%
Session Count	49
FortiClients	0 Vulnerable / 0 Online

Configure | Register

Security Fabric widget on the *Dashboard* > *Status* page:



System Information	
Hostname	FGTA-1
Serial Number	FG3H1E[redacted]
Firmware	v7.2.0
Mode	NAT
System Time	2022/03/08 17:00:54
Uptime	00:00:26:59
WAN IP	[redacted]

Licenses ([redacted] 173.243.140.6): FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering, FortiToken 0 / 2

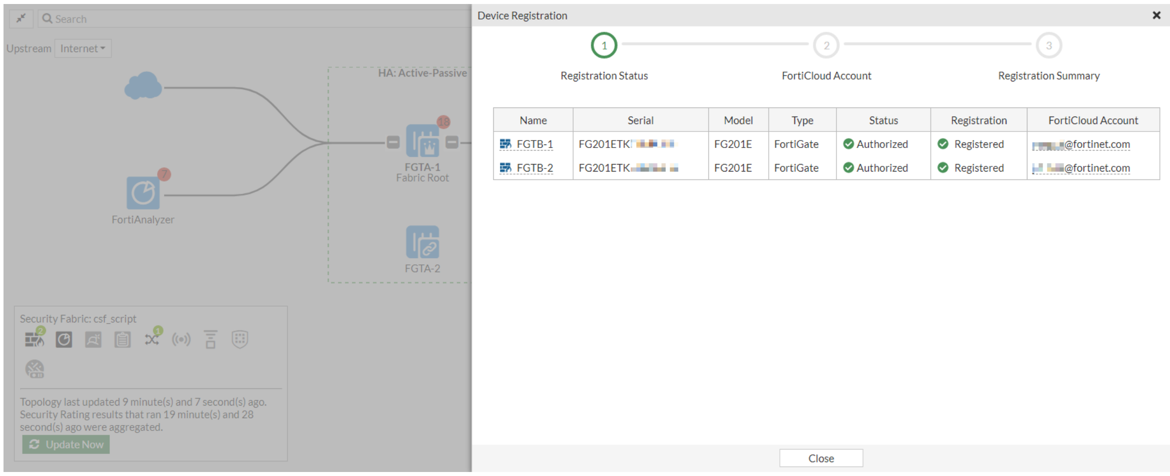
Administrators: 1 HTTPS, 0 FortiExplorer; admin super_admin

FortiGate	FGTA-1
Hostname	FGTA-1
Serial Number	FG3H1E[redacted]
Authorization Type	Serial Number
HA Group	FGTA-HA
Model	FortiGate 301E
Version	v7.2.0
Operation Mode	NAT
Management IP/FQDN	robot.csf
Topology	FGTA-1 4 Downstream Fabric Devices
CPU Usage	1%
Memory Usage	26%
Session Count	29
FortiClients	0 Vulnerable / 0 Online

HA Status	
Mode	Active-Passive
Group	FGTA-HA
Primary	FGTA-1
Secondary	FGTA-2
Uptime	00:00:25:58
State Changed	00:00:25:50

The FortiCare *Register* button is available for FortiGates, manged FortiSwitches, and managed FortiAPs.

Clicking *Register* opens the *Device Registration* pane. If a device is already registered, the pane still opens and displays the device information.



Device Registration

Name	Serial	Model	Type	Status	Registration	FortiCloud Account
FGTB-1	FG201ETK[redacted]	FG201E	FortiGate	Authorized	Registered	[redacted]@fortinet.com
FGTB-2	FG201ETK[redacted]	FG201E	FortiGate	Authorized	Registered	[redacted]@fortinet.com

Topology last updated 9 minute(s) and 7 second(s) ago. Security Rating results that ran 19 minute(s) and 28 second(s) ago were aggregated.

Example

In this example, a HA member is registered from the *Physical Topology* page.

To register a HA member to FortiCare:

1. On the primary unit, go to *Security Fabric > Physical Topology*.
2. Hover over the HA member and click *Register*. The *Device Registration* pane opens.
3. Select the device and click *Register*.

4. Enter the required FortiCloud account information (password, country or region, reseller) and click *Submit*.
5. Once the registration is complete, click *Close*.

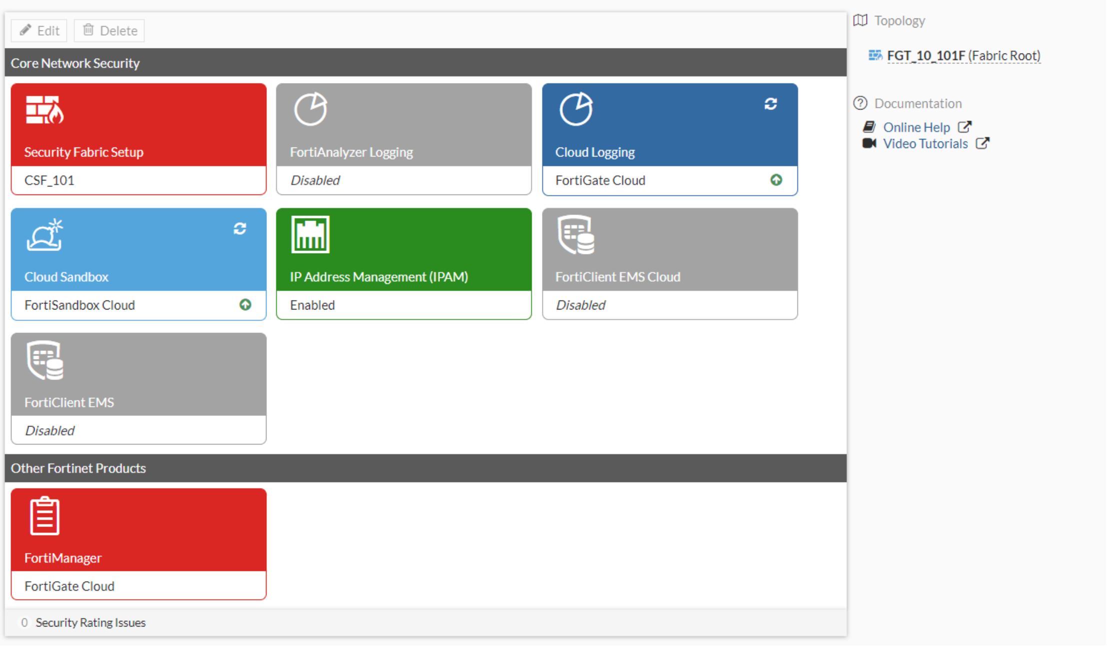
Remove support for Security Fabric loose pairing

Security Fabric loose pairing support is removed for FortiADC, FortiDDoS, and FortiWLC.

Devices that support tight pairing and loose pairing, such as FortiMail and FortiWeb, must be reconfigured to use tight pairing after upgrading. For other Fabric devices, such as FortiADC, FortiDDoS, and FortiWLC, the Security Fabric support must be configured on the device to pair with the FortiGate so they can join the Security Fabric after upgrading FortiOS.

In the GUI:

- The *Create New* button is removed from the *Security Fabric > Fabric Connectors* page.



- Loose pairing devices are not visible in topology pages or the *Topology* tree.

In the CLI:

- The `diagnose sys csf fabric-device` command is removed.
- The `config fabric-device` setting under `config system csf` is removed.

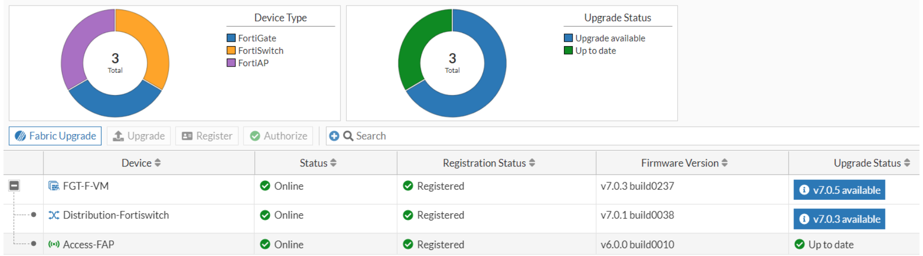
Allow FortiSwitch and FortiAP upgrade when the Security Fabric is disabled

When the Security Fabric is disabled for a FortiGate with managed devices, such as managed FortiSwitch and FortiAP devices, the *System > Fabric Management > Fabric Upgrade* GUI option remains visible to help you manage all devices. Administrators can use the *System > Fabric Management* pane to start a federated upgrade on a non-Security Fabric FortiGate with managed devices.

In this example, a FortiGate manages a FortiSwitch and a FortiAP, and the Security Fabric is disabled.

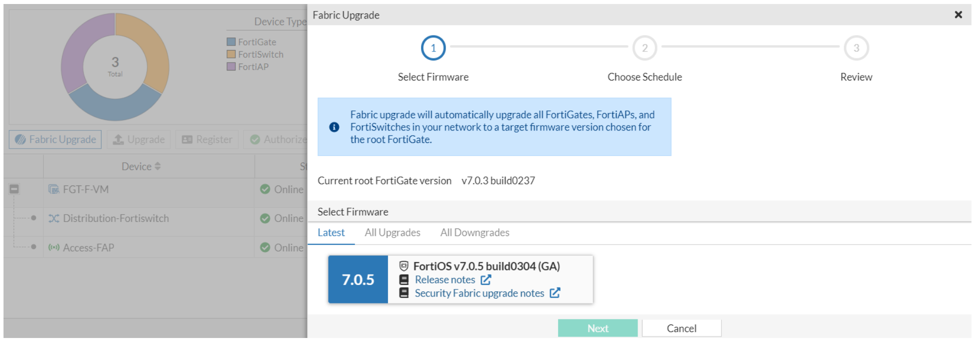
To start a federated upgrade for a non-Security Fabric in the GUI:

1. Go to *System* > *Fabric Management*. In this example, version *7.0.5* is available for the *FGT-F-VM* device.



Device	Status	Registration Status	Firmware Version	Upgrade Status
FGT-F-VM	Online	Registered	v7.0.3 build0237	v7.0.5 available
Distribution-Fortiswitch	Online	Registered	v7.0.1 build0038	v7.0.3 available
Access-FAP	Online	Registered	v6.0.0 build0010	Up to date

2. Click *Fabric Upgrade*. The *Fabric Upgrade* pane opens at the *Select Firmware* step, and the *Latest* tab is selected. In this example, version *7.0.5* is displayed on the *Latest* tab.

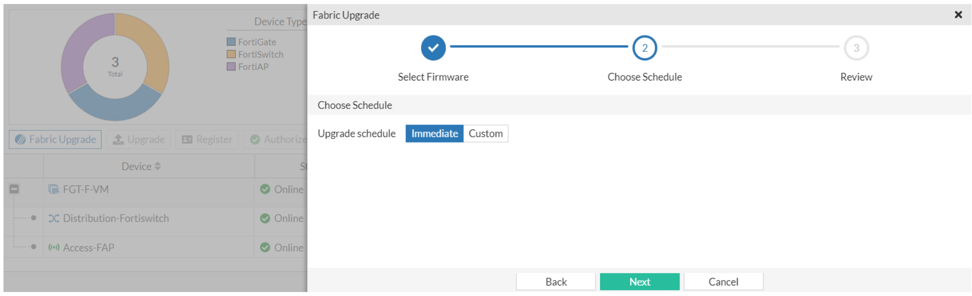


Fabric upgrade will automatically upgrade all FortiGates, FortiAPs, and FortiSwitches in your network to a target firmware version chosen for the root FortiGate.

Current root FortiGate version v7.0.3 build0237

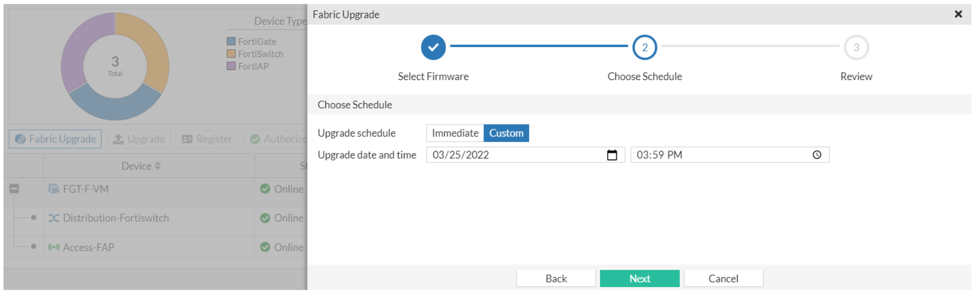
FortiOS v7.0.5 build0304 (GA)

3. On the *Latest* tab, select the version, and click *Next*. The wizard proceeds to the *Choose Schedule* step.
4. Choose to upgrade immediately, or create a custom upgrade schedule, and click *Next*:
   - Click *Immediate* to upgrade immediately.



Upgrade schedule: Immediate

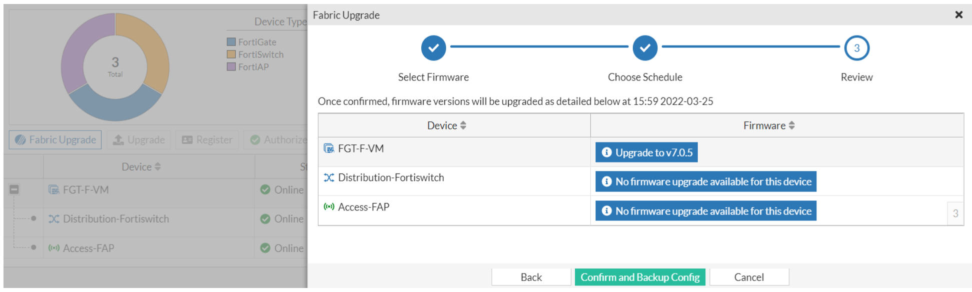
   - Click *Custom* to specify a date and time for the upgrade.



Upgrade schedule: Custom

Upgrade date and time: 03/25/2022 03:59 PM

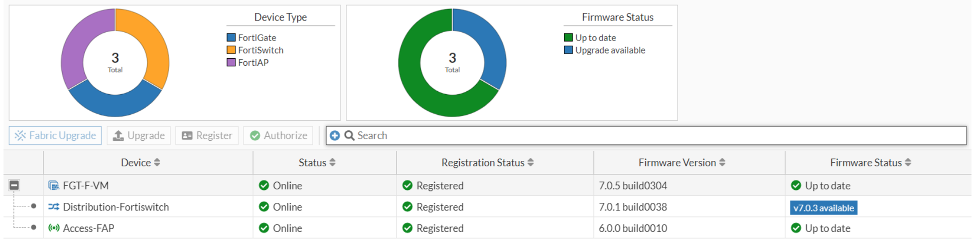
The wizard proceeds to the *Review* step.



Once confirmed, firmware versions will be upgraded as detailed below at 15:59 2022-03-25

Device	Firmware
FGT-F-VM	Upgrade to v7.0.5
Distribution-Fortiswitch	No firmware upgrade available for this device
Access-FAP	No firmware upgrade available for this device

5. Review the firmware versions, and click *Confirm and Backup Config*. The configuration is backed up, and the upgrade proceeds.
   After the upgrade completes, the *Firmware Version* displays *7.0.5 build0304*, and the *Firmware Status* displays *Up to date* for the *FGT-F-VM*.



Device	Status	Registration Status	Firmware Version	Firmware Status
FGT-F-VM	Online	Registered	7.0.5 build0304	Up to date
Distribution-Fortiswitch	Online	Registered	7.0.1 build0038	v7.0.3 available
Access-FAP	Online	Registered	6.0.0 build0010	Up to date

To start a federated upgrade for a non-Security Fabric in the CLI:

```
config system federated-upgrade
    set status ready
    set upgrade-id 2
    config node-list
        edit "FGVM<serial number>"
            set timing scheduled
            set time 22:59 2022/03/25 UTC
            set setup-time 21:30 2022/03/25 UTC
            set upgrade-path 7-0-5
        next
    end
end
```

Add support for multitenant FortiClient EMS deployments - 7.2.1

When FortiClient EMS multitenancy is configured, a FortiClient EMS site is no longer unique using its serial number alone. The FortiGate configuration for FortiClient EMS connectors and related diagnostic commands have been enhanced to distinguish EMS sites using their serial number and tenant ID.

This feature includes the following enhancements:

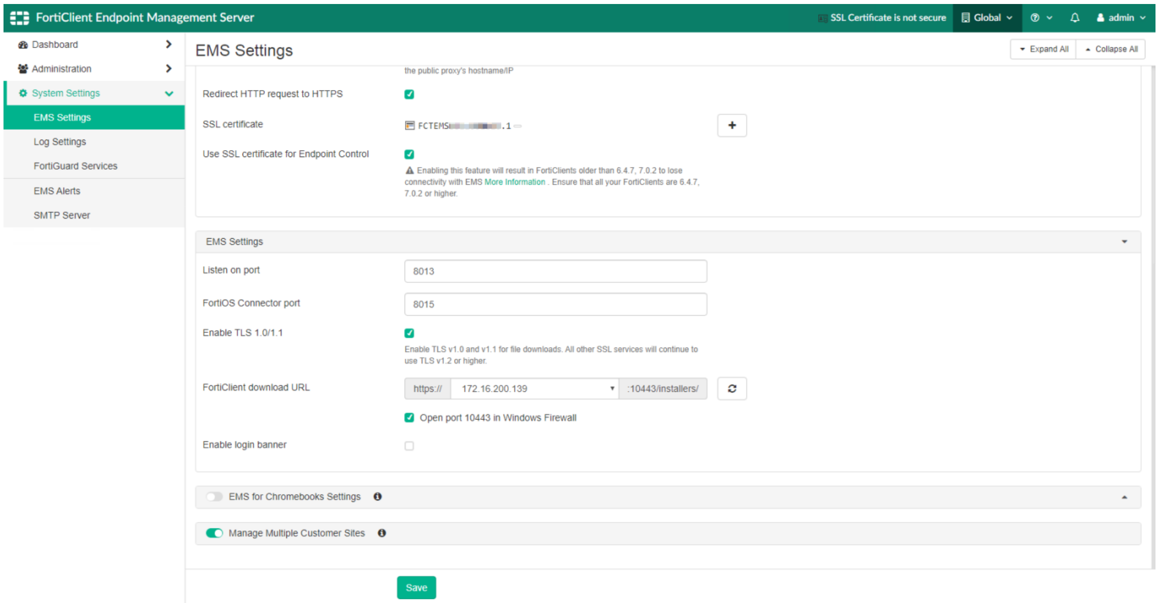
- Update `config endpoint-control fctems` to predefine five FortiClient EMS Fabric connectors that are referred to using numerical IDs from 1 to 5. Administrators can configure the `status` and `name` settings, and to display the tenant ID retrieved from FortiClient EMS sites with *Manage Multiple Customer Sites* enabled.

  ```
  config endpoint-control fctems
      edit {1 | 2 | 3 | 4 | 5}
  ```

```
        set status {enable | disable}
        set name <string>
        set server <string>
        set serial-number <string>
    next
end
```

A single tenant EMS server or the default site on a multitenant EMS server has a tenant ID consisting of all zeros (00000000000000000000000000000000).

For more details about Enabling and configuring multitenancy, refer to the FortiClient EMS Administration Guide. The *Manage Multiple Customer Sites* setting is enabled on the *System Settings* > *EMS Settings* page in FortiClient EMS.



EMS Settings

the public proxy's hostname/IP

Redirect HTTP request to HTTPS ☑

SSL certificate FCTEMS[redacted].1

Use SSL certificate for Endpoint Control ☑

Enabling this feature will result in FortiClients older than 6.4.7, 7.0.2 to lose connectivity with EMS More Information . Ensure that all your FortiClients are 6.4.7, 7.0.2 or higher.

EMS Settings

Listen on port 8013

FortiOS Connector port 8015

Enable TLS 1.0/1.1 ☑

Enable TLS v1.0 and v1.1 for file downloads. All other SSL services will continue to use TLS v1.2 or higher.

FortiClient download URL https:// 172.16.200.139 :10443/installers/

☑ Open port 10443 in Windows Firewall

Enable login banner ☐

EMS for Chromebooks Settings

Manage Multiple Customer Sites

- Update the FortiClient EMS Fabric connector to retrieve specific ZTNA tags from each configured FortiClient EMS site.
- Update `diagnose endpoint record list` to return the `EMS tenant id` field retrieved from each respective FortiClient EMS server.
- Update ZTNA and EMS debug commands to accept the EMS serial number and tenant ID as parameters.

```
# diagnose endpoint lls-comm send ztna find-uid <uid> <EMS_serial_number> <EMS_tenant_id>
```

```
# diagnose wad dev query-by uid <uid> <EMS_serial_number> <EMS_tenant_id>
```

To configure a FortiClient EMS Fabric connector:

```
config endpoint-control fctems
    edit 1
        set status enable
        set name "ems1"
        set server "ems1.test.com"
        set serial-number "FCTEMS0000000001"
        set tenant-id "00000000000000000000000000000000"
    next
end
```

To view FortiClient EMS Fabric connector configuration, including tenant ID:

```
# show endpoint-control fctems
config endpoint-control fctems
    edit 1
        set status enable
        set name "ems1"
        set server "ems1.test.com"
        set serial-number "FCTEMS0000000001"
        set tenant-id "00000000000000000000000000000000"
    next
    edit 2
    next
    edit 3
    next
    edit 4
    next
    edit 5
    next
end
```

To verify the endpoint record list:

```
# diagnose endpoint record list
Record #1:
                IP Address = 21.21.21.198
                MAC Address = 00:0c:29:59:79:08
                MAC list =
                VDOM = root (0)
                EMS serial number: FCTEMS0000000001
                EMS tenant id: 00000000000000000000000000000000
                Client cert SN: 19C72E7FC417E438AB2ED219FF435718FE164E88
                Public IP address: 172.18.62.10
                ...
```

To check the endpoint information from WAD:

```
# diagnose wad dev query-by uid 2E90E8F7ABAD4D1F8B615AD58A0982C9 FCTEMS0000000001
00000000000000000000000000000000
Attr of type=0, length=83, value(ascii)=2E90E8F7ABAD4D1F8B615AD58A0982C9
Attr of type=4, length=0, value(ascii)=
Attr of type=6, length=1, value(ascii)=true
Attr of type=5, length=40, value(ascii)=19C72E7FC417E438AB2ED219FF435718FE164E88
Attr of type=3, length=32, value(ascii)=EMS5_ZTNA_all_registered_clients
Attr of type=3, length=37, value(ascii)=EMS5_ZTNA_ems1_management_tag
Response termination due to no more data
```

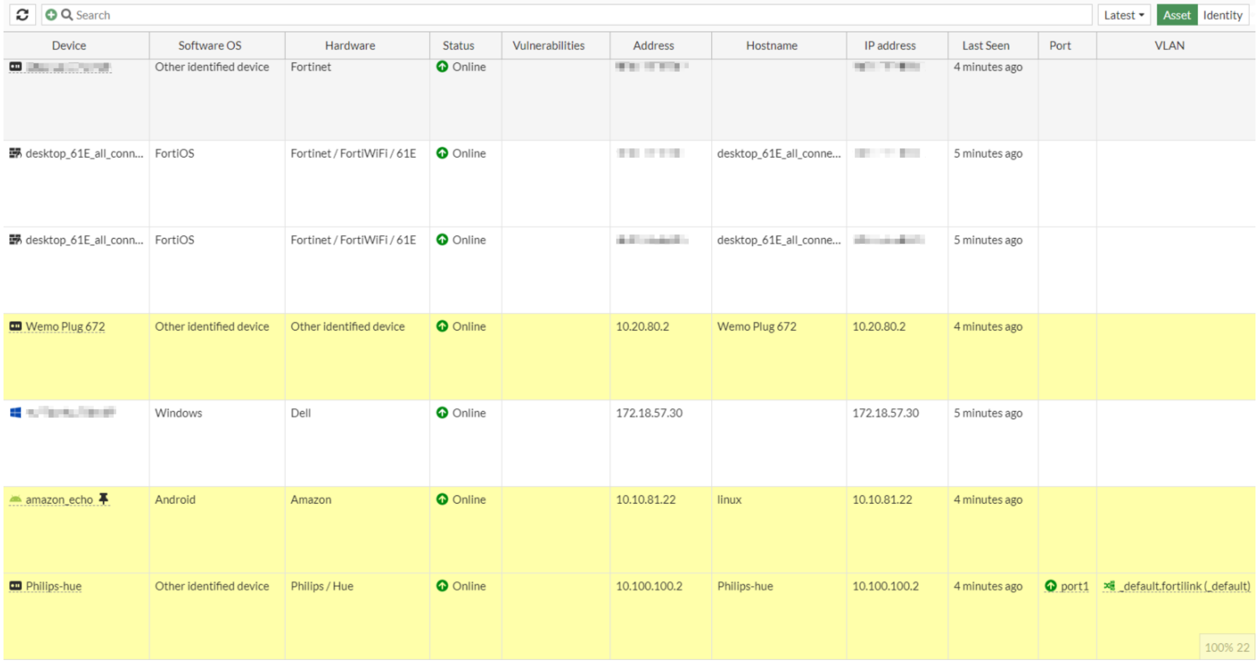
To check the endpoint information:

```
# diagnose endpoint lls-comm connect
Successfully connected.
# diagnose endpoint lls-comm send general register 8
# diagnose endpoint lls-comm send ztna find-uid 2E90E8F7ABAD4D1F8B615AD58A0982C9
FCTEMS0000000001 00000000000000000000000000000000
# diagnose endpoint lls-comm recv
```

```
Channel: ZTNA(3), Size: 617, Command: Update Device(82)

 - UID: 2E90E8F7ABAD4D1F8B615AD58A0982C9
 - EMS Fabric ID: FCTEMS0000000001 :00000000000000000000000000000000
 - Domain: ad864r2.com
 - User: Administrator
 - Owner:
 - Certificate SN: 19C72E7FC417E438AB2ED219FF435718FE164E88
 - online: true
 - Routes (1):
  -- Route #0: IP=21.21.21.198, vfid=0
 - FWAddrNames (2):
  -- Name (#0): EMS5_ZTNA_all_registered_clients
  -- Name (#1): EMS5_ZTNA_ems1_management_tag

received 1 messages.
```

Add IoT devices to Asset Identity Center page - 7.2.1

IoT device information is added to the *Security Fabric > Asset Identity Center* page, including the device name, software OS, hardware vendor, status, IP address, hostname, time last seen, port, VLAN, and so on.



Device	Software OS	Hardware	Status	Vulnerabilities	Address	Hostname	IP address	Last Seen	Port	VLAN
[redacted]	Other identified device	Fortinet	Online		[redacted]		[redacted]	4 minutes ago		
desktop_61E_all_conn...	FortiOS	Fortinet / FortiWiFi / 61E	Online		[redacted]	desktop_61E_all_conne...	[redacted]	5 minutes ago		
desktop_61E_all_conn...	FortiOS	Fortinet / FortiWiFi / 61E	Online		[redacted]	desktop_61E_all_conne...	[redacted]	5 minutes ago		
Wemo Plug 672	Other identified device	Other identified device	Online		10.20.80.2	Wemo Plug 672	10.20.80.2	4 minutes ago		
[redacted]	Windows	Dell	Online		172.18.57.30		172.18.57.30	5 minutes ago		
amazon_echo	Android	Amazon	Online		10.10.81.22	linux	10.10.81.22	4 minutes ago		
Philips-hue	Other identified device	Philips / Hue	Online		10.100.100.2	Philips-hue	10.100.100.2	4 minutes ago	port1	_default.fortilink (_default)

The following are required for IoT devices to be displayed on the *Asset Identity Center* page:

1. The FortiGate must have a valid IoT Detection Service license.
2. Device detection must be configured on a LAN interface used by IoT devices.

To configure device detection in the GUI:

a. Go to *Network > Interfaces* and edit a LAN interface.

b. Enable *Device detection*.

c. Click *OK*.

To configure device detection in the CLI:

```
config system interface
    edit <name>
        set device-identification enable
    next
end
```

3. Configure a firewall policy with an application control sensor.

Introduce distributed topology and security rating reports - 7.2.1

The Security Fabric backend has been improved to allow physical topology, logical topology, and security rating report information to be gathered by distributed means through each downstream FortiGate device. This results in less delays and memory usage on the Fabric root, and less API calls to the downstream devices.

For example, in a Security Fabric configured with 35 downstream devices, the following output shows normal CPU and memory usage.

To verify the system performance on the root FortiGate:

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU2 states: 1% user 0% system 0% nice 99% idle 0% iowait 0% irq 0% softirq
CPU3 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 1911252k total, 722276k used (37.8%), 1089216k free (57.0%), 99760k freeable (5.2%)
Average network usage: 10 / 13 kbps in 1 minute, 411 / 155 kbps in 10 minutes, 143 / 53 kbps
in 30 minutes
Maximal network usage: 55 / 32 kbps in 1 minute, 33156 / 4491 kbps in 10 minutes, 33156 /
4491 kbps in 30 minutes
Average sessions: 40 sessions in 1 minute, 27 sessions in 10 minutes, 22 sessions in 30
minutes
Maximal sessions: 45 sessions in 1 minute, 61 sessions in 10 minutes, 61 sessions in 30
minutes
Average session setup rate: 1 sessions per second in last 1 minute, 0 sessions per second in
last 10 minutes, 0 sessions per second in last 30 minutes
Maximal session setup rate: 5 sessions per second in last 1 minute, 18 sessions per second
in last 10 minutes, 18 sessions per second in last 30 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions
in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions
in last 30 minutes
Average nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
Maximal nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 7 days,  0 hours,  17 minutes
```

Add IoT vulnerabilities to the asset identity list and FortiGuard IoT security rating checks - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

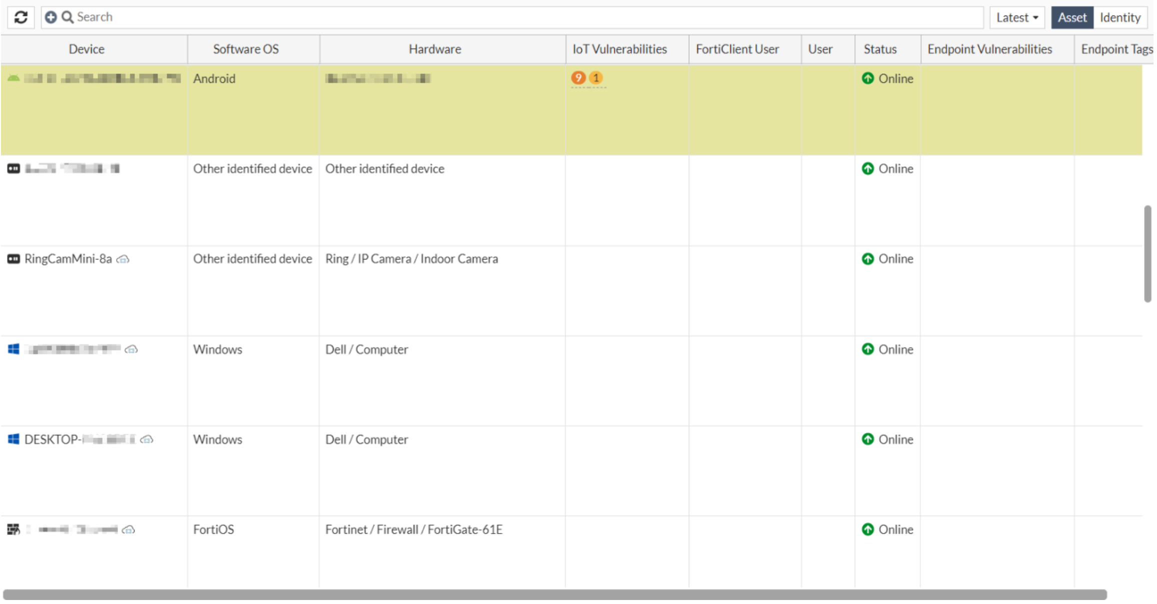
- IoT devices

IoT devices with known vulnerabilities are displayed on the *Security Fabric > Asset Identity Center* page's *Asset* list view. Hovering over the vulnerabilities count displays a *View IoT Vulnerabilities* tooltip, which opens the *View IoT Vulnerabilities* table that includes the *Vulnerability ID*, *Type*, *Severity*, *Reference*, *Description*, and *Patch Signature ID*. Each entry in the *Reference* column includes the CVE number and a link to the CVE details.

To detect IoT vulnerabilities, the FortiGate must have a valid IoT Detection Service license, device detection must be configured on a LAN interface used by IoT devices, and a firewall policy with an application control sensor must be configured. See Add IoT devices to Asset Identity Center page 7.2.1 on page 45 for more details.

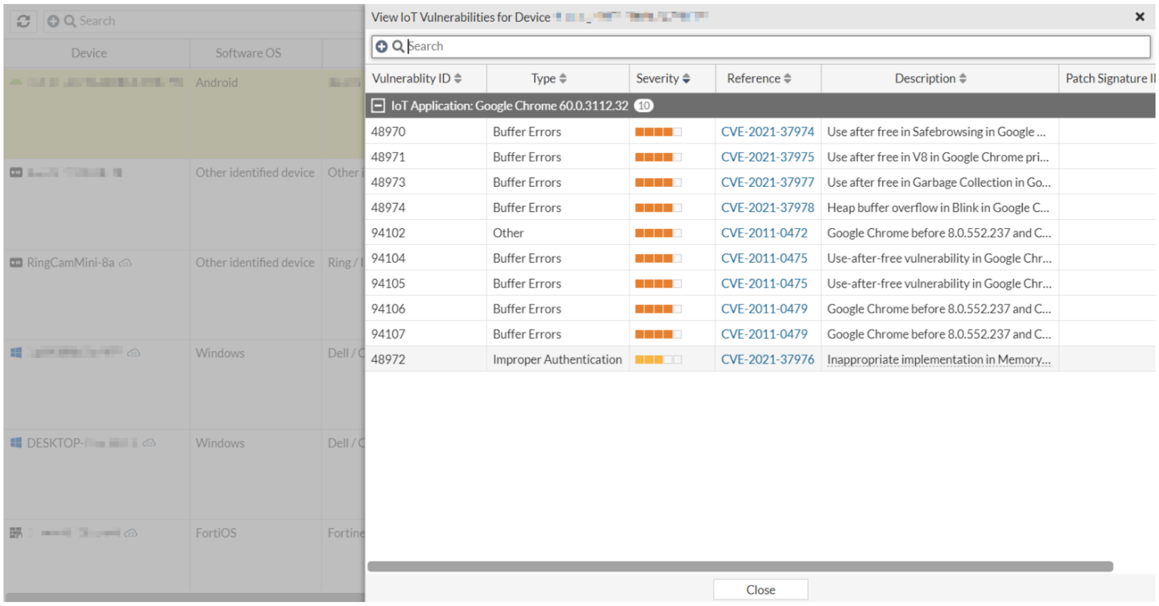
To view IoT asset vulnerabilities in the GUI:

1. Go to *Security Fabric > Asset Identity Center*. Ensure the *Asset* list view is selected.
2. Select a device with IoT vulnerabilities.



Device	Software OS	Hardware	IoT Vulnerabilities	FortiClient User	User	Status	Endpoint Vulnerabilities	Endpoint Tags
[redacted]	Android	[redacted]	9 1			Online		
[redacted]	Other identified device	Other identified device				Online		
RingCamMini-8a	Other identified device	Ring / IP Camera / Indoor Camera				Online		
[redacted]	Windows	Dell / Computer				Online		
DESKTOP-[redacted]	Windows	Dell / Computer				Online		
[redacted]	FortiOS	Fortinet / Firewall / FortiGate-61E				Online		

3. Hover over the *IoT Vulnerabilities* count to view the tooltip and click *View IoT Vulnerabilities*. A table with the list of vulnerabilities and related information for the device is displayed, including the CVE references and descriptions.



Device	Software OS	
[redacted]	Android	[redacted]
[redacted]	Other identified device	Other i
RingCamMini-8a	Other identified device	Ring / I
[redacted]	Windows	Dell / C
DESKTOP-[redacted]	Windows	Dell / C
[redacted]	FortiOS	Fortine

View IoT Vulnerabilities for Device [redacted]

Search

Vulnerablity ID	Type	Severity	Reference	Description	Patch Signature I
IoT Application: Google Chrome 60.0.3112.32 10					
48970	Buffer Errors	■■■■□	CVE-2021-37974	Use after free in Safebrowsing in Google ...	
48971	Buffer Errors	■■■■□	CVE-2021-37975	Use after free in V8 in Google Chrome pri...	
48973	Buffer Errors	■■■■□	CVE-2021-37977	Use after free in Garbage Collection in Go...	
48974	Buffer Errors	■■■■□	CVE-2021-37978	Heap buffer overflow in Blink in Google C...	
94102	Other	■■■■□	CVE-2011-0472	Google Chrome before 8.0.552.237 and C...	
94104	Buffer Errors	■■■■□	CVE-2011-0475	Use-after-free vulnerability in Google Chr...	
94105	Buffer Errors	■■■■□	CVE-2011-0475	Use-after-free vulnerability in Google Chr...	
94106	Buffer Errors	■■■■□	CVE-2011-0479	Google Chrome before 8.0.552.237 and C...	
94107	Buffer Errors	■■■■□	CVE-2011-0479	Google Chrome before 8.0.552.237 and C...	
48972	Improper Authentication	■■■□□	CVE-2021-37976	Inappropriate implementation in Memory...	

4. Click a hyperlink in the *Reference* column to view more information about the CVE, or click *Close*.

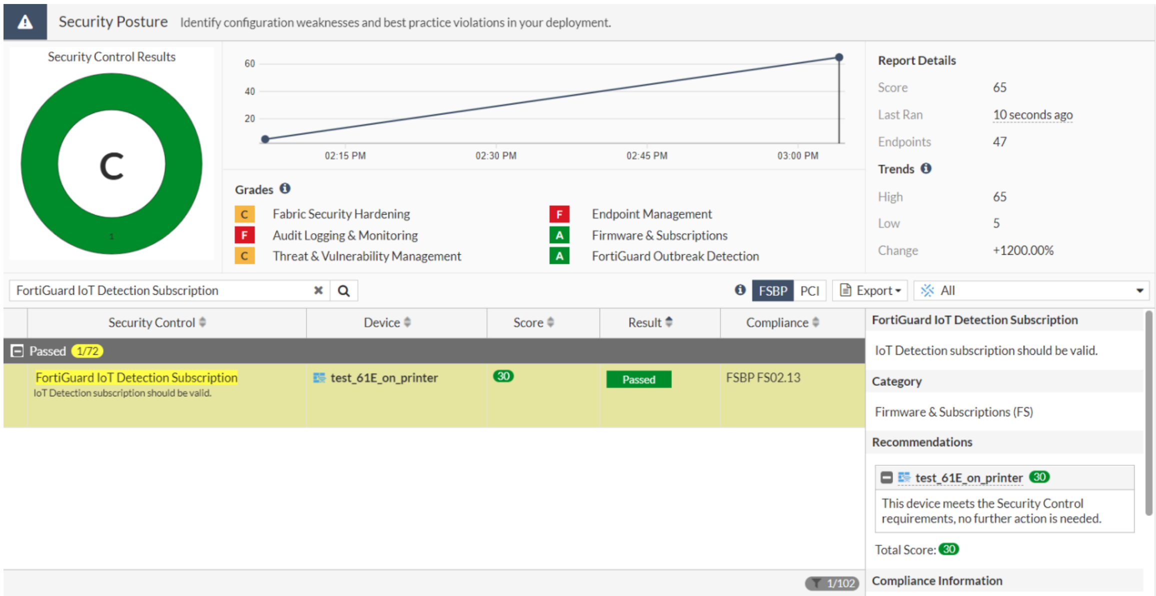
To view IoT asset vulnerabilities in the CLI:

```
# diagnose user-device-store device memory list
...
        device_info
                'ipv4_address' = '10.20.80.10'
                'mac' = '**:**:**:**:**:**'
                ...
                'vdom' = 'root'
                'os_name' = 'Android'
                'hostname' = '*********************'
                'last_seen' = '1670540312'
                'host_src' = 'dhcp'
                'unjoined_forticlient_endpoint' = 'false'
                'is_online' = 'true'
                'active_start_time' = '1670536763'
                ...
                'dhcp_lease_status' = 'leased'
                'dhcp_lease_expire' = '1671141562'
                'dhcp_lease_reserved' = 'false'
                'dhcp_server_id' = '10'
                'is_fortiguard_src' = 'false'
                'purdue_level' = '3'
                'iot_vuln_count' = '10'
...
        iot_info
                'vendor' = 'Google'
                'product' = 'Chrome'
                'version-min' = '60.0.3112.32'
                'validity' = 'true'
        iot_vulnerability
                'vulnerability_id' = '48970'
                'severity' = '3'
                'type' = 'Buffer Errors'
                'description' = 'Use after free in Safebrowsing in Google Chrome prior to 
94.0.4606.71 allowed a remote attacker who had compromised the renderer process to 
potentially exploit heap corruption via a crafted HTML page.'
                'references' = 'CVE-2021-37974'
                'date_added' = '2022-07-27 17:52:34.987194'
                'date_updated' = '2022-07-27 17:52:34.987220'
...
        iot_vulnerability
                'vulnerability_id' = '94107'
                'severity' = '3'
                'type' = 'Buffer Errors'
                'description' = 'Google Chrome before 8.0.552.237 and Chrome OS before 
8.0.552.344 do not properly interact with extensions, which allows remote attackers to cause 
a denial of service via a crafted extension that triggers an uninitialized pointer.'
                'references' = 'CVE-2011-0479'
                'date_added' = '2022-09-20 18:23:54.961465'
                'date_updated' = '2022-09-20 18:23:54.961481'
```

Security rating checks

The *Security Fabric > Security Rating > Security Posture* report includes two rating checks related to IoT vulnerabilities:

- The *FortiGuard IoT Detection Subscription* rating check will pass if the *System > FortiGuard* page shows that the *IoT Detection Service* is licensed. In this example, the result is marked as *Passed* because the license is valid.


Security Posture
Identify configuration weaknesses and best practice violations in your deployment.
Security Control Results
C
60
40
20
02:15 PM
02:30 PM
02:45 PM
03:00 PM
FortiGuard IoT Detection Subscription
FSBP
PCI
Export
All

Grades

C	Fabric Security Hardening	F	Endpoint Management
F	Audit Logging & Monitoring	A	Firmware & Subscriptions
C	Threat & Vulnerability Management	A	FortiGuard Outbreak Detection

Report Details

Score	65
Last Ran	10 seconds ago
Endpoints	47

Trends

High	65
Low	5
Change	+1200.00%

Security Control	Device	Score	Result	Compliance
Passed 1/72				
FortiGuard IoT Detection Subscription IoT Detection subscription should be valid.	test_61E_on_printer	30	Passed	FSBP FS02.13

1/102

FortiGuard IoT Detection Subscription

IoT Detection subscription should be valid.

Category

Firmware & Subscriptions (FS)

Recommendations

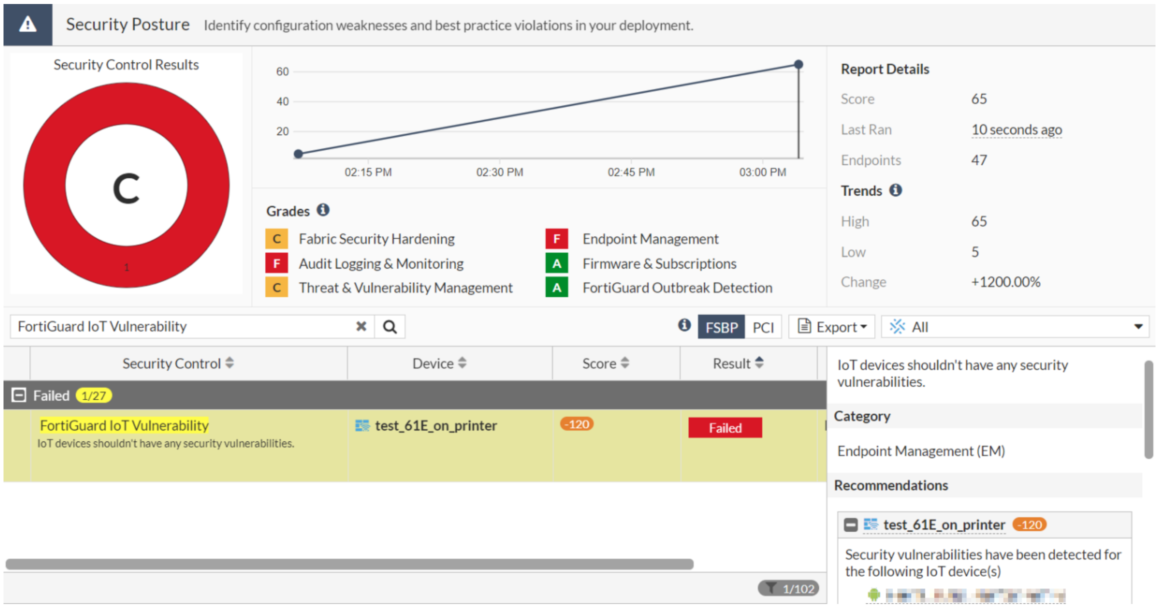
test_61E_on_printer 30

This device meets the Security Control requirements, no further action is needed.

Total Score: 30

Compliance Information

- The *FortiGuard IoT Vulnerability* rating check will fail if any IoT vulnerabilities are found. In this example, the result is marked as *Failed* because there is a device with IoT vulnerabilities.


Security Posture
Identify configuration weaknesses and best practice violations in your deployment.
Security Control Results
C
60
40
20
02:15 PM
02:30 PM
02:45 PM
03:00 PM
Grades
FortiGuard IoT Vulnerability
FSBP
PCI
Export
All
1/102

Report Details

Score	65
Last Ran	10 seconds ago
Endpoints	47

Trends

High	65
Low	5
Change	+1200.00%

Grades

C	Fabric Security Hardening	F	Endpoint Management
F	Audit Logging & Monitoring	A	Firmware & Subscriptions
C	Threat & Vulnerability Management	A	FortiGuard Outbreak Detection

Security Control	Device	Score	Result
Failed 1/27			
FortiGuard IoT Vulnerability IoT devices shouldn't have any security vulnerabilities.	test_61E_on_printer	-120	Failed

IoT devices shouldn't have any security vulnerabilities.

Category

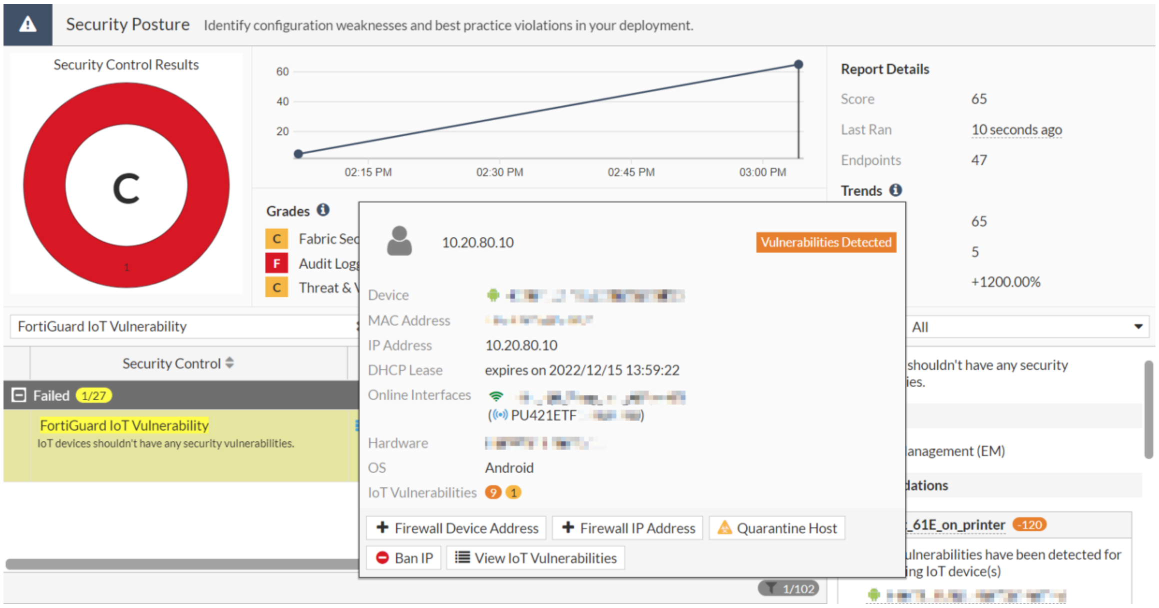
Endpoint Management (EM)

Recommendations

test_61E_on_printer -120

Security vulnerabilities have been detected for the following IoT device(s)

In the *Recommendations* section, hover over the device name to display the tooltip, which includes an option to *View IoT Vulnerabilities*.



10.20.80.10 Vulnerabilities Detected

Device	
MAC Address	
IP Address	10.20.80.10
DHCP Lease	expires on 2022/12/15 13:59:22
Online Interfaces	PU421ETF
Hardware	
OS	Android
IoT Vulnerabilities	9 1

Enhance the Fabric Connectors page - 7.2.4

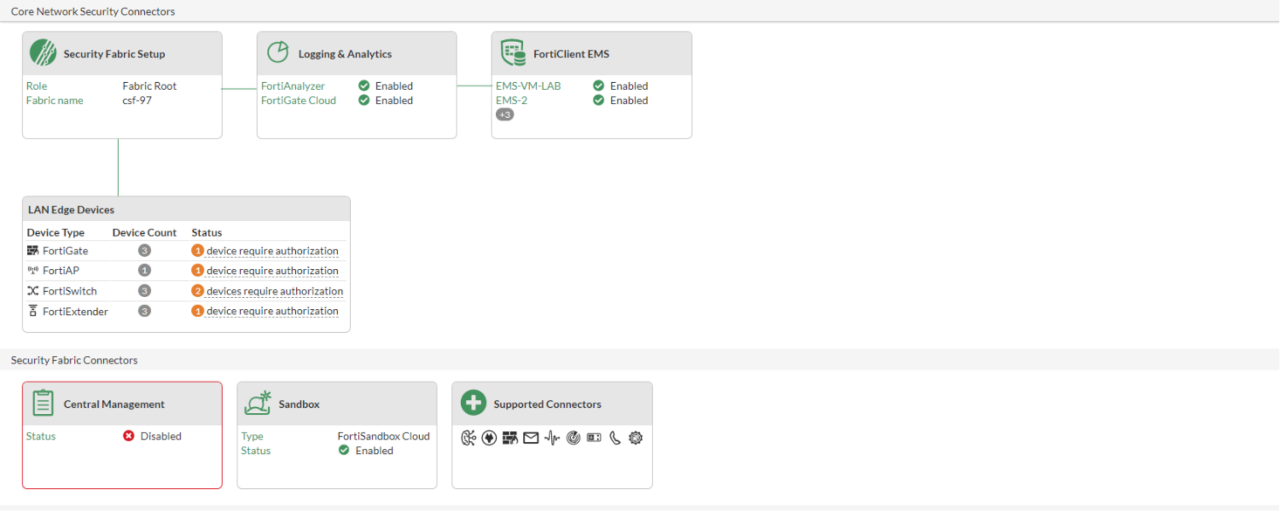
The *Security Fabric > Fabric Connectors* page has been enhanced to show a high-level overview of the Fabric components that are enabled and how they connect to each other. The *System > Fabric Management* page can be used to register and authorize Security Fabric devices instead of using the Security Fabric network topology gutter, which has been removed from the *Security Fabric > Fabric Connectors* page.

The following changes have been made to the *Security Fabric > Fabric Connectors* page:

- Improve the *Security Fabric Setup* configuration settings to select the *Security Fabric role* (standalone, root, or downstream) instead of just enabling the Security Fabric itself.

- Merge relevant connectors into *Core Network Security Connectors* and *Security Fabric Connectors* sections.
    - The *Core Network Security Connectors* section includes the *Security Fabric Setup*, *Logging & Analytics*, *FortiClient EMS*, and *LAN Edge Devices* cards.
    - The *Security Fabric Connectors* section includes the *Central Management*, *Sandbox*, and *Supported Connectors* cards.
- Add the *LAN Edge Devices* card that displays information about the LAN edge devices (FortiGates, FortiAPs, FortiSwitches, and FortiExtenders) including the device type, number of devices, and number of unregistered and unauthorized devices.
- Add the *Supported Connectors* card that displays the icons of different Fortinet devices that support full Security Fabric integration. Clicking the card displays a list of cards with device names that link to documentation to configure these devices in the Security Fabric since they do not have separate connector settings.
- Remove the IPAM connector.

Sample Fabric Connectors page on a root FortiGate:



Core Network Security Connectors

Security Fabric Setup

Role Fabric Root
Fabric name csf-97

Logging & Analytics

FortiAnalyzer ✓ Enabled
FortiGate Cloud ✓ Enabled

FortiClient EMS

EMS-VM-LAB ✓ Enabled
EMS-2 ✓ Enabled
+3

LAN Edge Devices

Device Type	Device Count	Status
FortiGate	3	1 device require authorization
FortiAP	1	1 device require authorization
FortiSwitch	3	2 devices require authorization
FortiExtender	3	1 device require authorization

Security Fabric Connectors

Central Management

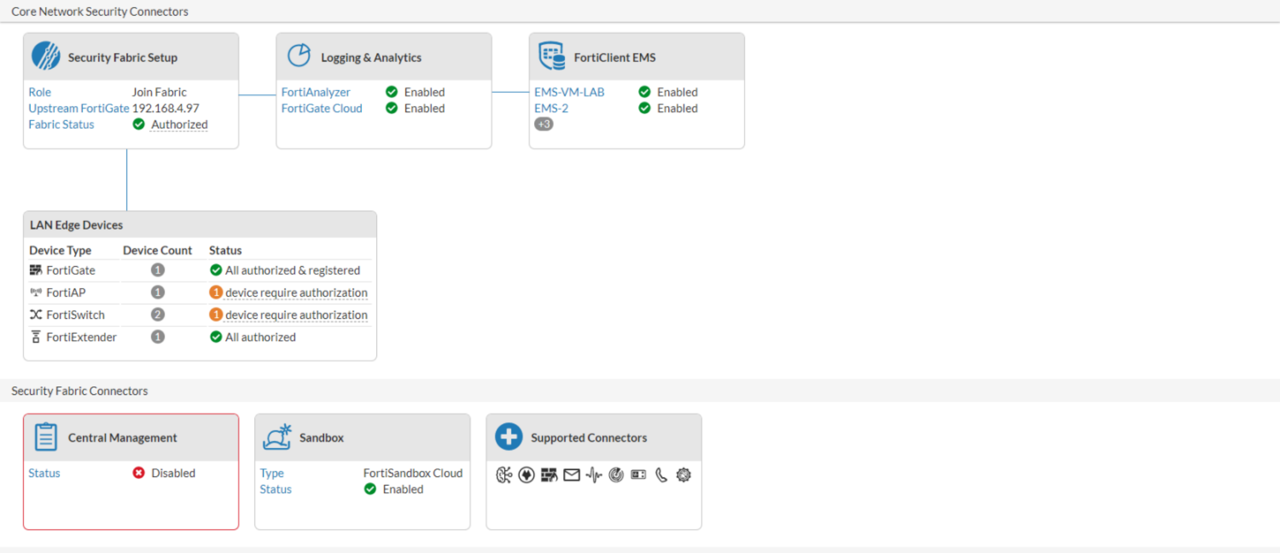
Status ✗ Disabled

Sandbox

Type FortiSandbox Cloud
Status ✓ Enabled

Supported Connectors

Sample Fabric Connectors page on a downstream FortiGate:



Core Network Security Connectors

Security Fabric Setup

Role Join Fabric
Upstream FortiGate 192.168.4.97
Fabric Status ✓ Authorized

Logging & Analytics

FortiAnalyzer ✓ Enabled
FortiGate Cloud ✓ Enabled

FortiClient EMS

EMS-VM-LAB ✓ Enabled
EMS-2 ✓ Enabled
+3

LAN Edge Devices

Device Type	Device Count	Status
FortiGate	1	✓ All authorized & registered
FortiAP	1	1 device require authorization
FortiSwitch	2	1 device require authorization
FortiExtender	1	✓ All authorized

Security Fabric Connectors

Central Management

Status ✗ Disabled

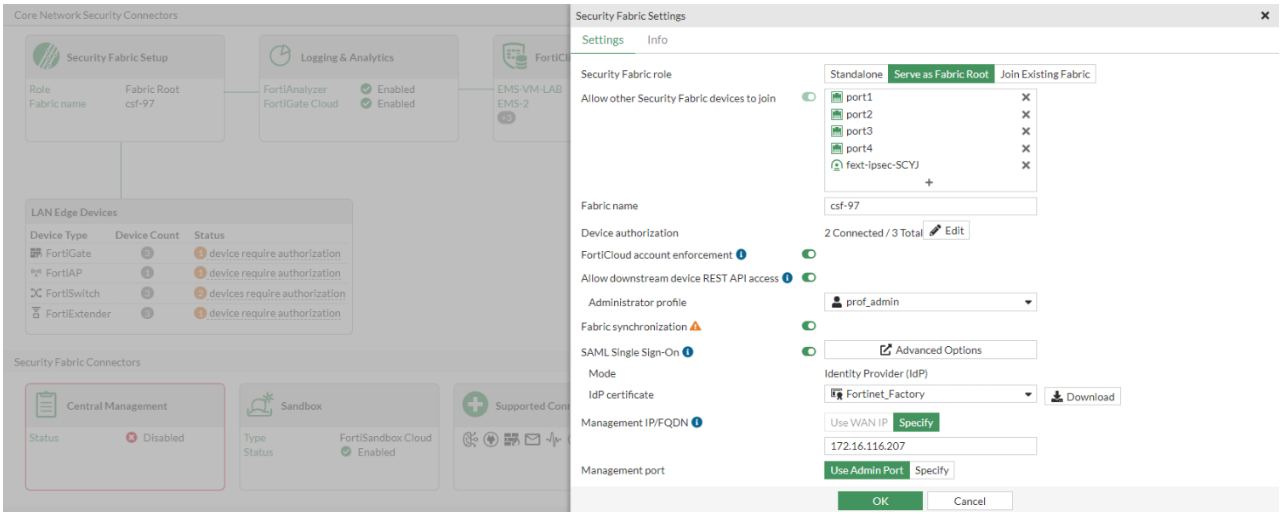
Sandbox

Type FortiSandbox Cloud
Status ✓ Enabled

Supported Connectors

To configure the root FortiGate:

1. Go to *Security Fabric* > *Fabric Connectors* and double-click the *Security Fabric Setup* card.
2. Select the *Settings* tab and set the *Security Fabric role* to *Serve as Fabric Root*.
3. Configure the remaining settings as needed.



Core Network Security Connectors

Security Fabric Setup
Role: Fabric Root
Fabric name: csf-97

Logging & Analytics
FortiAnalyzer: Enabled
FortiGate Cloud: Enabled

FortiCl
EMS-VM-LAB
EMS-2
+3

LAN Edge Devices

Device Type	Device Count	Status
FortiGate	3	1 device require authorization
FortiAP	1	1 device require authorization
FortiSwitch	3	2 devices require authorization
FortiExtender	3	1 device require authorization

Security Fabric Connectors

Central Management
Status: Disabled

Sandbox
Type: FortiSandbox Cloud
Status: Enabled

Supported Con

Security Fabric Settings

Settings | Info

Security Fabric role: Standalone | **Serve as Fabric Root** | Join Existing Fabric
Allow other Security Fabric devices to join: port1, port2, port3, port4, fext-ipsec-SCYJ
Fabric name: csf-97
Device authorization: 2 Connected / 3 Total Edit
FortiCloud account enforcement: enabled
Allow downstream device REST API access: enabled
Administrator profile: prof_admin
Fabric synchronization: enabled
SAML Single Sign-On: enabled Advanced Options
Mode: Identity Provider (IdP)
IdP certificate: Fortinet_Factory Download
Management IP/FQDN: Use WAN IP | **Specify**
172.16.116.207
Management port: **Use Admin Port** | Specify

OK Cancel

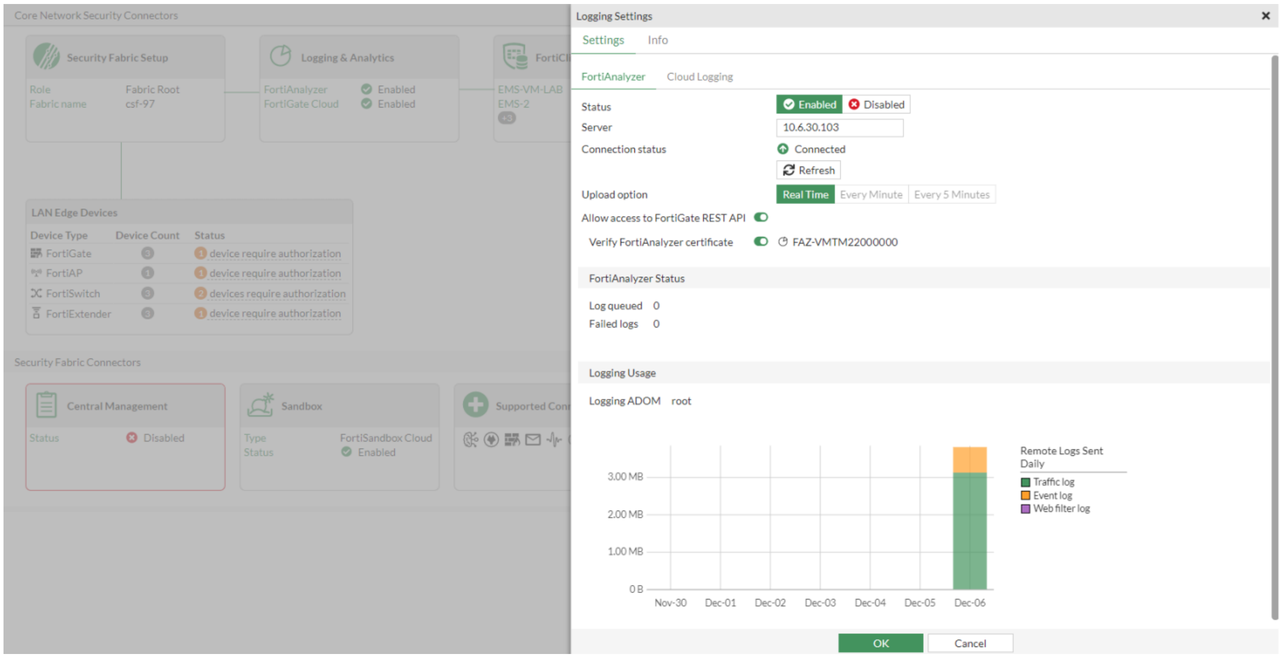
4. Click *OK*.

Logging & Analytics connector

Logging & Analytics is a new card that combines the settings from the previous *FortiAnalyzer Logging* and *Cloud Logging* cards into a single connector to configure the FortiAnalyzer, FortiGate Cloud, and FortiAnalyzer Cloud settings. In this example, FortiAnalyzer and FortiGate Cloud are enabled.

To configure the Logging & Analytics connector:

1. Go to *Security Fabric* > *Fabric Connectors* and double-click the *Logging & Analytics* card.
2. Select the *Settings* tab, select the *FortiAnalyzer* tab, and set the *Status* to *Enabled*.
3. Configure the remaining settings as needed.



Logging Settings

Settings | Info

FortiAnalyzer | Cloud Logging

Status: Enabled | Disabled

Server: 10.6.30.103

Connection status: Connected

Refresh

Upload option: Real Time | Every Minute | Every 5 Minutes

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate: FAZ-VMTM22000000

FortiAnalyzer Status

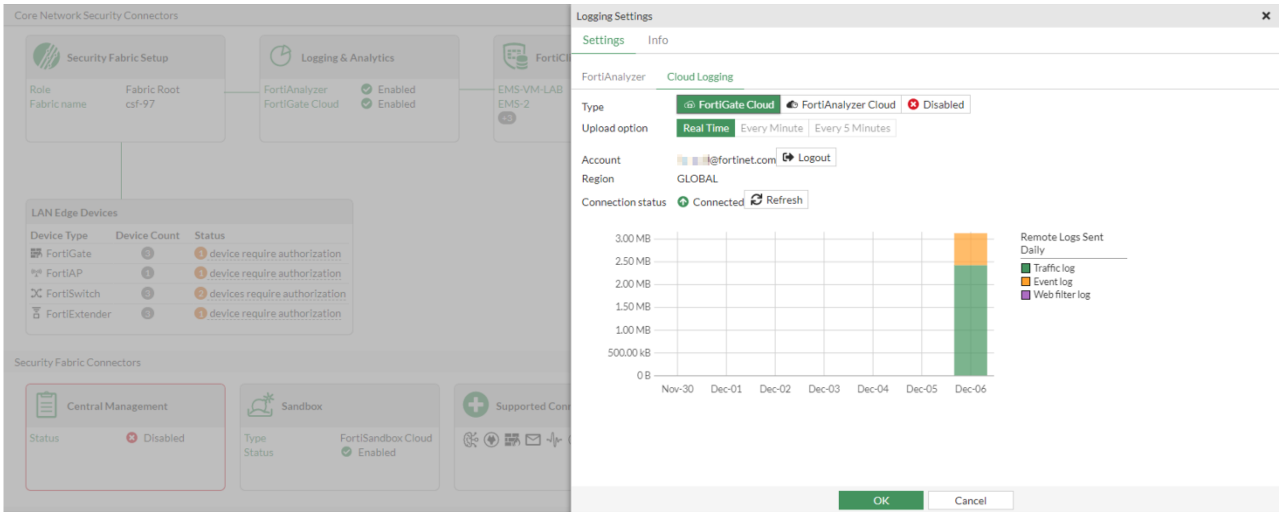
Log queued 0

Failed logs 0

Logging Usage

Logging ADOM root

4. Select the *Cloud Logging* tab, and set the *Type* to *FortiGate Cloud*.



Logging Settings

Settings | Info

FortiAnalyzer | Cloud Logging

Type: FortiGate Cloud | FortiAnalyzer Cloud | Disabled

Upload option: Real Time | Every Minute | Every 5 Minutes

Account: [redacted]@fortinet.com Logout

Region: GLOBAL

Connection status: Connected Refresh

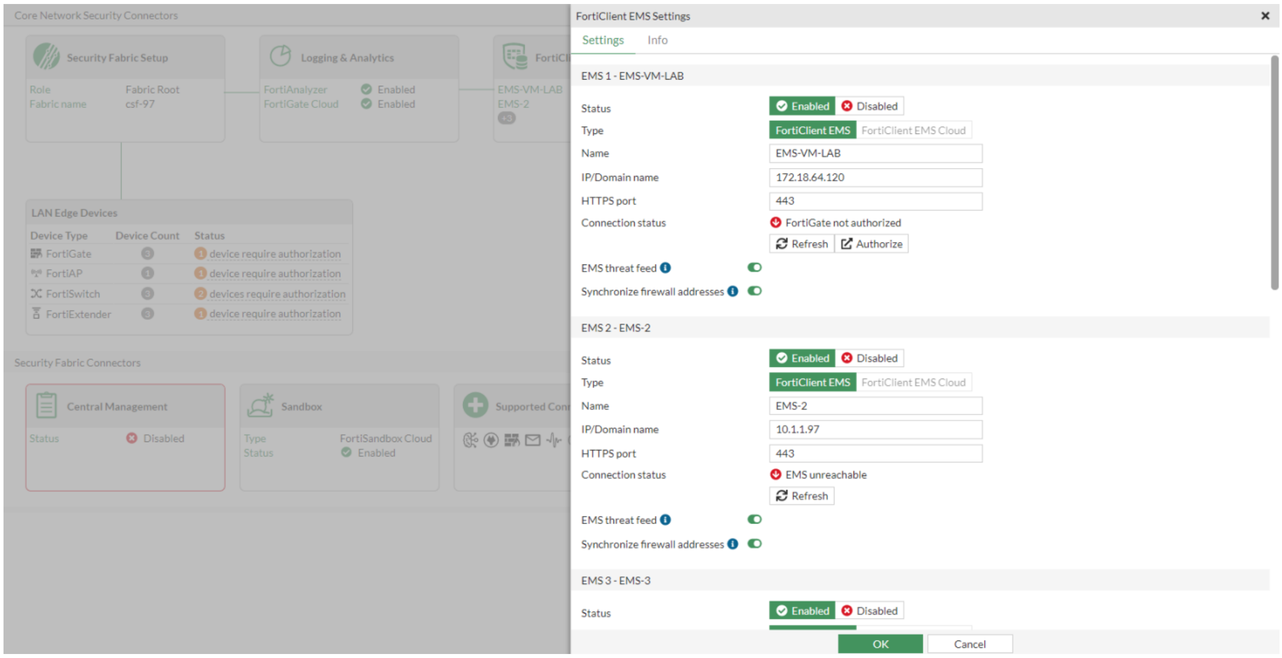
5. Click *OK*.

FortiClient EMS connector

FortiClient EMS is an updated card that combines the settings from the previous individual *FortiClient EMS* connector cards into one card. There are separate sections within the *Settings* tab to configure each EMS entry.

To configure the FortiClient EMS connectors:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiClient EMS* card.
2. Select the *Settings* tab and set the *Status* to *Enabled*.
3. Configure the remaining settings as needed.



FortiClient EMS Settings

EMS 1 - EMS-VM-LAB

Status	✓ Enabled ☒ Disabled
Type	FortiClient EMS FortiClient EMS Cloud
Name	EMS-VM-LAB
IP/Domain name	172.18.64.120
HTTPS port	443
Connection status	FortiGate not authorized
EMS threat feed	●
Synchronize firewall addresses	●

EMS 2 - EMS-2

Status	✓ Enabled ☒ Disabled
Type	FortiClient EMS FortiClient EMS Cloud
Name	EMS-2
IP/Domain name	10.1.1.97
HTTPS port	443
Connection status	EMS unreachable
EMS threat feed	●
Synchronize firewall addresses	●

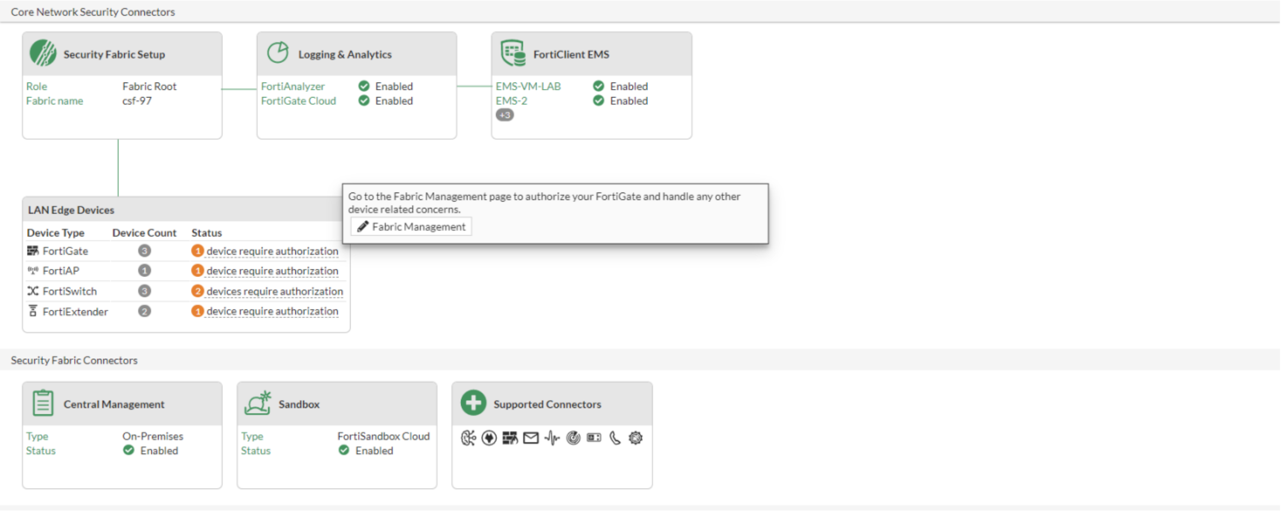
EMS 3 - EMS-3

Status	✓ Enabled ☒ Disabled

4. Click *OK*.

LAN Edge Devices

LAN Edge Devices is a new card that displays a summary about the LAN edge devices. This includes FortiGates, FortiAPs, FortiSwitches, and FortiExtenders. Information about the device type, number of devices, and number of unregistered and unauthorized devices is displayed. If there are devices that do not have a green checkmark in the *Status* column, hover over the status message to view the tooltip with required action. In this example, there are downstream FortiGates that require authorization. The tooltip includes a link to the *System* > *Fabric Management* page to authorize the FortiGates.



Core Network Security Connectors

Security Fabric Setup

Role	Fabric Root
Fabric name	csf-97

Logging & Analytics

FortiAnalyzer	✓ Enabled
FortiGate Cloud	✓ Enabled

FortiClient EMS

EMS-VM-LAB	✓ Enabled
EMS-2	✓ Enabled
+3	

LAN Edge Devices

Device Type	Device Count	Status
FortiGate	3	1 device require authorization
FortiAP	1	1 device require authorization
FortiSwitch	3	2 devices require authorization
FortiExtender	2	1 device require authorization

Go to the Fabric Management page to authorize your FortiGate and handle any other device related concerns.

Security Fabric Connectors

Central Management

Type	On-Premises
Status	✓ Enabled

Sandbox

Type	FortiSandbox Cloud
Status	✓ Enabled

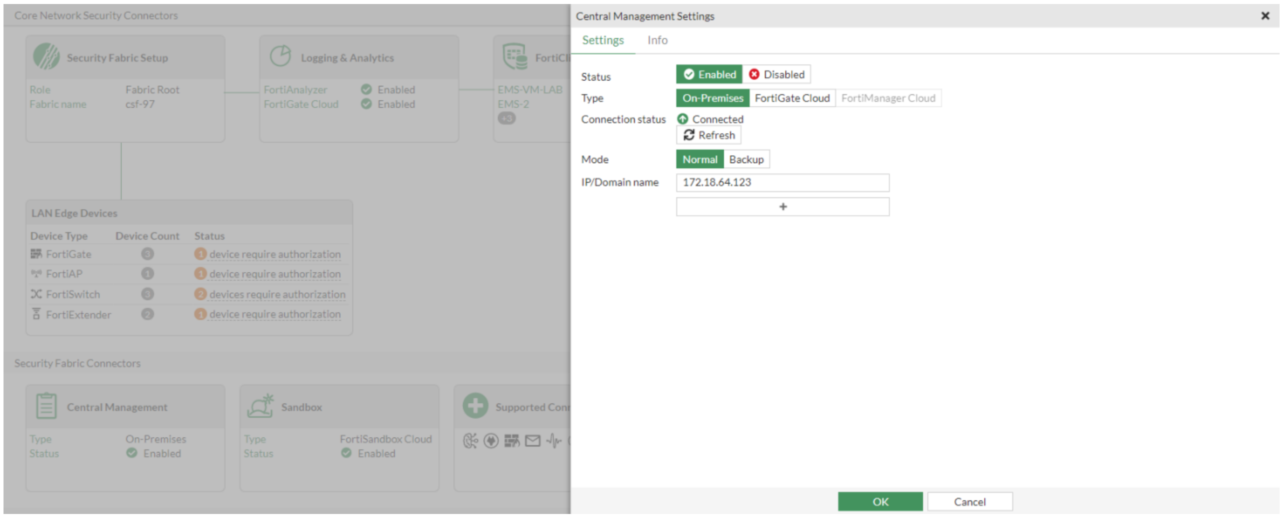
Supported Connectors

Central Management connector

Central Management is a new card that replaces the settings from the previous *FortiManager* card. In this example, on-premises FortiManager is enabled.

To configure the Central Management connector:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Central Management* card.
2. Set the *Status* to *Enabled*.
3. Set the *Type* to *On-Premises*.
4. Configure the remaining settings as needed.



Central Management Settings

Settings | Info

Status: Enabled | Disabled

Type: On-Premises | FortiGate Cloud | FortiManager Cloud

Connection status: Connected

Refresh

Mode: Normal | Backup

IP/Domain name: 172.18.64.123

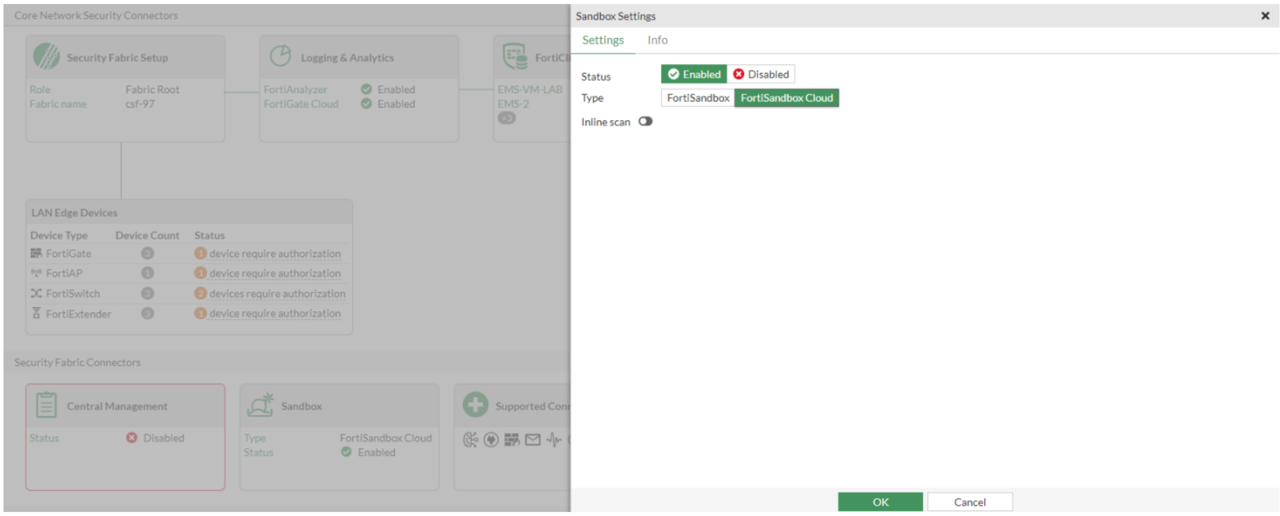
5. Click *OK*.

Sandbox connector

Sandbox is a new card that combines the settings from the previous *FortiSandbox* and *Cloud Sandbox* cards into a single connector to configure the sandboxing settings. In this example, FortiSandbox Cloud is enabled.

To configure the sandboxing settings:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Sandbox* card.
2. Set the *Status* to *Enabled*.
3. Set the *Type* to *FortiSandbox Cloud*.


Core Network Security Connectors
Security Fabric Setup
Role Fabric Root
Fabric name csf-97
Logging & Analytics
FortiAnalyzer Enabled
FortiGate Cloud Enabled
FortiCl
EMS-VM-LAB
EMS-2
+3
LAN Edge Devices
Device Type Device Count Status
FortiGate 3 1 device require authorization
FortiAP 1 1 device require authorization
FortiSwitch 3 2 devices require authorization
FortiExtender 3 1 device require authorization
Security Fabric Connectors
Central Management
Status Disabled
Sandbox
Type FortiSandbox Cloud
Status Enabled
Supported Con

Sandbox Settings ×

Settings | Info

Status: ● Enabled | Disabled

Type: FortiSandbox | **FortiSandbox Cloud**

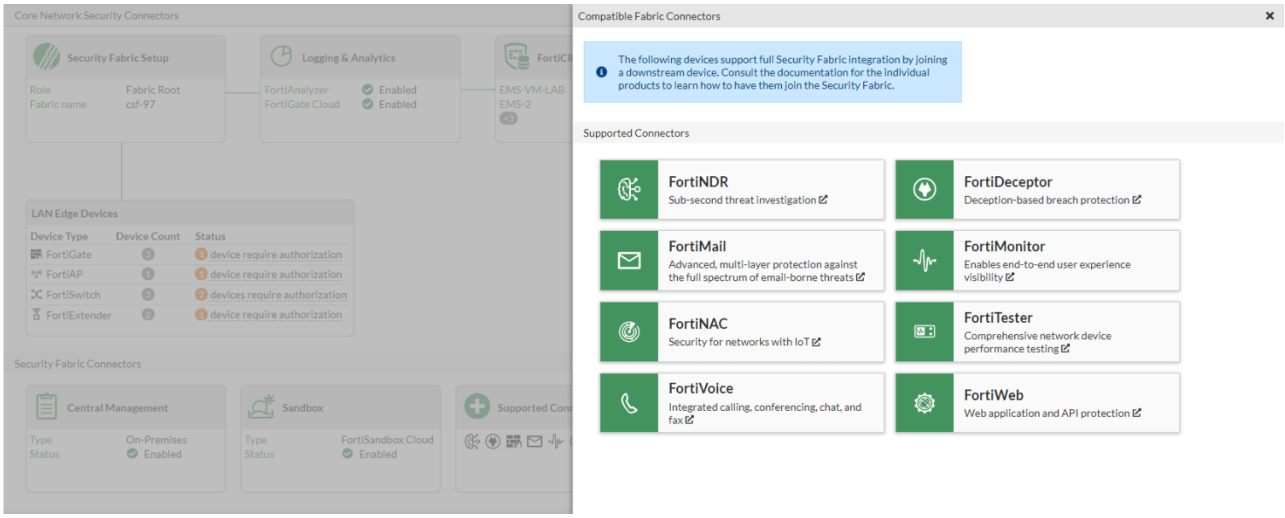
Inline scan: ○

OK | Cancel

4. Click *OK*.

Supported Connectors

Supported Connectors is a new card that displays the icons of different Fortinet devices that support full Security Fabric integration. Supported connectors do not have separate connector settings within FortiOS. Clicking the *Supported Connectors* card displays a list of cards with compatible device names.



Compatible Fabric Connectors ×

The following devices support full Security Fabric integration by joining a downstream device. Consult the documentation for the individual products to learn how to have them join the Security Fabric.

Supported Connectors

FortiNDR Sub-second threat investigation	**FortiDeceptor** Deception-based breach protection
FortiMail Advanced, multi-layer protection against the full spectrum of email-borne threats	**FortiMonitor** Enables end-to-end user experience visibility
FortiNAC Security for networks with IoT	**FortiTester** Comprehensive network device performance testing
FortiVoice Integrated calling, conferencing, chat, and fax	**FortiWeb** Web application and API protection

Clicking a device name card links to documentation that explains how configure it in the Security Fabric. Once the device is configured, it can be authorized on the *System > Fabric Management* page in FortiOS.

Add FortiPolicy as Security Fabric device - 7.2.4

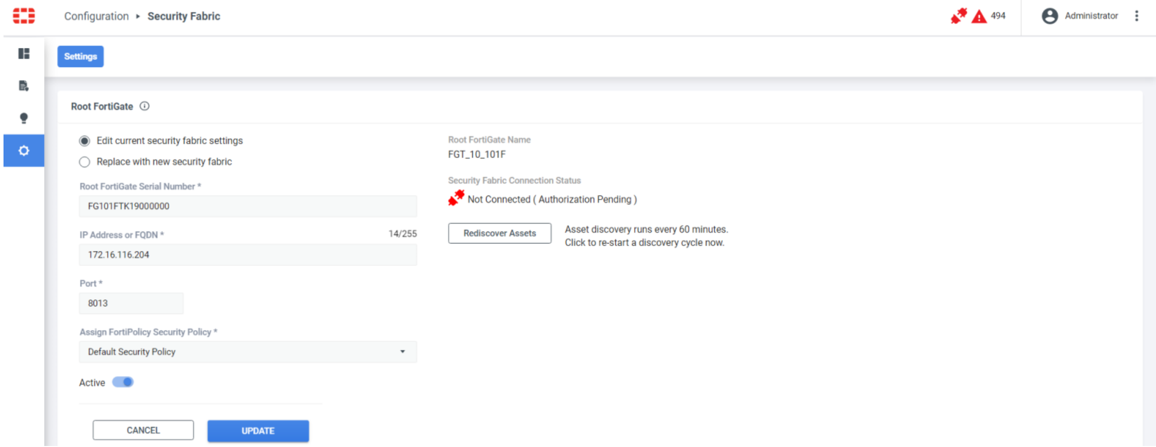
This information is also available in the FortiOS 7.2 Administration Guide:

- Configuring FortiPolicy

FortiPolicy can be added to the Security Fabric. When FortiPolicy joins the Security Fabric and is authorized in the *Security Fabric* widget, it appears in the Fabric topology pages. A FortiGate can grant permission to FortiPolicy to perform firewall address and policy changes. Two security rating tests for FortiPolicy have been added to the *Security Posture* scorecard.

To add FortiPolicy to the Security Fabric:

1. Enable the Security Fabric (see Configuring the root FortiGate and downstream FortiGates in the FortiOS Administration Guide) with the following settings:
   a. Configure the interface to allow other Security Fabric devices to join.
   b. Enable *Allow downstream device REST API access* and select an *Administrator profile*.
2. In FortiPolicy, edit the Security Fabric settings (this example assumes a root FortiGate has already been configured, see Creating a fabric connector in the FortiPolicy Administration Guide):
   a. Go to *Configuration* > *Security Fabric* and select *Edit current security fabric settings*.
   b. Enter the root FortiGate's IP address.
   c. Set the *Port* (the default is *8013*).
   d. Select a FortiPolicy security policy.



Root FortiGate

● Edit current security fabric settings
○ Replace with new security fabric

Root FortiGate Serial Number *
FG101FTK19000000

IP Address or FQDN * 14/255
172.16.116.204

Port *
8013

Assign FortiPolicy Security Policy *
Default Security Policy

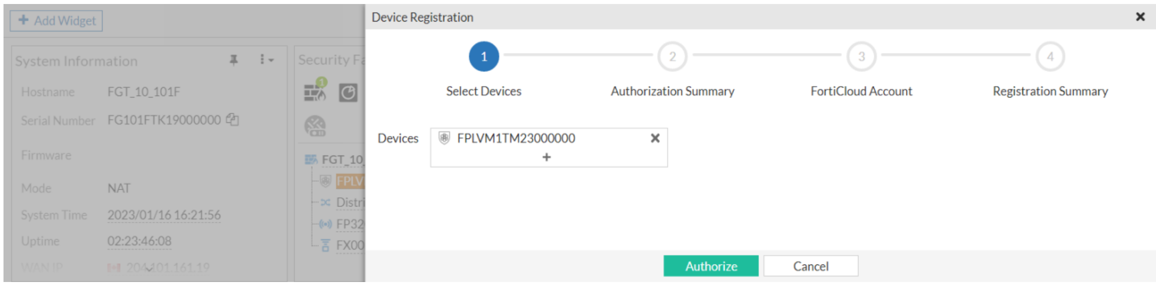
Active

Root FortiGate Name
FGT_10_101F

Security Fabric Connection Status
Not Connected (Authorization Pending)

Asset discovery runs every 60 minutes.
Click to re-start a discovery cycle now.

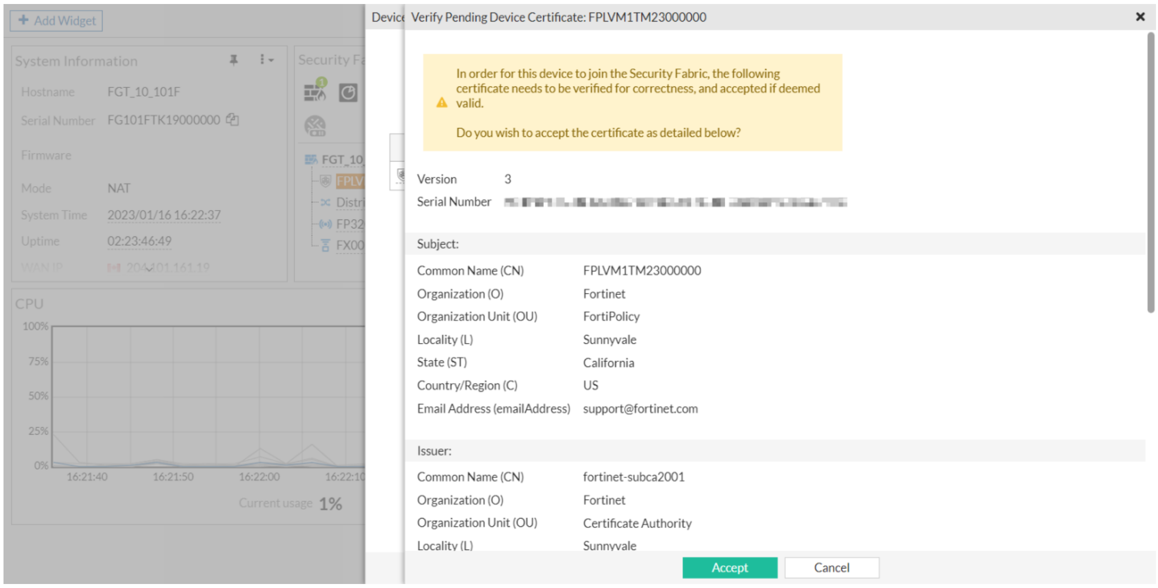
   e. Click *UPDATE*. The connection status is *Not Connected (Authorization Pending)*.
3. Authorize the FortiPolicy in FortiOS:
   a. Go to *Dashboard* > *Status* and locate the *Security Fabric* widget.
   b. In the topology tree, click the highlighted FortiPolicy and select *Authorize*. The *Device Registration* pane opens.
   c. Click *Authorize*.



Hostname FGT_10_101F
Serial Number FG101FTK19000000
Firmware
Mode NAT
System Time 2023/01/16 16:21:56
Uptime 02:23:46:08
WAN IP 204.101.161.19

Devices FPLVM1TM23000000

   d. Click *Accept* to verify the device certificate.



Verify Pending Device Certificate: FPLVM1TM23000000

In order for this device to join the Security Fabric, the following certificate needs to be verified for correctness, and accepted if deemed valid.

Do you wish to accept the certificate as detailed below?

Version	3
Serial Number	[redacted]

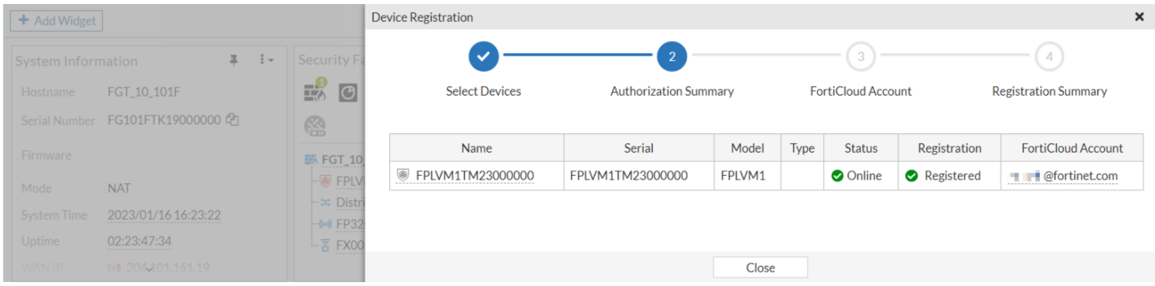
Subject:

Common Name (CN)	FPLVM1TM23000000
Organization (O)	Fortinet
Organization Unit (OU)	FortiPolicy
Locality (L)	Sunnyvale
State (ST)	California
Country/Region (C)	US
Email Address (emailAddress)	support@fortinet.com

Issuer:

Common Name (CN)	fortinet-subca2001
Organization (O)	Fortinet
Organization Unit (OU)	Certificate Authority
Locality (L)	Sunnyvale

e. Once the FortiPolicy is registered, click *Close*.

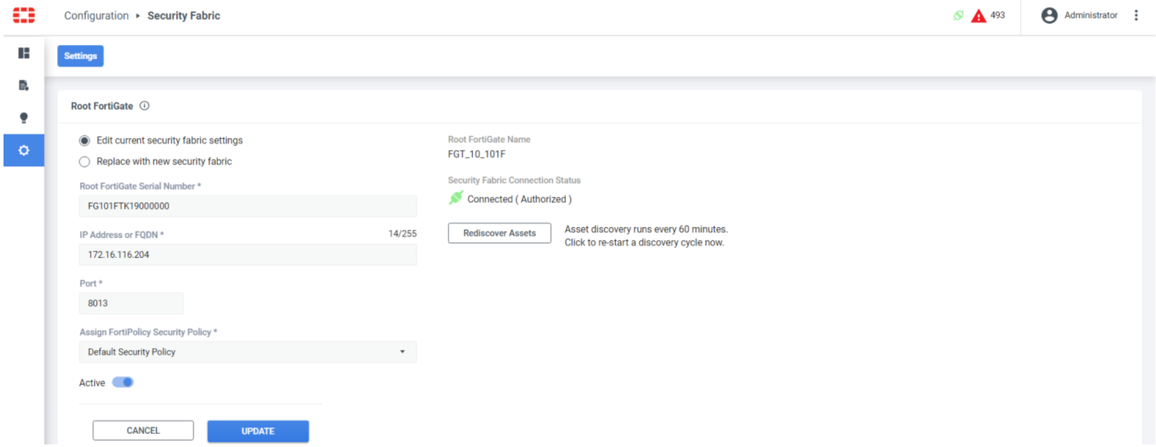


Device Registration

1 Select Devices — 2 Authorization Summary — 3 FortiCloud Account — 4 Registration Summary

Name	Serial	Model	Type	Status	Registration	FortiCloud Account
FPLVM1TM23000000	FPLVM1TM23000000	FPLVM1		✓ Online	✓ Registered	[redacted]@fortinet.com

4. In FortiPolicy, refresh the *Configuration* > *Security Fabric* page. and verify that the connection status is *Connected (Authorized)*.



Configuration ▸ Security Fabric

Root FortiGate

● Edit current security fabric settings

○ Replace with new security fabric

Root FortiGate Serial Number *: FG101FTK19000000

IP Address or FQDN *: 172.16.116.204 (14/255)

Port *: 8013

Assign FortiPolicy Security Policy *: Default Security Policy

Active: on

Root FortiGate Name: FGT_10_101F

Security Fabric Connection Status: Connected (Authorized)

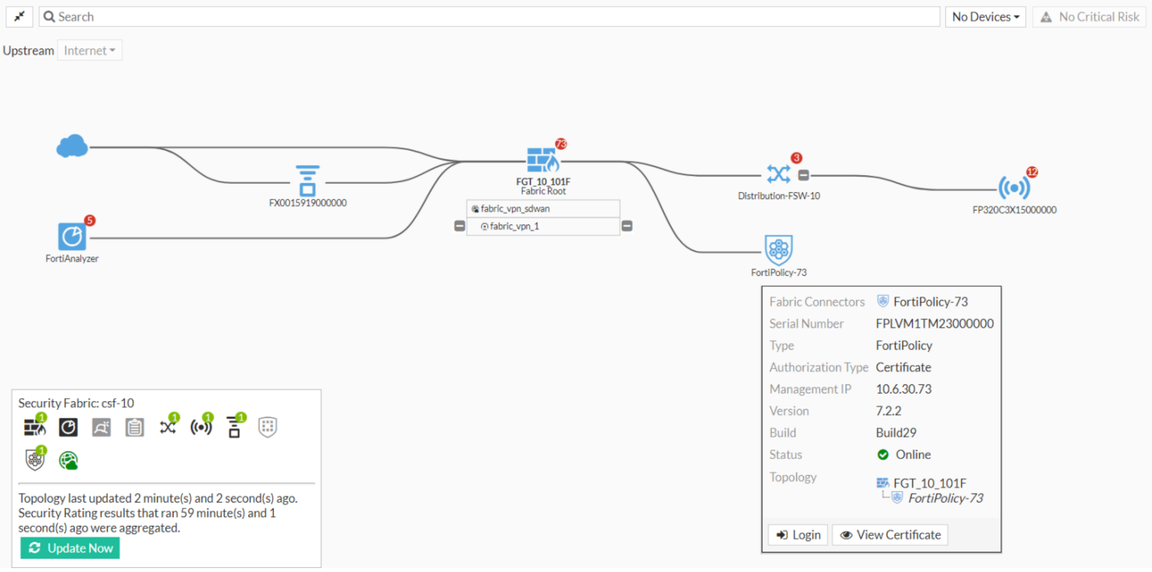
Asset discovery runs every 60 minutes. Click to re-start a discovery cycle now.

5. In FortiOS, grant FortiPolicy write access permission in the CLI:

```
config system csf
    config fabric-connector
        edit "FPLVM1TM23000000"
            set configuration-write-access enable
        next
        end
    end
```

6. Go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology* to view more information.

   Physical topology view:

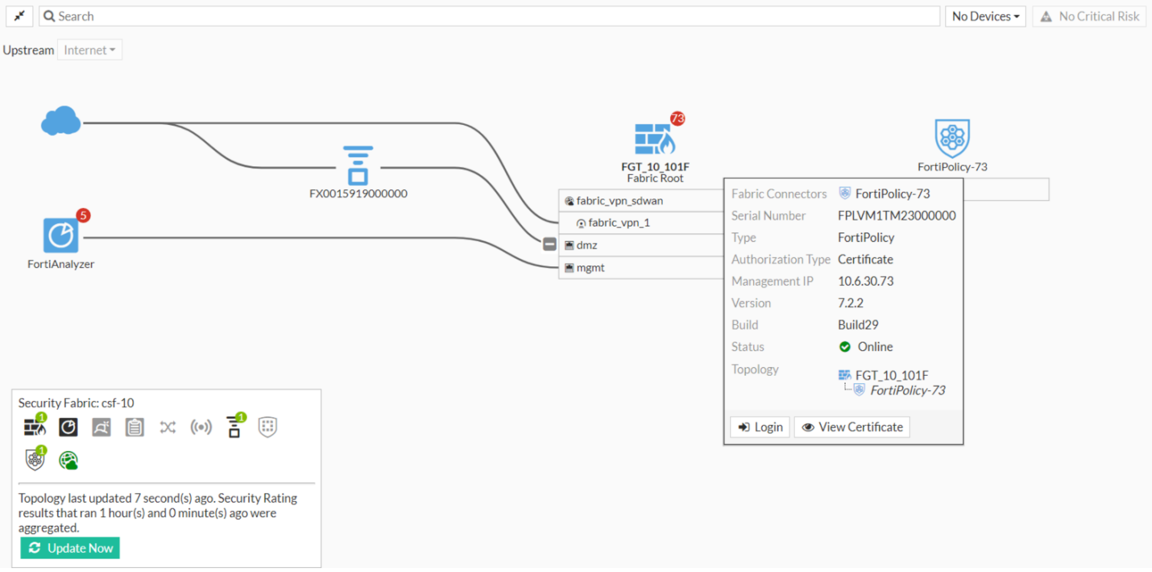


Fabric Connectors	FortiPolicy-73
Serial Number	FPLVM1TM23000000
Type	FortiPolicy
Authorization Type	Certificate
Management IP	10.6.30.73
Version	7.2.2
Build	Build29
Status	Online
Topology	FGT_10_101F └ *FortiPolicy-73*

Security Fabric: csf-10

Topology last updated 2 minute(s) and 2 second(s) ago. Security Rating results that ran 59 minute(s) and 1 second(s) ago were aggregated.

   Logical topology view:



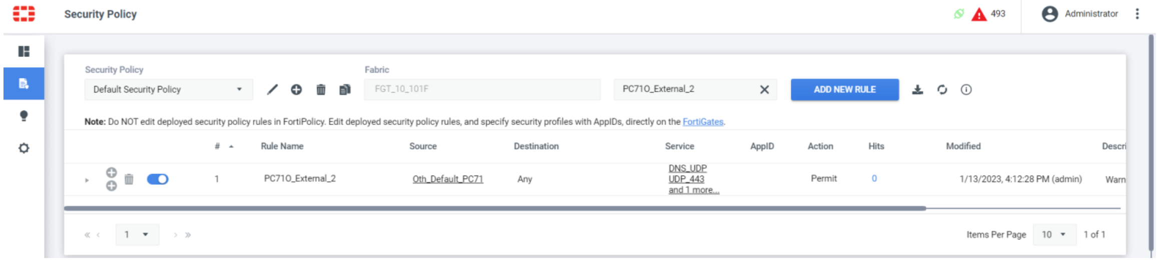
Fabric Connectors	FortiPolicy-73
Serial Number	FPLVM1TM23000000
Type	FortiPolicy
Authorization Type	Certificate
Management IP	10.6.30.73
Version	7.2.2
Build	Build29
Status	Online
Topology	FGT_10_101F └ *FortiPolicy-73*

Security Fabric: csf-10

Topology last updated 7 second(s) ago. Security Rating results that ran 1 hour(s) and 0 minute(s) ago were aggregated.

To deploy firewall policies from FortiPolicy to the root FortiGate:

1. Create a policy in FortiPolicy (see Customizing policies in the FortiPolicy Administration Guide).



Security Policy: Default Security Policy
Fabric: FGT_10_101F
PC710_External_2

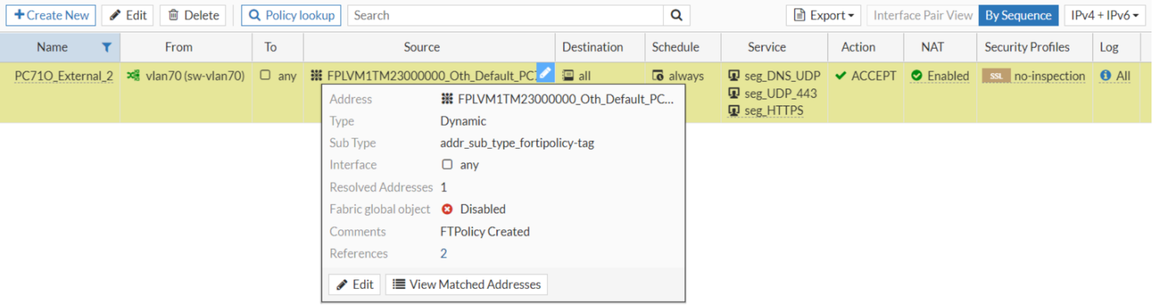
Note: Do NOT edit deployed security policy rules in FortiPolicy. Edit deployed security policy rules, and specify security profiles with AppIDs, directly on the FortiGates.

#	Rule Name	Source	Destination	Service	AppID	Action	Hits	Modified	Descri
1	PC710_External_2	Oth_Default_PC71	Any	DNS_UDP UDP_443 and 1 more...		Permit	0	1/13/2023, 4:12:28 PM (admin)	Warn

Items Per Page 10 1 of 1

In this example, a default security policy rule called *PC71O_External_2* is created. Since the FortiPolicy is integrated in the Security Fabric, it will use the REST API to push the static policy, dynamic firewall objects, and service objects to the root FortiGate.

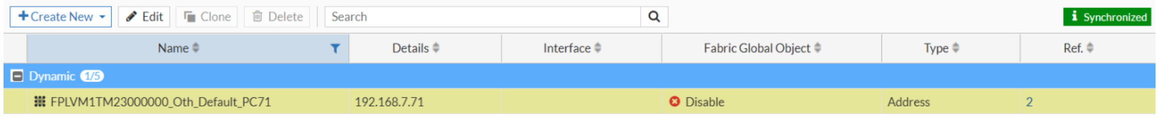
2. In FortiOS, go to *Policy & Objects > Firewall Policy* to view the policy named *PC71O_External_2*.



Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
PC71O_External_2	vlan70 (sw-vlan70)	any	FPLVM1TM23000000_Oth_Default_PC7	all	always	seg_DNS_UDP seg_UDP_443 seg_HTTPS	ACCEPT	Enabled	SSL no-inspection	All

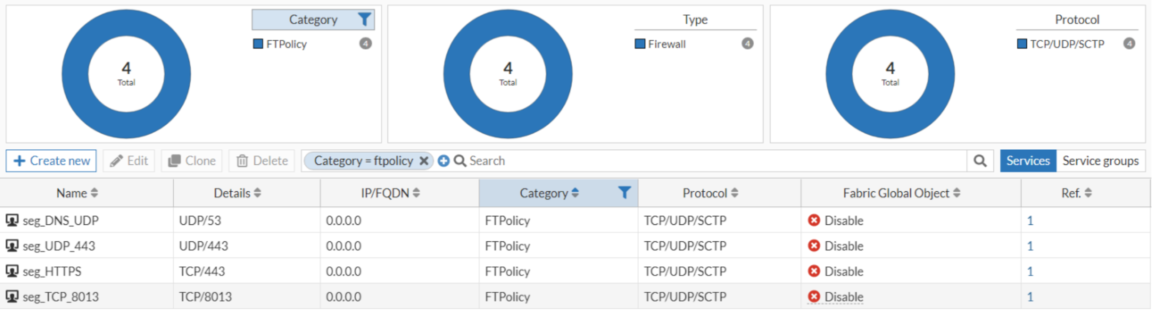
Address	FPLVM1TM23000000_Oth_Default_PC...
Type	Dynamic
Sub Type	addr_sub_type_fortipolicy-tag
Interface	any
Resolved Addresses	1
Fabric global object	Disabled
Comments	FTPolicy Created
References	2

3. Go to *Policy & Objects > Addresses* to view the dynamic firewall address associated with the policy (*FPLVM1TM23000000_Oth_Default_PC71*).



Name	Details	Interface	Fabric Global Object	Type	Ref.
Dynamic 1/5					
FPLVM1TM23000000_Oth_Default_PC71	192.168.7.71		Disable	Address	2

4. Go to *Policy & Objects > Services* to view the service objects associated with the policy (*seg_DNS_UDP*, *seg_UDP_443*, *seg_HTTPS*, and *seg_TCP_8013*).



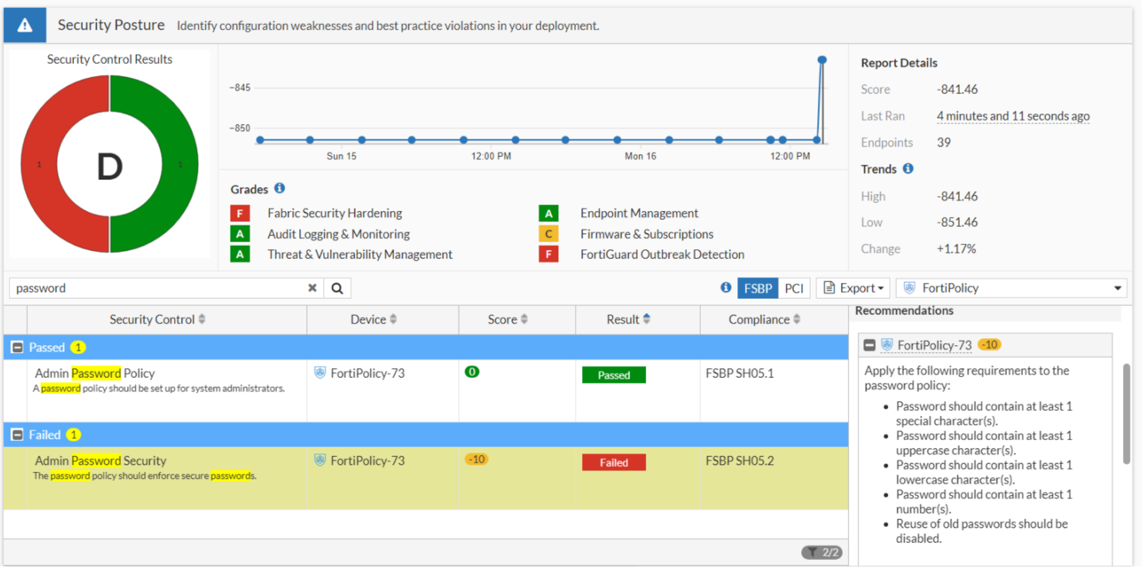
Name	Details	IP/FQDN	Category	Protocol	Fabric Global Object	Ref.
seg_DNS_UDP	UDP/53	0.0.0.0	FTPolicy	TCP/UDP/SCTP	Disable	1
seg_UDP_443	UDP/443	0.0.0.0	FTPolicy	TCP/UDP/SCTP	Disable	1
seg_HTTPS	TCP/443	0.0.0.0	FTPolicy	TCP/UDP/SCTP	Disable	1
seg_TCP_8013	TCP/8013	0.0.0.0	FTPolicy	TCP/UDP/SCTP	Disable	1

Security rating tests

There are two security rating tests pertaining to FortiPolicy available on the *Security Posture* scorecard:

- *Admin Password Policy* ensures that there is password policy in place for system administrators. In this result, the test is marked as *Passed* because there is a login rule configured in FortiPolicy with *Local Password Criteria* enabled.

- *Admin Password Security* ensures that the password policy enforces secure passwords. In this result, the test is marked as *Failed* because the password policy does not include set variables for the *Local Password Criteria*.



Security Posture   Identify configuration weaknesses and best practice violations in your deployment.

Grades

F	Fabric Security Hardening	A	Endpoint Management
A	Audit Logging & Monitoring	C	Firmware & Subscriptions
A	Threat & Vulnerability Management	F	FortiGuard Outbreak Detection

Report Details

Score	-841.46
Last Ran	4 minutes and 11 seconds ago
Endpoints	39

Trends

High	-841.46
Low	-851.46
Change	+1.17%

password

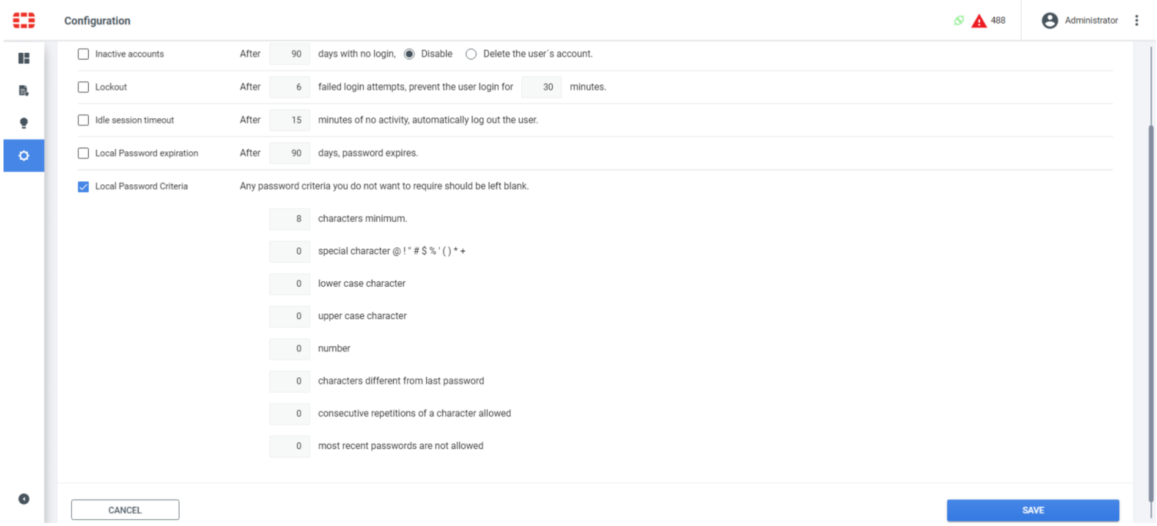
Security Control	Device	Score	Result	Compliance
Passed 1				
Admin Password Policy A password policy should be set up for system administrators.	FortiPolicy-73	0	Passed	FSBP SH05.1
Failed 1				
Admin Password Security The password policy should enforce secure passwords.	FortiPolicy-73	-10	Failed	FSBP SH05.2

Recommendations

FortiPolicy-73 -10

Apply the following requirements to the password policy:

- Password should contain at least 1 special character(s).
- Password should contain at least 1 uppercase character(s).
- Password should contain at least 1 lowercase character(s).
- Password should contain at least 1 number(s).
- Reuse of old passwords should be disabled.



Configuration

☐ Inactive accounts   After 90 days with no login, ● Disable ○ Delete the user´s account.

☐ Lockout   After 6 failed login attempts, prevent the user login for 30 minutes.

☐ Idle session timeout   After 15 minutes of no activity, automatically log out the user.

☐ Local Password expiration   After 90 days, password expires.

☑ Local Password Criteria   Any password criteria you do not want to require should be left blank.

8 characters minimum.

0 special character @ ! " # $ % ' ( ) * +

0 lower case character

0 upper case character

0 number

0 characters different from last password

0 consecutive repetitions of a character allowed

0 most recent passwords are not allowed

See Users in the FortiPolicy Administration Guide for more information about configuring these settings.

Allow FortiClient EMS connectors to trust EMS server certificate renewals based on the CN field - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Allowing FortiClient EMS connectors to trust EMS server certificate renewals based on the CN field

When a FortiGate establishes a Fabric connection with FortiClient EMS, the FortiGate must trust the CA that signed the server certificate. Previously, upon the user's approval of the certificate, the certificate fingerprint was saved on the

FortiGate. This required the FortiGate to re-authorize the EMS connection each time the server certificate is updated. With this enhancement, upon the approval of the EMS certificate, the FortiGate saves the CN field and will trust future certificates that are signed by the same CA and have the same CN field. This allows EMS servers to update their certificates at regular intervals without requiring re-authorization on the FortiGate side, as long as the CN field matches. This prevents interruptions to the EMS Fabric connection when a certificate is updated.

```
config endpoint-control fctems
    edit <id>
        set trust-ca-cn {enable | disable}
    next
end
```

This feature is supported for EMS on-premise and cloud connections, and is the new default setting. To authorize based on the certificate fingerprint, disable the `trust-ca-cn` setting. If the setting is changed back to be enabled at a later time, the user will have to re-approve the EMS certificate.

To configure the EMS Fabric connector to trust EMS server certificate renewals based on the CN field:

```
config endpoint-control fctems
    edit 1
        set status enable
        set name "ems133"
        set dirty-reason none
        set fortinetone-cloud-authentication disable
        set server "172.18.62.35"
        set https-port 443
        set serial-number "FCTEMS8822000000"
        set tenant-id "00000000000000000000000000000000"
        set source-ip 0.0.0.0
        set pull-sysinfo enable
        set pull-vulnerabilities enable
        set pull-avatars enable
        set pull-tags enable
        set pull-malware-hash enable
        set capabilities fabric-auth silent-approval websocket websocket-malware push-ca-
certs common-tags-api tenant-id
        set call-timeout 30
        set out-of-sync-threshold 180
        set websocket-override disable
        set preserve-ssl-session disable
        set interface-select-method auto
        set trust-ca-cn enable
    next
end
```

To verify the configuration:

1. Download the FortiGate configuration file.
2. Verify the `ca-cn-info` entry, which lists the trusted CA certificate information. In this example, ems133 connector has `trust-ca-cn` enabled and ems138 connector has `trust-ca-cn` disabled. For ems138, the `ca-cn-info` entry does not appear, and there is a `certificate-fingerprint` field instead:

```
config endpoint-control fctems
    edit 1
        set status enable
        set name "ems133"
        set server "172.18.62.35"
        set serial-number "FCTEMS8822000000"
        set tenant-id "00000000000000000000000000000000"
        set capabilities fabric-auth silent-approval websocket websocket-malware push-
ca-certs common-tags-api tenant-id
        set ca-cn-info "C = CA, ST = BC, L = VANCOUVER, O = FTNT, OU = ReleaseQA, CN =
Release_QA, emailAddress = ********@fortinet.comRelease_QA"
    next
    edit 2
        set status enable
        set name "ems138"
        set server "172.18.62.18"
        set serial-number "FCTEMS8821000000"
        set tenant-id "00000000000000000000000000000000"
        set capabilities fabric-auth silent-approval websocket websocket-malware push-
ca-certs common-tags-api tenant-id
        set certificate-fingerprint
"18:51:76:67:EB:4C:31:A1:51:3F:74:F7:8E:1D:47:5C:18:0F:FE:45:DF:52:91:52:37:0B:27:E7:F1:
85:5B:01:8C:7D:FB:2D:C7:D2:CC:FE:4A:E3:0E:A9:2A:1C:27:4D:D2:A6:C5:87:B8:97:98:57:75:10:1
5:28:EF:A2:23:7C"
        set trust-ca-cn disable
    next
    ...
end
```

3. Run diagnostics to view the certificate information:

```
# diagnose test application fcnacd 96
ems_id 1, certificate authority and common name: C = CA, ST = BC, L = VANCOUVER, O =
FTNT, OU = ReleaseQA, CN = Release_QA, emailAddress = ********@fortinet.comRelease_QA
ems_id 1, fingerprint_sha512:
ems_id 2, certificate authority and common name:
ems_id 2, fingerprint_sha512:
18:51:76:67:EB:4C:31:A1:51:3F:74:F7:8E:1D:47:5C:18:0F:FE:45:DF:52:91:52:37:0B:27:E7:F1:8
5:5B:01:8C:7D:FB:2D:C7:D2:CC:FE:4A:E3:0E:A9:2A:1C:27:4D:D2:A6:C5:87:B8:97:98:57:75:10:15
:28:EF:A2:23:7C
```

External connectors

This section includes information about SDN connector related new features:

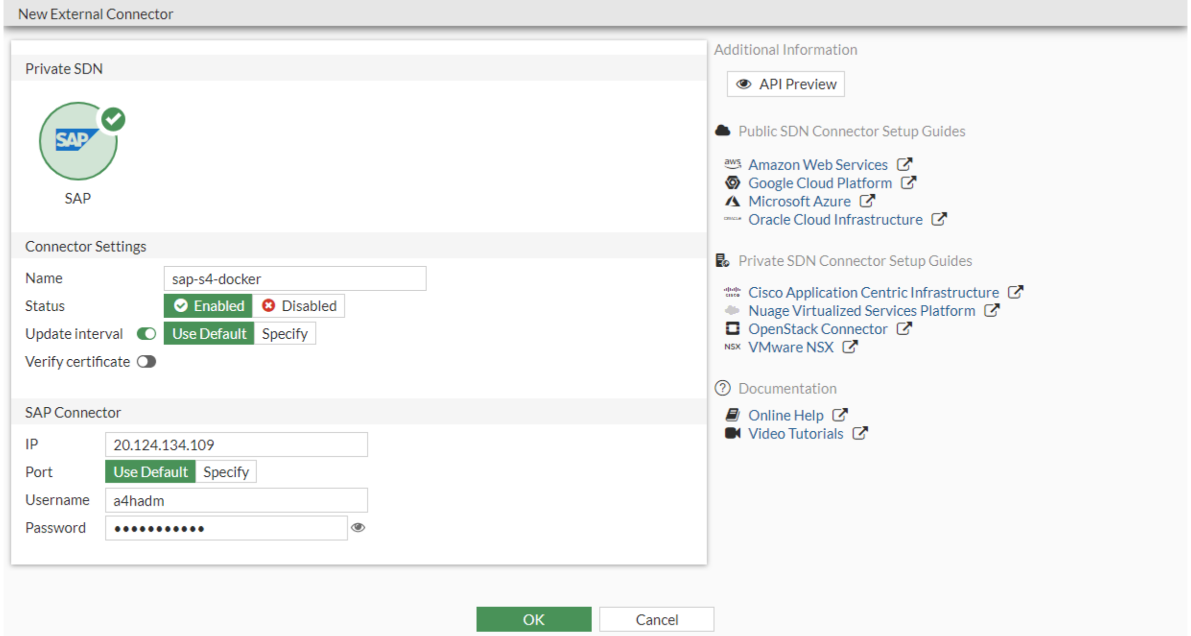
- SAP external connector 7.2.1 on page 63
- Using the REST API to push updates to external threat feeds 7.2.1 on page 66
- Support IPv6 dynamic addresses retrieved from Cisco ACI SDN connector 7.2.1 on page 71

SAP external connector - 7.2.1

The SAP external Fabric connector allows the FortiGate to connect to an SAP instance to synchronize dynamic address objects and ports for SAP workloads. These address objects can be used in firewall policies to grant access control to dynamic SAP workloads.

To configure an SAP connector in the GUI:

1. Configure the SAP SDN connector:
   a. Go to *Security Fabric > External Connectors* and click *Create New*.
   b. In the *Private SDN* section, select *SAP*.
   c. Enter a *Name* (*sap-s4-docker*).
   d. Enter the *IP* for the SAP instance.
   e. Enter the *Username* and *Password*.



New External Connector

Private SDN

SAP

Connector Settings

Name: sap-s4-docker

Status: Enabled | Disabled

Update interval: Use Default | Specify

Verify certificate

SAP Connector

IP: 20.124.134.109

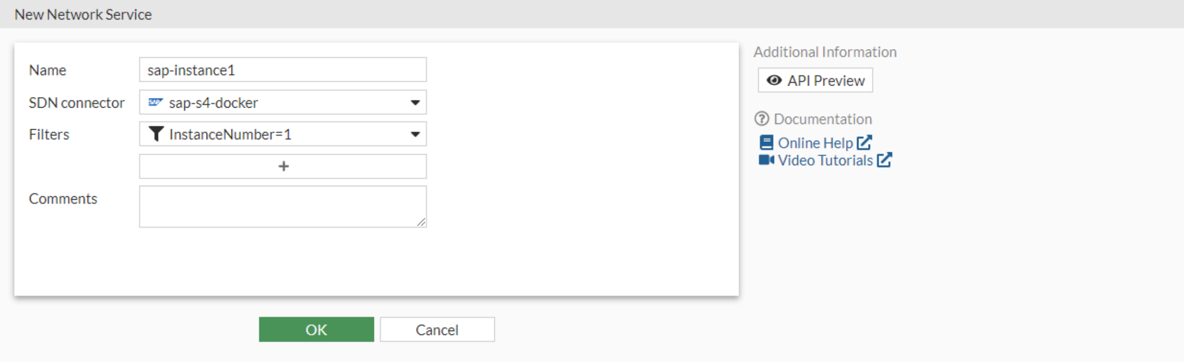
Port: Use Default | Specify

Username: a4hadm

Password: •••••••••••

Additional Information
API Preview
Public SDN Connector Setup Guides
Amazon Web Services
Google Cloud Platform
Microsoft Azure
Oracle Cloud Infrastructure
Private SDN Connector Setup Guides
Cisco Application Centric Infrastructure
Nuage Virtualized Services Platform
OpenStack Connector
VMware NSX
Documentation
Online Help
Video Tutorials
OK
Cancel

   f. Click *OK*.
2. Configure a network service associated with the configured SAP SDN connector:
   a. Go to *Policy & Objects > Internet Service Database*, select the *Network Services* tab, and click *Create New*.
   b. Enter a *Name* (*sap-instance1*).
   c. Set *SDN connector* to *sap-s4-docker*.
   d. Select a filter, such as *InstanceNumber=1*. The available filters are for HostName, InstanceNumber, and ServiceName.



New Network Service

Name: sap-instance1

SDN connector: sap-s4-docker

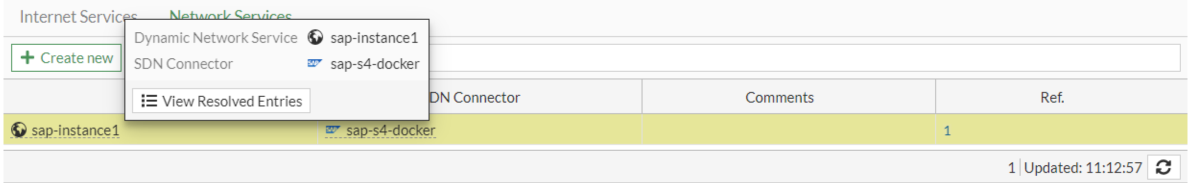
Filters: InstanceNumber=1

Comments

   e. Click *OK*.
3. Ensure that the SAP SDN connector resolves dynamic network services:

a. Go to *Policy & Objects* > *Internet Service Database*, select the *Network Services* tab.

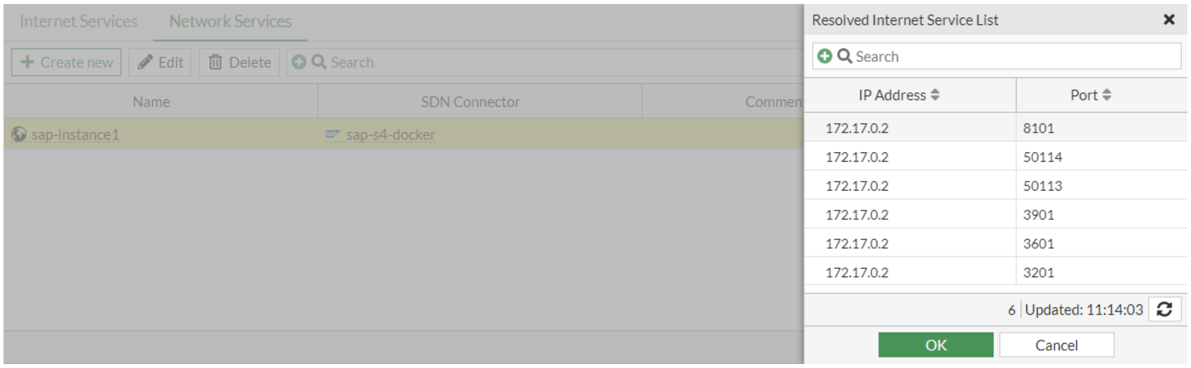
b. Hover over the *sap-instance1* and click *View Resolved Entries*.



Dynamic Network Service: sap-instance1
SDN Connector: sap-s4-docker

Name	SDN Connector	Comments	Ref.
sap-instance1	sap-s4-docker		1

A list of resolved internet services is displayed.



Name	SDN Connector	Comments
sap-instance1	sap-s4-docker	

IP Address	Port
172.17.0.2	8101
172.17.0.2	50114
172.17.0.2	50113
172.17.0.2	3901
172.17.0.2	3601
172.17.0.2	3201

Click *OK* to close the list.

4. Configure a firewall policy with the resolved dynamic network service as the destination:

   a. Go to *Policy & Objects* >*Firewall Policy* and click *Create New*.

   b. Set the *Destination* to the *sap-instance1* network service.

   c. Configure the other settings as needed.

   d. Click *OK*.

To configure an SAP connector in the CLI:

1. Configure the SAP SDN connector:

```
config system sdn-connector
    edit "sap-s4-docker"
        set type sap
        set verify-certificate disable
        set server "20.124.134.109"
        set server-port 50014
        set username "a4hadm"
        set password ************
    next
end
```

2. Configure a network service associated with the configured SAP SDN connector (available filters are HostName, InstanceNumber, and ServiceName):

```
config firewall network-service-dynamic
    edit "sap-instance1"
        set sdn "sap-s4-docker"
        set filter "InstanceNumber=1"
    next
end
```

3. Ensure that the SAP SDN connector resolves dynamic network services:

```
# diagnose firewall network-service-dynamic list "sap-instance1"
List internet service in kernel(custom):
name=sap-instance1 id=4294770689 reputation=0 (null) singularity=0 flags=0x0 protocol=6
port=8101-8101
addr ip range(1): 172.17.0.2-172.17.0.2
name=sap-instance1 id=4294770689 reputation=0 (null) singularity=0 flags=0x0 protocol=6
port=50114-50114
addr ip range(1): 172.17.0.2-172.17.0.2
name=sap-instance1 id=4294770689 reputation=0 (null) singularity=0 flags=0x0 protocol=6
port=50113-50113
addr ip range(1): 172.17.0.2-172.17.0.2
name=sap-instance1 id=4294770689 reputation=0 (null) singularity=0 flags=0x0 protocol=6
port=3901-3901
addr ip range(1): 172.17.0.2-172.17.0.2
name=sap-instance1 id=4294770689 reputation=0 (null) singularity=0 flags=0x0 protocol=6
port=3601-3601
addr ip range(1): 172.17.0.2-172.17.0.2
name=sap-instance1 id=4294770689 reputation=0 (null) singularity=0 flags=0x0 protocol=6
port=3201-3201
addr ip range(1): 172.17.0.2-172.17.0.2
```

4. Configure a firewall policy with the resolved dynamic network service as the destination:

```
config firewall policy
    edit 2
        set name "FGT97-service-dynamic"
        set srcintf "port3"
        set dstintf "port10"
        set action accept
        set srcaddr "all"
        set internet-service enable
        set network-service-dynamic "sap-instance1"
        set schedule "always"
        set nat enable
    next
end
```

Using the REST API to push updates to external threat feeds - 7.2.1

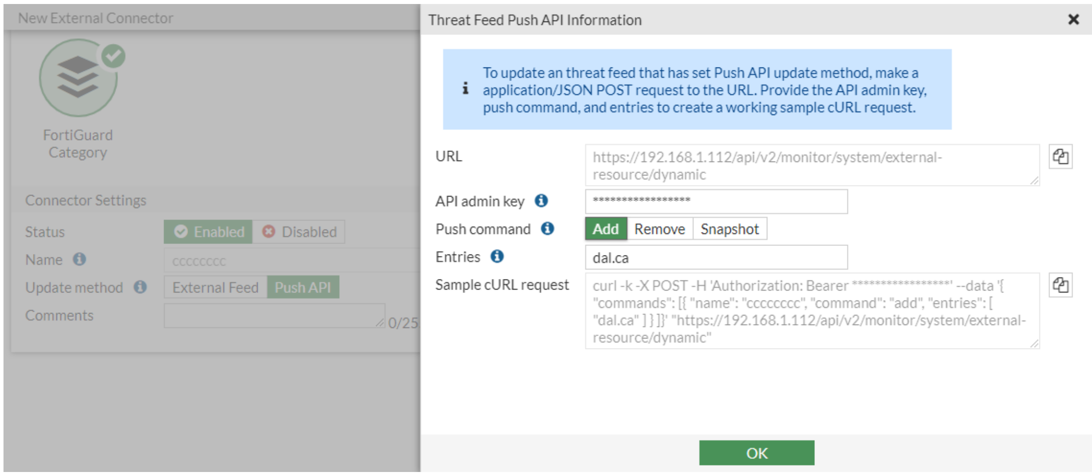
When configuring a *FortiGuard Category*, *Malware Hash*, *IP Address*, or *Domain Name* threat feed from the *Security Fabric > External Connectors* page, selecting the *Push API* update method provides the code samples needed to perform add, remove, and snapshot operations. The code samples can be used to perform updates on the external threat feeds.

In the following example, a *FortiGuard Category* threat feed is used to show the different API push options.

To configure the threat feed in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *FortiGuard Category*.
3. Enter a name.
4. Set the *Update method* to *Push API*.

5. Click *OK*. The *Threat Feed Push API Information* pane opens that contains the following fields:
    - *URL*: the FortiGate's API URL to call in order to perform the update.
    - *API admin key*: when an API administrator user is configured on the FortiGate, an *API admin key* will be associated with the API administrator. Input the API key to see the final cURL request.
    - *Push command*: select one of three push methods.
        - *Add*: add the specified entries to the threat feed.



New External Connector

FortiGuard Category

Connector Settings

Status: Enabled | Disabled

Name: cccccccc

Update method: External Feed | Push API

Comments: 0/255

Threat Feed Push API Information

To update an threat feed that has set Push API update method, make a application/JSON POST request to the URL. Provide the API admin key, push command, and entries to create a working sample cURL request.

URL: https://192.168.1.112/api/v2/monitor/system/external-resource/dynamic

API admin key: ******************

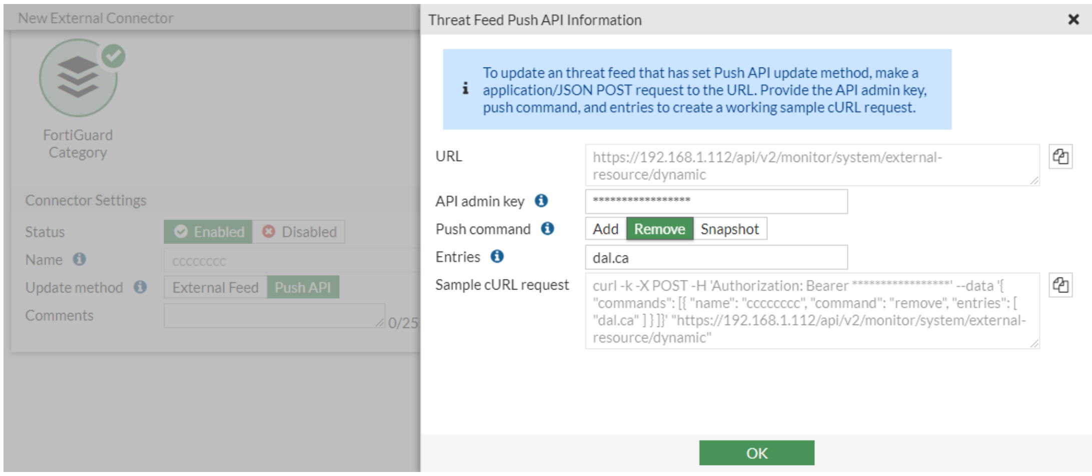
Push command: Add | Remove | Snapshot

Entries: dal.ca

Sample cURL request:

```
curl -k -X POST -H 'Authorization: Bearer ******************' --data '{ "commands": [{ "name": "cccccccc", "command": "add", "entries": [ "dal.ca" ] } ]}' "https://192.168.1.112/api/v2/monitor/system/external-resource/dynamic"
```

        - *Remove*: remove the specified entries from the threat feed.



New External Connector

FortiGuard Category

Connector Settings

Status: Enabled | Disabled

Name: cccccccc

Update method: External Feed | Push API

Comments: 0/255

Threat Feed Push API Information

To update an threat feed that has set Push API update method, make a application/JSON POST request to the URL. Provide the API admin key, push command, and entries to create a working sample cURL request.

URL: https://192.168.1.112/api/v2/monitor/system/external-resource/dynamic

API admin key: ******************

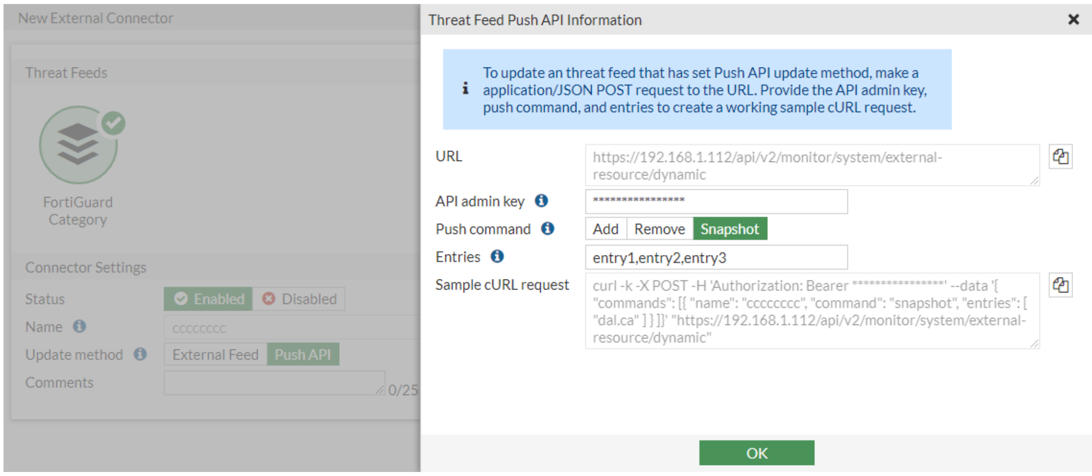
Push command: Add | Remove | Snapshot

Entries: dal.ca

Sample cURL request:

```
curl -k -X POST -H 'Authorization: Bearer ******************' --data '{ "commands": [{ "name": "cccccccc", "command": "remove", "entries": [ "dal.ca" ] } ]}' "https://192.168.1.112/api/v2/monitor/system/external-resource/dynamic"
```

- *Snapshot*: replace the threat feed with all specified entries.



New External Connector

Threat Feeds

FortiGuard Category

Connector Settings

Status: Enabled | Disabled

Name: cccccccc

Update method: External Feed | Push API

Comments: 0/25

Threat Feed Push API Information

To update an threat feed that has set Push API update method, make a application/JSON POST request to the URL. Provide the API admin key, push command, and entries to create a working sample cURL request.

URL: https://192.168.1.112/api/v2/monitor/system/external-resource/dynamic

API admin key: ****************

Push command: Add | Remove | Snapshot

Entries: entry1,entry2,entry3

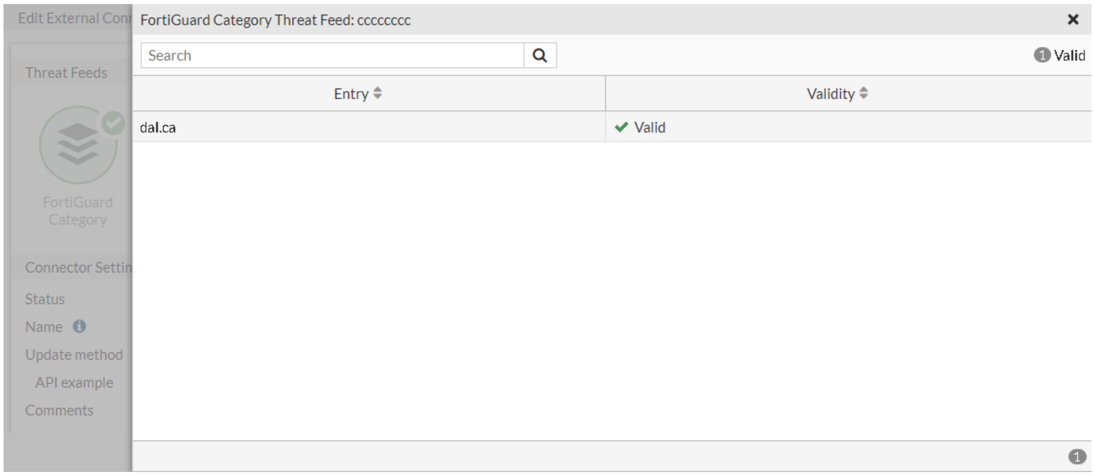
Sample cURL request: curl -k -X POST -H 'Authorization: Bearer ***************' --data '{ "commands": [{ "name": "cccccccc", "command": "snapshot", "entries": ["dal.ca"] }]}' "https://192.168.1.112/api/v2/monitor/system/external-resource/dynamic"

OK

- *Entries*: enter the entries separated by a comma (,) to be applied to the FortiGuard Category threat feed list.
- *Sample cURL request*: copy this cURL command to perform the push API update on the FortiGate against the list (*cccccccc*).

See REST API administrator in the FortiOS Administration Guide for more information.

6. Copy the content in the *Sample cURL request* field (*Add* is used in this example).
7. Click *OK*.
8. On a client, generate the API request for the threat feed.
9. Go to *Security Fabric* > *External Connectors* and edit the connector.
10. In the right-side pane, click *View Entries* to view the list of entries for the threat feed.



Edit External Con

Threat Feeds

FortiGuard Category

Connector Settin

Status

Name

Update method

API example

Comments

FortiGuard Category Threat Feed: cccccccc

Search

1 Valid

Entry	Validity
dal.ca	✓ Valid

1

To configure the threat feed in the CLI:

```
config system external-resource
    edit "cccccccc"
        set update-method push
        set category 201
    next
end
```

To use the API in the CLI:

```
# diagnose system external-resource {push-add | push-remove | push-snapshot} <feed_name>
<entry>
```

To use the API with a JSON file:

```
# diagnose sys external-resource push-api-json-commands
```

```
{
  "commands": [<array (mandatory)>
    {<object (mandatory)>
         "name": <string (mandatory)>,
      "command": <string (mandatory, "add", "remove", or "snapshot")>,
      "entries": [<array (mandatory)>
        <string (mandatory, such as "10.100.1.1")>,
      ]
    }
  ]
}
```

Sample:

```
# diagnose sys external-resource push-api-json-commands '{"commands":
[{"name":"test","command":"add","entries":["10.10.10.1","10.10.10.2"]},
{"name":"test","command":"whatever","entries":["10.10.10.3","10.10.10.4"]}]}'
command returned: EXT_RESOURCE_PUSH_CMD_RETURN_OK
Returned json:
[
  {
    "name":"test",
    "command":"add",
    "status":"success"
  },
  {
    "name":"test",
    "command":"whatever",
    "error":"Invalid command.",
    "status":"error"
  }
]
```

To use the API with a Postman REST client:

1. Create an API administrator in FortiOS with write access.
2. Ensure the API token is generated.
3. Configure the external resource list as needed.
4. In the Postman client, create a new request, set the HTTP method to *POST*, enter the URL.
5. Configure the access token using one of the following methods:
   - To use the bearer token: click the *Authorization* tab, set the *Type* to *Bearer*, and enter the REST API administrator token.
   - To use the access_token parameter: click the *Params* tab and enter the access_token key-value pair (*access_token* and <*key*>).

6. Click the *Body* tab and configure the following:
   a. Select *raw* and set the input type to *JSON*.
   b. Insert the JSON data payload.
7. Click *Send* to send the POST request. If there is a response, the response body appears. For example,

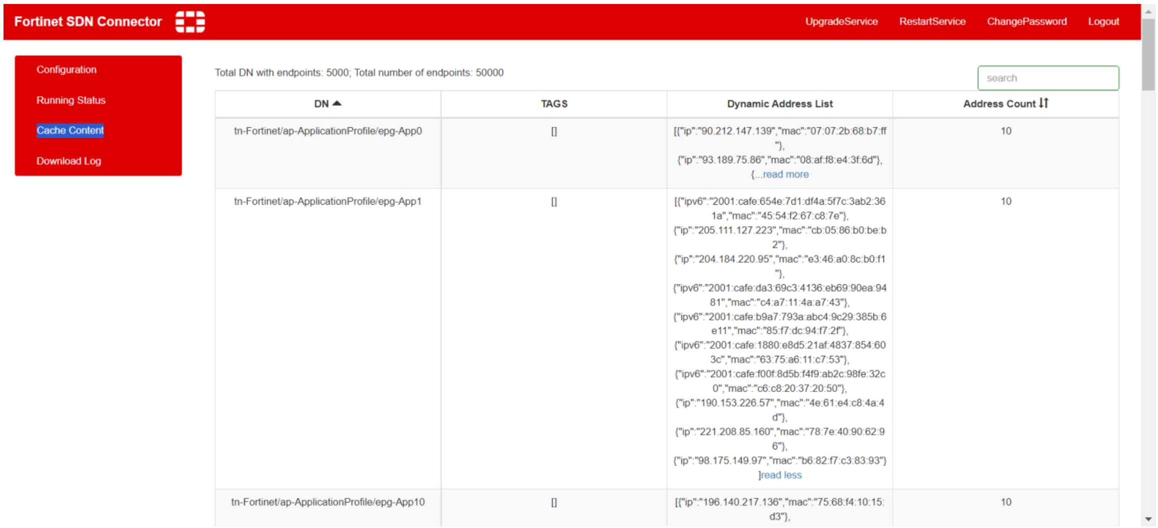
```
POST https://172.18.52.153/api/v2/monitor/system/external-resource/dynamic?access_
token=g1mnfs8bzxk5hf8Qwcz4kx7yn3jHmG&vdom=vd1
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 04e10736-190e-4119-92e1-04e91bf99c10
Host: 172.18.52.153
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 485

{
   "commands":[
      {
         "name":"ip",
         "command":"add",
         "entries":[
            "10.10.10.1",
            "10.10.10.2"
         ]
      },
      {
         "name":"fqdn",
         "command":"remove",
         "entries":[
            "10.10.10.1",
            "10.10.10.2"
         ]
      },
      {
         "name":"fortiguard",
         "command":"snapshot",
         "entries":[
            "10.10.10.1",
            "10.10.10.2"
         ]
      }
   ]
}

HTTP/1.1 200 OK
date: Fri, 22 Jul 2022 21:10:39 GMT
x-frame-options: SAMEORIGIN
content-security-policy: frame-ancestors 'self'
x-xss-protection: 1; mode=block
cache-control: no-cache, must-revalidate
content-length: 480
content-type: application/json
Connection: keep-alive

{
   "http_method":"POST",
   "results":[
      {
         "name":"ip",
         "command":"add",
         "status":"success"
      },
      {
         "name":"fqdn",
         "command":"remove",
         "status":"success"
      },
      {
         "name":"fortiguard",
         "command":"snapshot",
         "status":"success"
      }
   ],
   "vdom":"vd1",
   "path":"system",
   "name":"external-resource",
   "action":"dynamic",
   "status":"success",
   "serial":"FG6H1E5819900000",
   "version":"v7.2.1",
   "build":1254
}
```

Support IPv6 dynamic addresses retrieved from Cisco ACI SDN connector - 7.2.1

IPv6 dynamic addresses can be retrieved from Cisco ACI SDN connectors. IPv6 addresses imported from Cisco ACI to the Fortinet SDN Connector VM can be imported into the FortiGate as IPv6 dynamic addresses. The Fortinet SDN Connector VM must be running version 1.1.10 or later.

```
config firewall address6
    edit <name>
        set type dynamic
        set sdn <ACI_connector>
    next
end
```

The following example assumes the Fortinet SDN Connector VM has already connected to Cisco ACI and learned the IPv6 addresses. See Configuring the SDN Connector in the Cisco ACI Administration Guide for more information. The *Dynamic Address List* values for the DN with the filter *tn-Fortinet/ap-ApplicationProfile/epg-App1* is used in this example.



Total DN with endpoints: 5000; Total number of endpoints: 50000

DN ▲	TAGS	Dynamic Address List	Address Count ⇅
tn-Fortinet/ap-ApplicationProfile/epg-App0	[]	[{"ip":"90.212.147.139","mac":"07:07:2b:68:b7:ff"}, {"ip":"93.189.75.86","mac":"08:af:f8:e4:3f:6d"}, {...read more	10
tn-Fortinet/ap-ApplicationProfile/epg-App1	[]	[{"ipv6":"2001:cafe:654e:7d1:df4a:5f7c:3ab2:361a","mac":"45:54:f2:67:c8:7e"}, {"ip":"205.111.127.223","mac":"cb:05:86:b0:be:b2"}, {"ip":"204.184.220.95","mac":"e3:46:a0:8c:b0:f1"}, {"ipv6":"2001:cafe:da3:69c3:4136:eb69:90ea:9481","mac":"c4:a7:11:4a:a7:43"}, {"ipv6":"2001:cafe:b9a7:793a:abc4:9c29:385b:6e11","mac":"85:f7:dc:94:f7:2f"}, {"ipv6":"2001:cafe:1880:e8d5:21af:4837:854:603c","mac":"63:75:a6:11:c7:53"}, {"ipv6":"2001:cafe:f00f:8d5b:f4f9:ab2c:98fe:32c0","mac":"c6:c8:20:37:20:50"}, {"ip":"190.153.226.57","mac":"4e:61:e4:c8:4a:4d"}, {"ip":"221.208.85.160","mac":"78:7e:40:90:62:96"}, {"ip":"98.175.149.97","mac":"b6:82:f7:c3:83:93"}]read less	10
tn-Fortinet/ap-ApplicationProfile/epg-App10	[]	[{"ip":"196.140.217.136","mac":"75:68:f4:10:15:d3"},	10

To configure the Cisco ACI connector and dynamic address:

1. Configure the Cisco ACI SDN connector:

```
config system sdn-connector
    edit "aci_64.115_115"
        set type aci
        set server-list "10.6.30.115"
        set server-port 5671
        set username "admin"
        set password xxxxxxx
    next
end
```

2. Verify that the SDN connector status is up:

```
# diagnose sys sdn status "aci_64.115_115"
SDN Connector                       Type        Status
-------------------------------------------------------------
aci_64.115_115                      aci         Up
```

3. Configure the IPv6 dynamic firewall address (filters for tenant and endpoint group are used in this example):

```
config firewall address6
    edit "aci-add6-App1"
        set type dynamic
        set sdn "aci_64.115_115"
        set color 17
        set tenant "Fortinet"
        set epg-name "App1"
    next
end
```

4. Verify the list of resolved IPv6 addresses:

```
# diagnose firewall dynamic6 list "aci-add6-App1"
aci_64.115_115.aci.Fortinet.App1.*: ID(220)
        ADDR(2001:cafe:654e:7d1:df4a:5f7c:3ab2:361a)
        ADDR(2001:cafe:da3:69c3:4136:eb69:90ea:9481)
```

```
            ADDR(2001:cafe:b9a7:793a:abc4:9c29:385b:6e11)
            ADDR(2001:cafe:1880:e8d5:21af:4837:854:603c)
            ADDR(2001:cafe:f00f:8d5b:f4f9:ab2c:98fe:32c0)
```

Automation stitches

This section includes information about automation stitches related new features:

- Add new automation triggers for event logs on page 73
- Certificate expiration trigger 7.2.1 on page 76
- System automation actions to back up, reboot, or shut down the FortiGate 7.2.1 on page 79
- Enhance automation trigger to execute only once at a scheduled date and time 7.2.1 on page 83

Add new automation triggers for event logs

Six new automation triggers have been added based on event log categories:

- Anomaly logs
- IPS logs
- SSH logs
- Traffic violations
- Virus logs
- Web filter violations

When multi VDOM mode is enabled, individual VDOMs can be specified so that the trigger is only applied to those VDOMs.

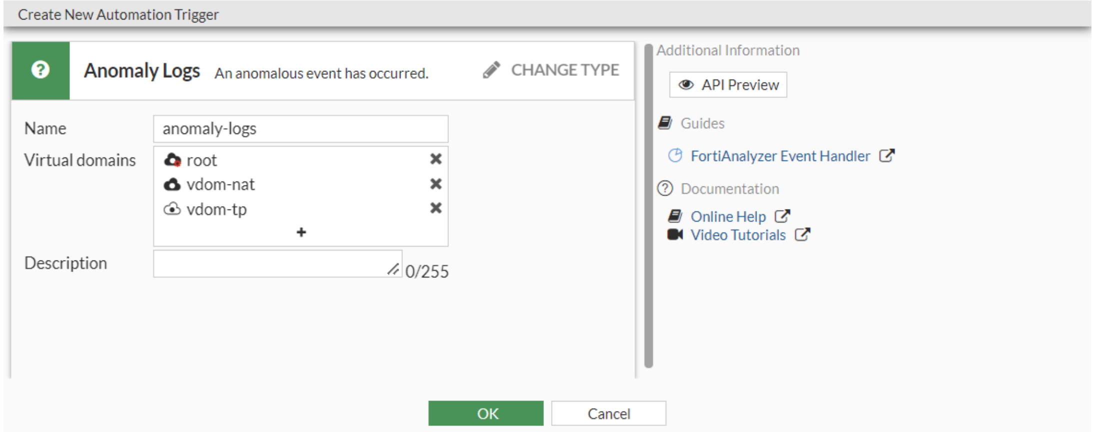
```
config system automation-trigger
    edit <name>
        set event-type {ips-logs | anomaly-logs | virus-logs | ssh-logs | webfilter-
violation | traffic-violation}
        set vdom <name>
    next
end
```

Example

In this example, an automation stitch is created that uses an anomaly logs trigger and an email notification action. The trigger specifies which VDOMs should be used. There is a three-second delay between the trigger and action.

To configure an automation stitch with the anomaly logs trigger in the GUI:

1. Configure the trigger:
    a. Go to *Security Fabric > Automation*, select the *Trigger* tab, and click *Create New*.
    b. In the *Event Log Category* section, click *Anomaly Logs*.
    c. Enter a name (*anomaly-logs*) and add the required VDOMs (*root*, *vdom-nat*, *vdom-tp*).



Create New Automation Trigger

Anomaly Logs An anomalous event has occurred.

Name: anomaly-logs

Virtual domains: root, vdom-nat, vdom-tp

Description: 0/255

   d. Click *OK*.
2. Configure the action:
   a. Go to *Security Fabric > Automation*, select the *Action* tab, and click *Create New*.
   b. In the *Notifications* section, click *Email* and enter the following:

Name	*email_default_rep_message*
To	Enter an email address
Subject	*CSF stitch alert*
Replacement message	Enable

   c. Click *OK*.
3. Configure the stitch:
   a. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
   b. Enter the name, *anomaly-logs-stitch*.
   c. Click *Add Trigger*. Select *anomaly-logs* and click *Apply*.
   d. Click *Add Action*. Select *email_default_rep_message* and click *Apply*.
   e. Click *Add delay* (between the trigger and action). Enter *3* and click *OK*.
   f. Click *OK*.

To configure an automation stitch with the anomaly logs trigger in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "anomaly-logs"
        set event-type anomaly-logs
        set vdom "root" "vdom-nat" "vdom-tp"
    next
end
```

2. Configure the action:

```
config system automation-action
    edit "email_default_rep_message"
        set action-type email
        set email-to "admin@fortinet.com"
```

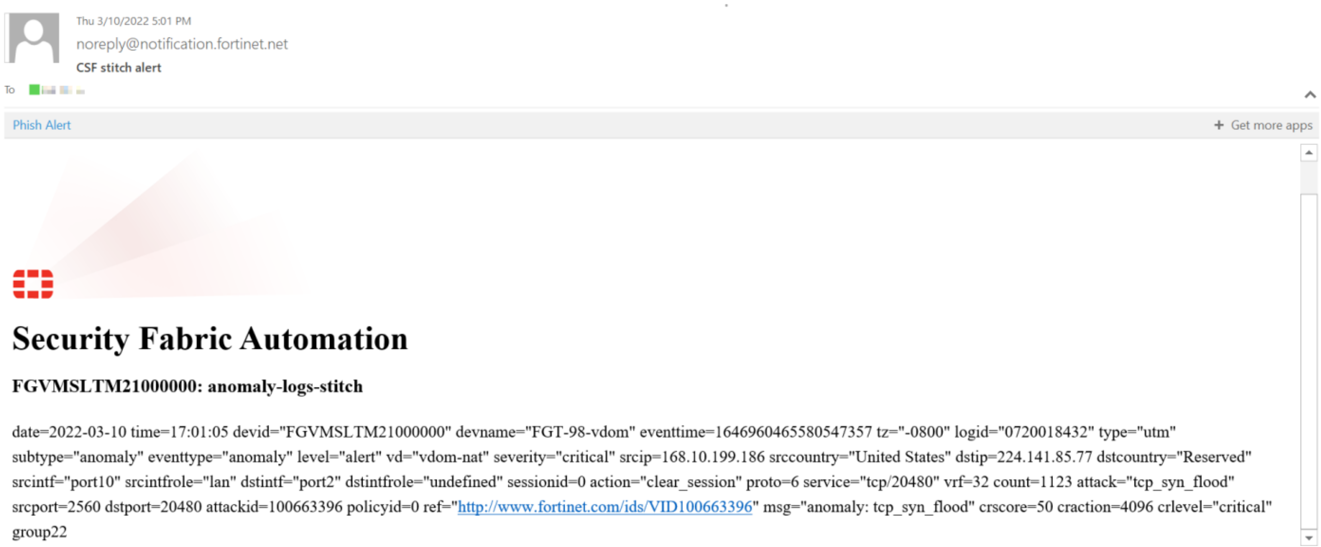
```
            set email-subject "CSF stitch alert"
            set replacement-message enable
        next
    end
```

3. Configure the stitch:

```
    config system automation-stitch
        edit "anomaly-logs-stitch"
            set description "anomaly-logs"
            set trigger "anomaly-logs"
            config actions
                edit 1
                    set action "email_default_rep_message"
                    set delay 3
                    set required enable
                next
            end
        next
    end
```

Verification

Once the anomaly log is generated, the automation stitch is triggered end the email notification is sent.



Thu 3/10/2022 5:01 PM

noreply@notification.fortinet.net

CSF stitch alert

To [redacted]

Security Fabric Automation

FGVMSLTM21000000: anomaly-logs-stitch

date=2022-03-10 time=17:01:05 devid="FGVMSLTM21000000" devname="FGT-98-vdom" eventtime=1646960465580547357 tz="-0800" logid="0720018432" type="utm" subtype="anomaly" eventtype="anomaly" level="alert" vd="vdom-nat" severity="critical" srcip=168.10.199.186 srccountry="United States" dstip=224.141.85.77 dstcountry="Reserved" srcintf="port10" srcintfrole="lan" dstintf="port2" dstintfrole="undefined" sessionid=0 action="clear_session" proto=6 service="tcp/20480" vrf=32 count=1123 attack="tcp_syn_flood" srcport=2560 dstport=20480 attackid=100663396 policyid=0 ref="http://www.fortinet.com/ids/VID100663396" msg="anomaly: tcp_syn_flood" crscore=50 craction=4096 crlevel="critical" group22

To confirm that the stitch was triggered in the GUI:

1. Go to *Security Fabric* > *Automation* and select the *Stitch* tab.
2. Verify the *Last Triggered* column.

To confirm that the stitch was triggered in the CLI:

```
# diagnose test application autod 2
...
stitch: anomaly-logs-stitch
        destinations: all
        trigger: anomaly-logs
```

```
                type:anomaly logs

                field ids:
                        (id:6)vd=root,vdom-nat,vdom-tp

        local hit: 1 relayed to: 0 relayed from: 0
        actions:
                email_default_rep_message type:email interval:0
                        delay:3 required:yes
                        subject: CSF stitch alert
                        body: %%log%%
                        sender:
                        mailto:admin@fortinet.com;
```

Certificate expiration trigger - 7.2.1

The local certificate expiry trigger (`local-certificate-near-expiry`) can be used in an automation stitch if a user-supplied local certificate used for SSL VPN, deep inspection, or other purpose is about to expire. This trigger relies on a VPN certificate setting in the CLI configuration setting for the certificate log expiring warning threshold:

```
config vpn certificate setting
    set cert-expire-warning <integer>
end
```

`cert-expire-warning <integer>`	Set the certificate log expiring warning threshold, in days (0 - 100, default = 14).

Example

In this example, the local certificate expiry trigger is used with an email notification action to remind an administrator to re-sign or load a new local certificate to avoid any service interruptions. The local certificate, fw-cert-30-days, will expire in 30 days. The certificate log expiring warning threshold is set to 31 days.

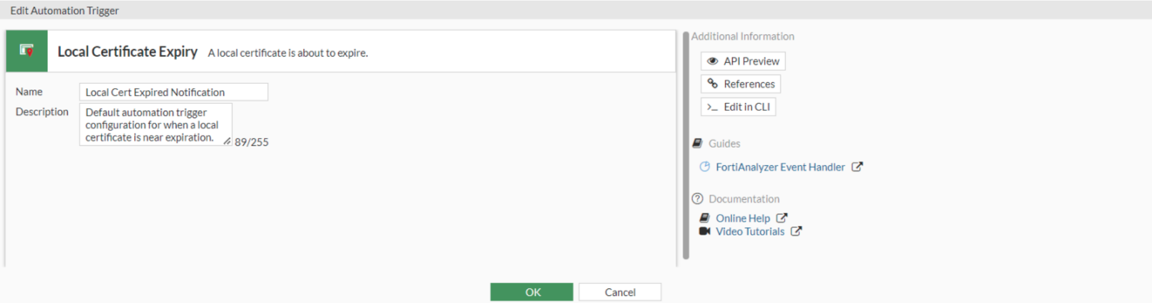
To configure the certificate log expiring warning threshold:

```
config vpn certificate setting
    set cert-expire-warning 31
end
```

To configure an automation stitch with the local certificate expiry trigger in the GUI:

1. Configure the trigger:
   a. Go to *Security Fabric > Automation*, select the *Trigger* tab, and click *Create New*.
   b. In the *System* section, click *Local Certificate Expiry*, and enter the following:

Name	*Local Cert Expired Notification*
Description	*Default automation trigger configuration for when a local certificate is near expiration.*



Edit Automation Trigger

Local Certificate Expiry A local certificate is about to expire.

Name: Local Cert Expired Notification

Description: Default automation trigger configuration for when a local certificate is near expiration. 89/255

   c. Click *OK*.

2. Configure the action:
   a. Go to *Security Fabric* > *Automation*, select the *Action* tab, and click *Create New*.
   b. In the *Notifications* section, click *Email*, and enter the following:

Name	*email_no_rep_message*
To	Enter an email address.
Subject	*CSF stitch alert*

   c. Click *OK*.

3. Configure the stitch:
   a. Go to *Security Fabric* > *Automation*, select the *Stitch* tab, and click *Create New*.
   b. Enter the name, *cert-expiry*.
   c. Click *Add Trigger*. Select *Local Cert Expired Notification* and click *Apply*.
   d. Click *Add Action*. Select *email_no_rep_message* and click *Apply*.
   e. Click *OK*.

To configure an automation stitch with the local certificate expiry trigger in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "Local Cert Expired Notification"
        set description "Default automation trigger configuration for when a local
certificate is near expiration."
        set event-type local-cert-near-expiry
    next
end
```

2. Configure the action:

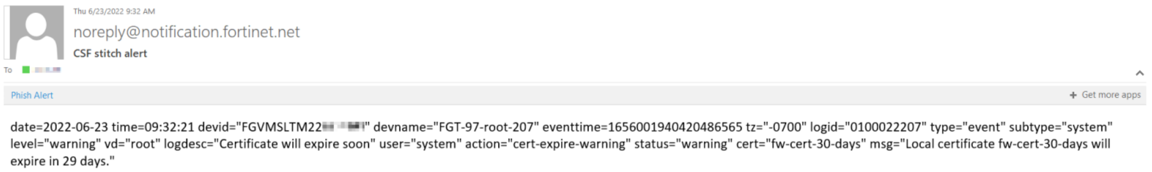
```
config system automation-action
    edit "email_no_rep_message"
        set action-type email
        set email-to "*******@fortinet.com"
        set email-subject "CSF stitch alert"
    next
end
```

3. Configure the stitch:

```
config system automation-stitch
    edit "cert-expiry"
        set trigger "Local Cert Expired Notification"
        config actions
            edit 1
                set action "email_no_rep_message"
                set required enable
            next
        end
    next
end
```

Verification

Once the event log is generated for the local certificate expiry, the automation stitch is triggered end the email notification is sent.



Thu 6/23/2022 9:32 AM

noreply@notification.fortinet.net

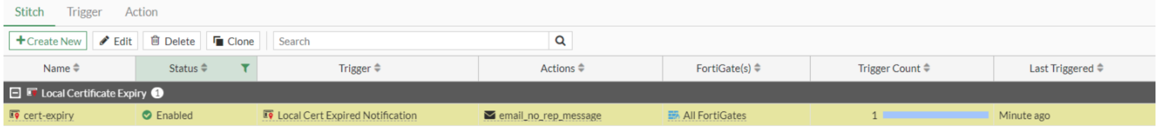
CSF stitch alert

To [redacted]

date=2022-06-23 time=09:32:21 devid="FGVMSLTM22[redacted]" devname="FGT-97-root-207" eventtime=1656001940420486565 tz="-0700" logid="0100022207" type="event" subtype="system" level="warning" vd="root" logdesc="Certificate will expire soon" user="system" action="cert-expire-warning" status="warning" cert="fw-cert-30-days" msg="Local certificate fw-cert-30-days will expire in 29 days."

To confirm that the stitch was triggered in the GUI:

1. Go to *Security Fabric* > *Automation* and select the *Stitch* tab.
2. Verify the *Last Triggered* column.



Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
Local Certificate Expiry 1						
cert-expiry	Enabled	Local Cert Expired Notification	email_no_rep_message	All FortiGates	1	Minute ago

To confirm that the stitch was triggered in the CLI:

```
# diagnose test application autod 3
alert mail log count: 0

stitch: cert-expiry

        local hit: 1 relayed to: 0 relayed from: 0
        last trigger:Thu Jun 23 09:32:21 2022
        last relay:
        actions:
                email_no_rep_message:
                        done: 1 relayed to: 0 relayed from: 0
                        last trigger:Thu Jun 23 09:32:21 2022
                        last relay:

logid to stitch mapping:
id:22207  local hit: 1 relayed hits: 0
        cert-expiry
```

System automation actions to back up, reboot, or shut down the FortiGate - 7.2.1

The *System Action* automation action can be used to back up the configuration of the FortiGate, reboot the FortiGate, or shut down the FortiGate.

These actions can occur even if the FortiGate is in conserve mode, and allows the automation stitch to bypass the CLI user confirmation prompts, which the CLI script action does not support.

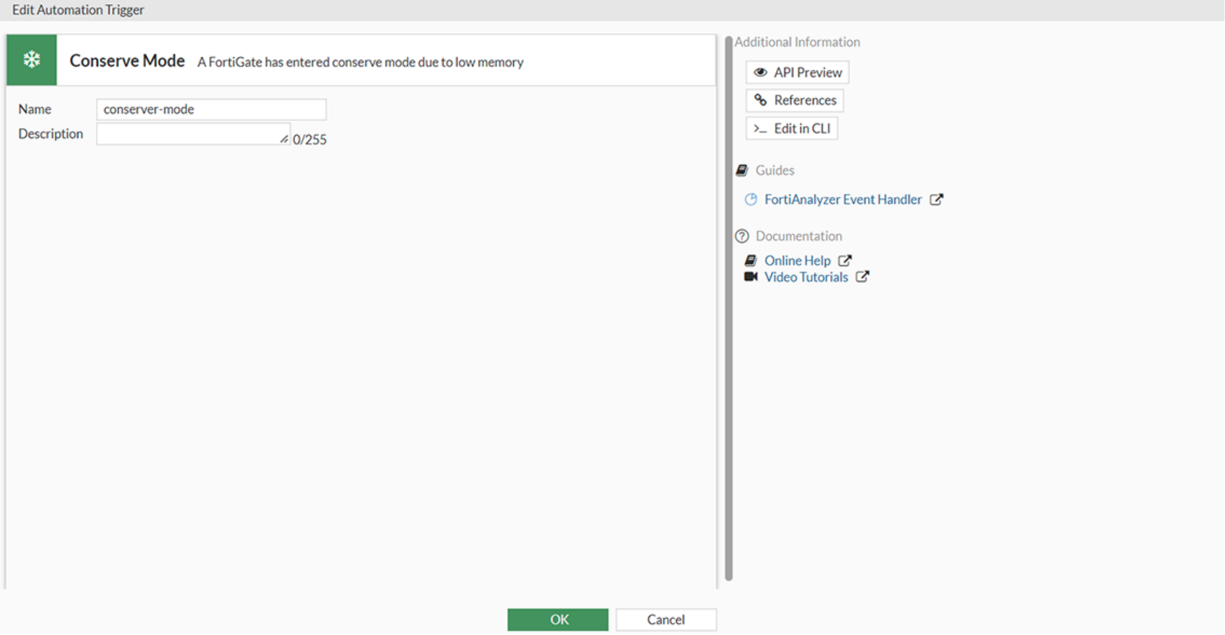
```
config system automation-action
    edit <name>
        set action-type system-actions
        set system-action {reboot | shutdown | backup-config}
    next
end
```

Example

In this example, an automation stitch is created that uses a `low-memory` event trigger, a `backup-config` action to back up the configuration to the FortiGate's disk, and then a `reboot` action to reboot the FortiGate. There is a 120-second delay between the two actions.

To configure an automation stitch with system actions in the GUI:

1. Configure the trigger:
   a. Go to *Security Fabric > Automation*, select the *Trigger* tab, and click *Create New*.
   b. In the *System* section, click *Conserve Mode*.
   c. Enter a name (*conserver-mode*).



Edit Automation Trigger

Conserve Mode A FortiGate has entered conserve mode due to low memory

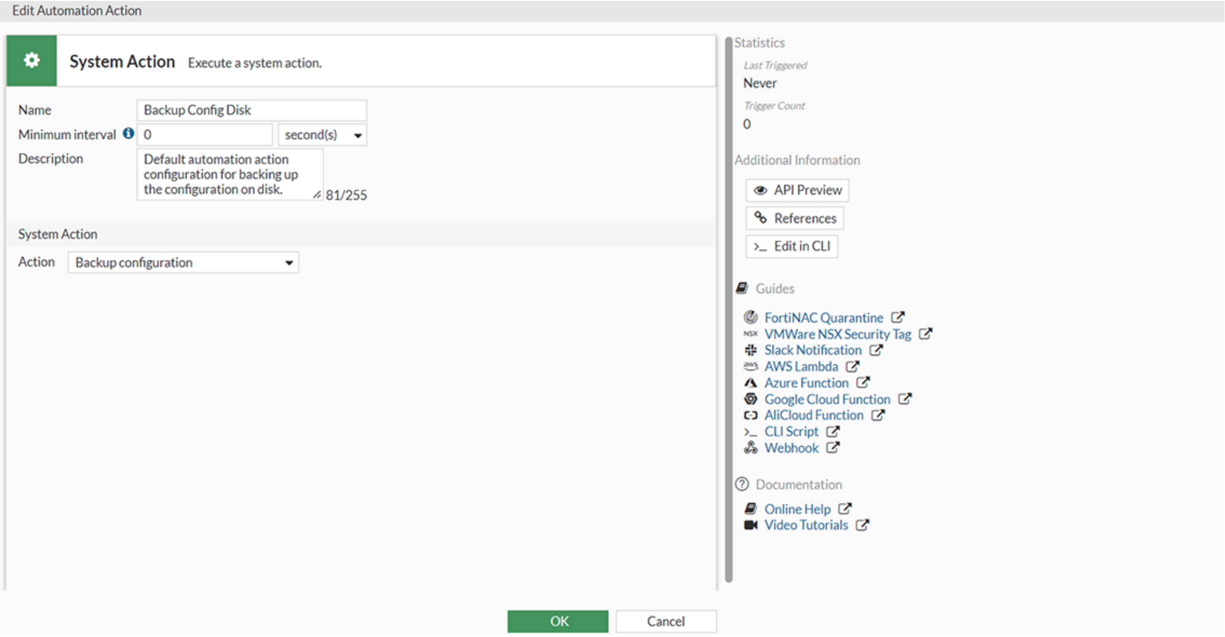
Name: conserver-mode

Description: 0/255

   d. Click *OK*.

2. Configure the back up action:
   a. Go to *Security Fabric > Automation*, select the *Action* tab, and click *Create New*.
   b. In the *General* section, click *System Action* and enter the following:

Name	*Backup Config Disk*
Description	*Default automation action configuration for backing up the configuration on disk.*
Action	*Backup configuration*



Edit Automation Action

System Action Execute a system action.

Name	Backup Config Disk
Minimum interval	0 second(s)
Description	Default automation action configuration for backing up the configuration on disk. 81/255

System Action

Action	Backup configuration

Statistics

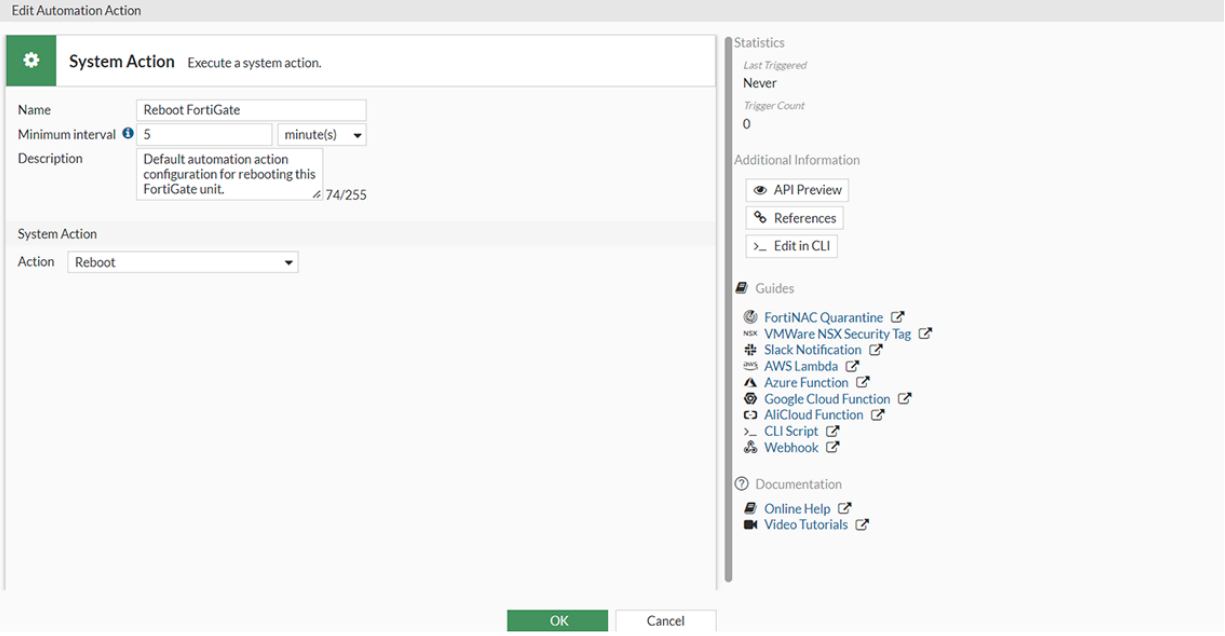
Last Triggered: Never

Trigger Count: 0

   c. Click *OK*.

3. Configure the reboot action:
   a. Go to *Security Fabric > Automation*, select the *Action* tab, and click *Create New*.
   b. In the *General* section, click *System Action* and enter the following:

Name	*Reboot FortiGate*
Description	*Default automation action configuration for rebooting this FortiGate unit.*
Action	*Reboot*
Minimum interval	*5 minutes*



Edit Automation Action

System Action Execute a system action.

Name: Reboot FortiGate

Minimum interval: 5 minute(s)

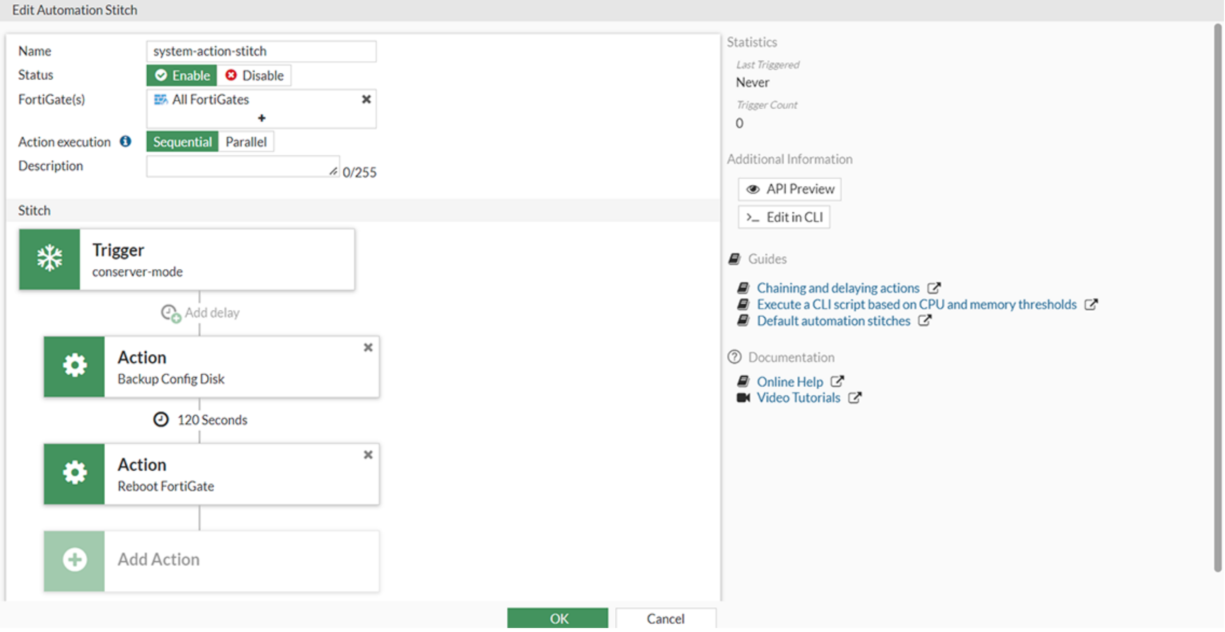
Description: Default automation action configuration for rebooting this FortiGate unit. 74/255

System Action

Action: Reboot

   c. Click *OK*.

4. Configure the stitch:
   a. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
   b. Enter the name, *system-action-stitch*.
   c. Click *Add Trigger*. Select *conserver-mode* and click *Apply*.
   d. Click *Add Action*. Select *Backup Config Disk* and click *Apply*.
   e. Click *Add Action*. Select *Reboot FortiGate* and click *Apply*.
   f. Click *Add delay* (between the actions). Enter *120* and click *OK*.



Edit Automation Stitch

Name: system-action-stitch

Status: Enable Disable

FortiGate(s): All FortiGates

Action execution: Sequential Parallel

Description: 0/255

Stitch

Trigger: conserver-mode

Action: Backup Config Disk

120 Seconds

Action: Reboot FortiGate

   g. Click *OK*.

To configure an automation stitch with system actions in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "conserver-mode"
        set event-type low-memory
    next
end
```

2. Configure the back up and reboot actions:

```
config system automation-action
    edit "Backup Config Disk"
        set description "Default automation action configuration for backing up the
configuration on disk."
        set action-type system-actions
        set system-action backup-config
    next
    edit "Reboot FortiGate"
        set description "Default automation action configuration for rebooting this
FortiGate unit."
        set action-type system-actions
        set system-action reboot
        set minimum-interval 300
    next
end
```

3. Configure the stitch:

```
config system automation-stitch
    edit "system-action-stitch"
        set trigger "conserver-mode"
        config actions
            edit 1
                set action "Backup Config Disk"
                set required enable
            next
            edit 2
                set action "Reboot FortiGate"
                set delay 120
                set required enable
            next
        end
    next
end
```

Verification

When the FortiGate enters conserve mode due to low memory, the automation stitch will be triggered and it will back up the configuration to the FortiGate disk, then reboot the FortiGate.

To confirm that the stitch was triggered in the GUI:

1. Go to *Security Fabric* > *Automation* and select the *Stitch* tab.
2. Verify the *Last Triggered* column.

To confirm that the stitch was triggered in the CLI:

```
# diagnose test application autod 3
alert mail log count: 0

stitch: system-action-stitch

    local hit: 1 relayed to: 0 relayed from: 0
    last trigger:Thu Jun 23 11:31:25 2022
    last relay:
    actions:
        Backup Config Disk:
            done: 1 relayed to: 0 relayed from: 0
            last trigger:Thu Jun 23 11:31:25 2022
            last relay:
        Reboot FortiGate:
            done: 0 relayed to: 0 relayed from: 0
            last trigger:Thu Jun 23 11:31:25 2022
            last relay:

logid to stitch mapping:
id:22011  local hit: 1 relayed hits: 0
    system-action-stitch

log category to stitch mapping:
```

To locate the backed up configuration in the GUI:

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration* > *Revisions*.
2. Click the + in the table to expand and view more details.

To locate the backed up configuration in the CLI:

```
# execute revision list config
Last Firmware Version: V0.0.0-build000-REL0
1   2022-04-01 09:27:26    daemon_admin      V7.2.0-build1157-REL0      Automatic backup
(upgrade)
2   2022-06-20 13:41:02    daemon_admin      V7.2.1-build1254-REL0      Automatic backup
(upgrade)
3   2022-06-23 11:31:25    daemon_admin      V7.2.1-build1254-REL0      Autod backup config
by stitch: system-action-stitch
```

Enhance automation trigger to execute only once at a scheduled date and time - 7.2.1

The *Schedule* automation trigger has been updated to allow one-time triggers that occur only once at a specified date and time. This trigger can be used to support one-time automation actions, including one-time configuration backup to a disk, a reboot, or a shutdown.

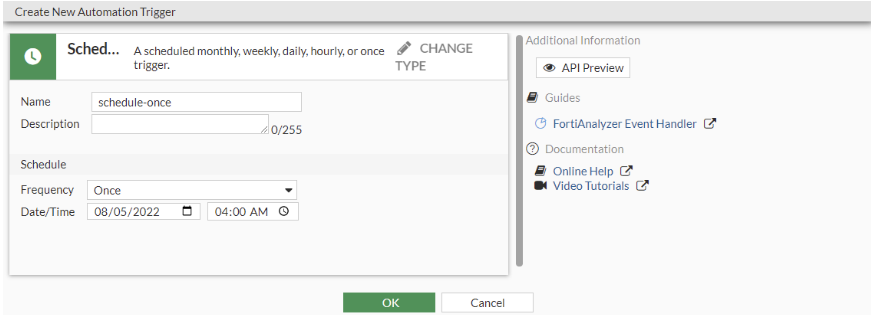
```
config system automation-trigger
    edit <name>
        set trigger-type scheduled
        set trigger-frequency once
        set trigger-datetime <YYYY-MM-DD HH:MM:SS>
    next
end
```

Example

In this example, an automation stitch is created to trigger a one-time configuration backup to a disk. The backup will occur August 5, 2022 at 4:00 AM.

To schedule a one-time automation stitch in the GUI:

1. Configure the trigger:
    a. Go to *Security Fabric > Automation*, select the *Trigger* tab, and click *Create New*.
    b. In the *Miscellaneous* section, click *Schedule*.
    c. Enter a name (*schedule-once*) in the *Name* field.
    d. In the *Frequency* dropdown list, select *Once*.
    e. Select when the trigger will occur in the *Date/Time* fields.



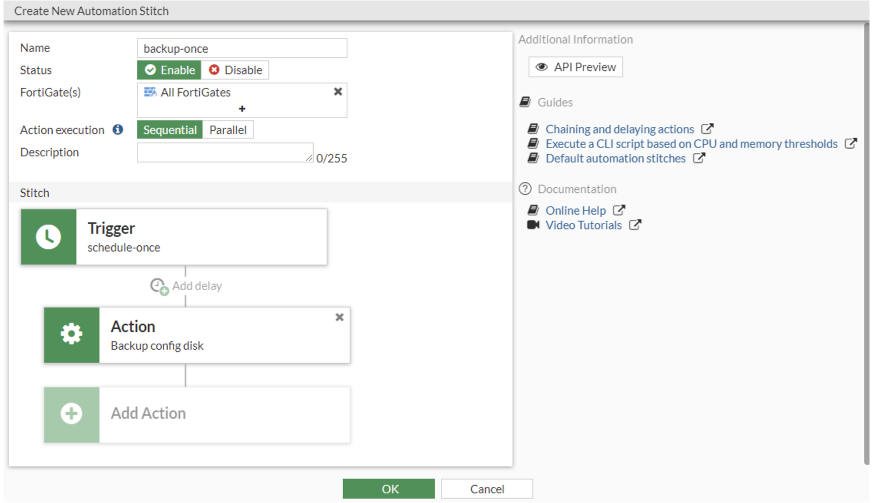
Create New Automation Trigger

Sched... A scheduled monthly, weekly, daily, hourly, or once trigger.

Name: schedule-once
Description: 0/255

Schedule
Frequency: Once
Date/Time: 08/05/2022 04:00 AM

    f. Click *OK*.
2. Configure the action:
    a. Go to *Security Fabric > Automation*, select the *Action* tab, and click *Create New*.
    b. In the *General* section, click *System Action*.
    c. Enter a name (*Backup config disk*) and an action description.
    d. In the *Action* dropdown list, select *Backup configuration*.
    e. Click *OK*.
3. Configure the stitch:
    a. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
    b. Enter the name, *backup-once*.
    c. Click *Add Trigger*. Select *schedule-once* and click *Apply*.
    d. Click *Add Action*. Select *Backup config disk* and click *Apply*.



Create New Automation Stitch

Name: backup-once

Status: Enable

FortiGate(s): All FortiGates

Action execution: Sequential

Description: 0/255

Stitch

Trigger: schedule-once

Action: Backup config disk

e. Click *OK*. The backup configuration will occur once at the date and time you set.

To schedule a one-time automation stitch in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "schedule-once"
        set trigger-type scheduled
        set trigger-frequency once
        set trigger-datetime 2022-08-05 04:00:00
    next
end
```

2. Configure the action:

```
config system automation-action
    edit "Backup config disk"
        set description "Default automation action configuration for backing up the
configuration on disk."
        set action-type system-actions
        set system-action backup-config
    next
end
```

3. Configure the stitch:

```
config system automation-stitch
    edit "backup-once"
        set trigger "schedule-once"
        config actions
            edit 1
                set action "Backup config disk"
                set required enable
            next
        end
    next
end
```

4. To view automation stitch information:

```
# diagnose test application autod 3
stitch: backup-once (scheduled)

        local hit: 0 relayed to: 0 relayed from: 0
        last trigger:   last relay:
        next scheduled trigger:Fri Aug  5 05:00:00 2022
        actions:
                backup config disk:
                        done: 0 relayed to: 0 relayed from: 0
                        last trigger:                   last relay:

logid to stitch mapping:
id:0 (scheduled stitches) local hit: 0 relayed hits: 0
        backup-once
```

Security ratings

This section includes information about security rating related new features:

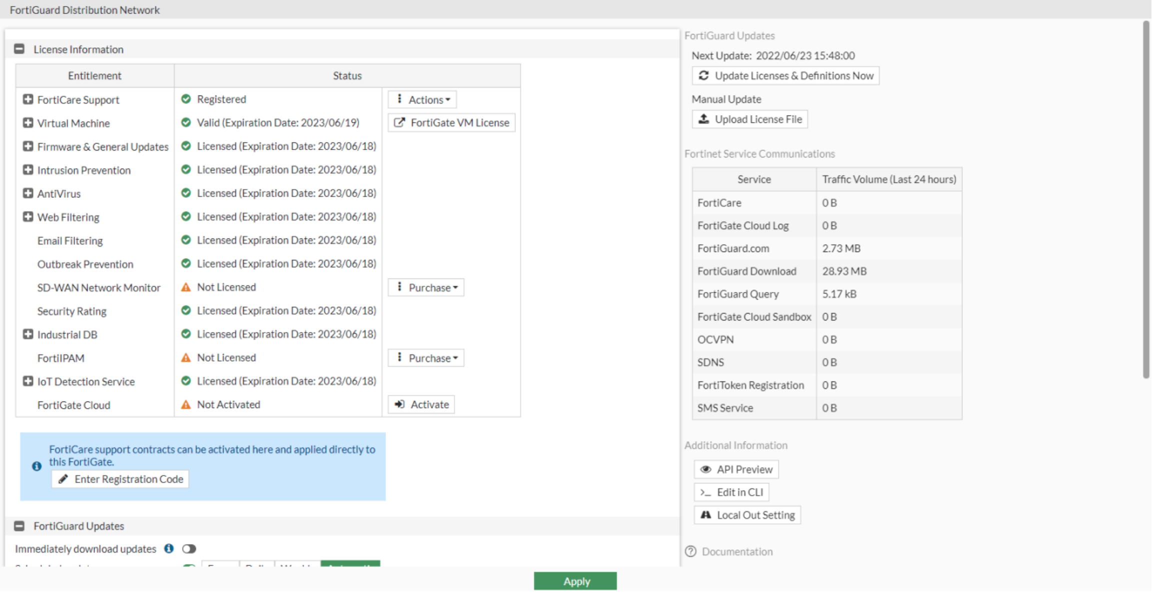
- Add PSIRT vulnerabilities to security ratings and notifications for critical vulnerabilities found on Fabric devices 7.2.1 on page 86

Add PSIRT vulnerabilities to security ratings and notifications for critical vulnerabilities found on Fabric devices - 7.2.1

On a FortiGate with a valid Security Rating license, the separate Security Rating package downloaded from FortiGuard supports PSIRT vulnerabilities, which are highlighted in security rating results.

To verify the FortiGuard license entitlement in the GUI:

1. Go to *System* > *FortiGuard* and expand the *License Information* table.
2. Check that *Security Rating* appears in the list and the license is valid.



FortiGuard Distribution Network

License Information

Entitlement	Status	
FortiCare Support	Registered	Actions
Virtual Machine	Valid (Expiration Date: 2023/06/19)	FortiGate VM License
Firmware & General Updates	Licensed (Expiration Date: 2023/06/18)	
Intrusion Prevention	Licensed (Expiration Date: 2023/06/18)	
AntiVirus	Licensed (Expiration Date: 2023/06/18)	
Web Filtering	Licensed (Expiration Date: 2023/06/18)	
Email Filtering	Licensed (Expiration Date: 2023/06/18)	
Outbreak Prevention	Licensed (Expiration Date: 2023/06/18)	
SD-WAN Network Monitor	Not Licensed	Purchase
Security Rating	Licensed (Expiration Date: 2023/06/18)	
Industrial DB	Licensed (Expiration Date: 2023/06/18)	
FortiIPAM	Not Licensed	Purchase
IoT Detection Service	Licensed (Expiration Date: 2023/06/18)	
FortiGate Cloud	Not Activated	Activate

FortiCare support contracts can be activated here and applied directly to this FortiGate.

FortiGuard Updates

Immediately download updates

FortiGuard Updates

Next Update: 2022/06/23 15:48:00

Manual Update

Fortinet Service Communications

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiGate Cloud Log	0 B
FortiGuard.com	2.73 MB
FortiGuard Download	28.93 MB
FortiGuard Query	5.17 kB
FortiGate Cloud Sandbox	0 B
OCVPN	0 B
SDNS	0 B
FortiToken Registration	0 B
SMS Service	0 B

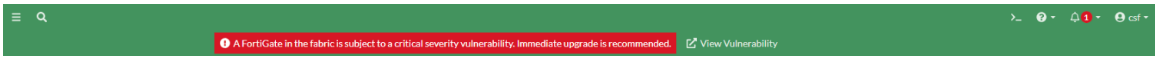
Additional Information

To verify the FortiGuard license entitlement in the CLI:

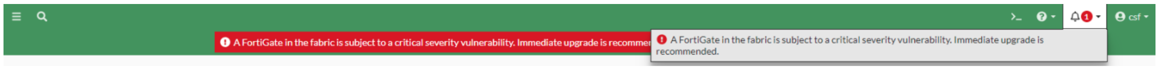
```
# diagnose autoupdate versions
...
Security Rating Data Package
---------
Version: 4.00008
Contract Expiry Date: Sun Jun 18 2023
Last Updated using scheduled update on Thu Jun 23 15:48:13 2022
Last Update Attempt: Thu Jun 23 15:48:13 2022
Result: Updates Installed

FDS Address
---------
173.243.140.6:443
```

GUI notifications

If the security rating result indicates a vulnerability with a critical severity, then the FortiOS GUI displays a warning message in the header and a new notification under the bell icon. The *View Vulnerability* link appears in the header for global administrators.



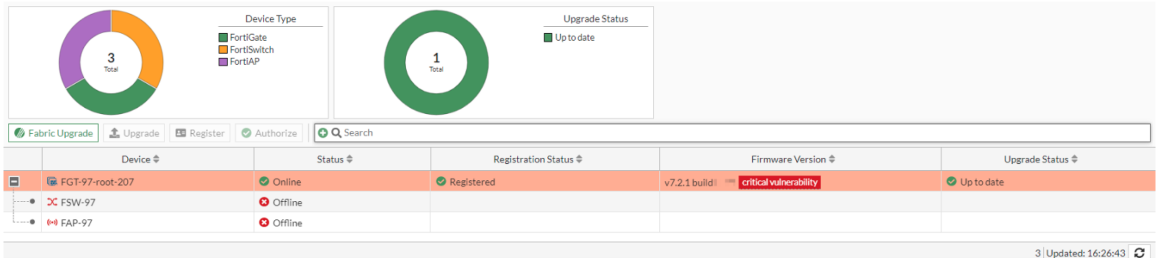
A FortiGate in the fabric is subject to a critical severity vulnerability. Immediate upgrade is recommended.



A FortiGate in the fabric is subject to a critical severity vulnerability. Immediate upgrade is recommen

A FortiGate in the fabric is subject to a critical severity vulnerability. Immediate upgrade is recommended.

Clicking the warning message redirects to the *System* > *Fabric Management* page, where users are encouraged to update any affected Fortinet Fabric devices to the latest firmware releases to resolve the critical vulnerabilities.

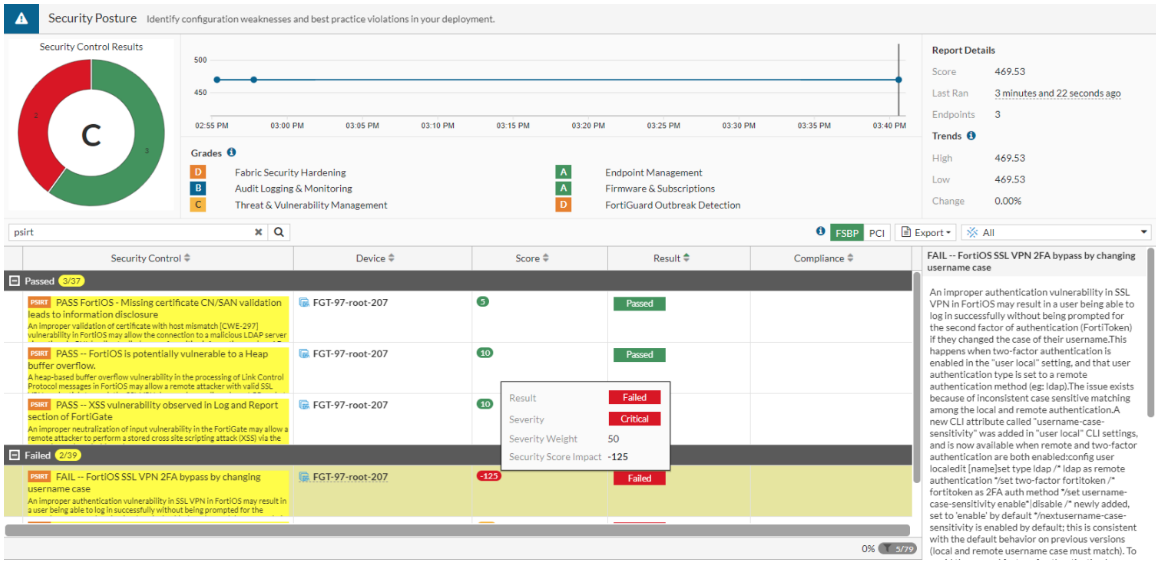


	Device	Status	Registration Status	Firmware Version	Upgrade Status
⊟	FGT-97-root-207	Online	Registered	v7.2.1 build[redacted] critical vulnerability	Up to date
	FSW-97	Offline			
	FAP-97	Offline			

3 Updated: 16:26:43

Security Rating page

When a failed result is selected, the security panel provides a description of the PSIRT vulnerability for failed results.



Grades

D	Fabric Security Hardening	A	Endpoint Management
B	Audit Logging & Monitoring	A	Firmware & Subscriptions
C	Threat & Vulnerability Management	D	FortiGuard Outbreak Detection

Report Details

Score	469.53
Last Ran	3 minutes and 22 seconds ago
Endpoints	3

Trends

High	469.53
Low	469.53
Change	0.00%

psirt

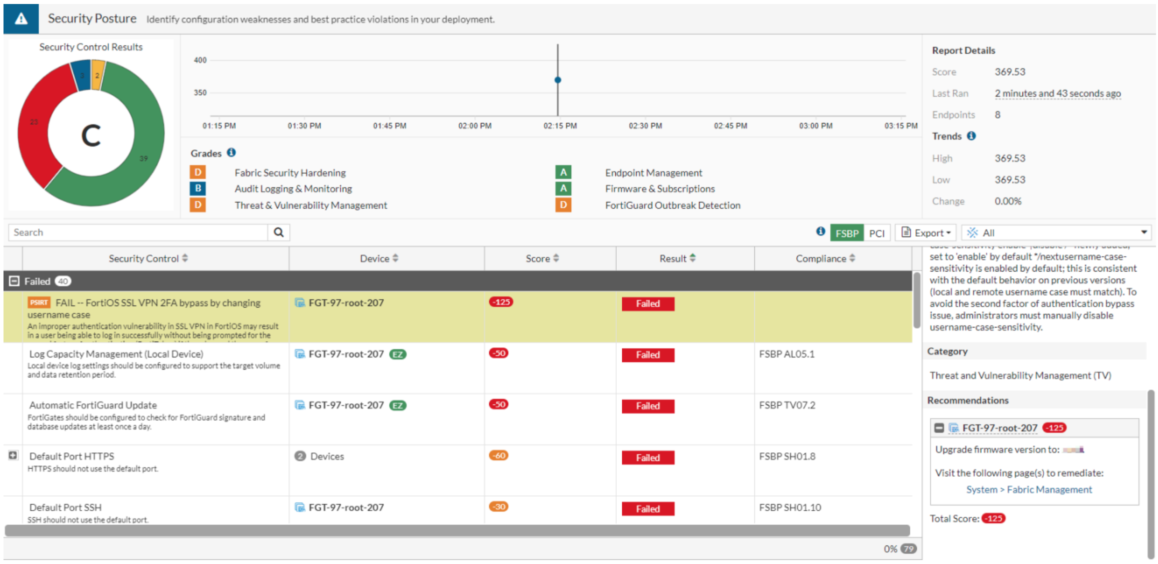
Security Control	Device	Score	Result	Compliance
Passed 3/37				
PSIRT PASS FortiOS - Missing certificate CN/SAN validation leads to information disclosure An improper validation of certificate with host mismatch [CWE-297] vulnerability in FortiOS may allow the connection to a malicious LDAP server	FGT-97-root-207	5	Passed	
PSIRT PASS -- FortiOS is potentially vulnerable to a Heap buffer overflow. A heap-based buffer overflow vulnerability in the processing of Link Control Protocol messages in FortiOS may allow a remote attacker with valid SSL	FGT-97-root-207	10	Passed	
PSIRT PASS -- XSS vulnerability observed in Log and Report section of FortiGate An improper neutralization of input vulnerability in the FortiGate may allow a remote attacker to perform a stored cross site scripting attack (XSS) via the	FGT-97-root-207	10		
Failed 2/39				
PSIRT FAIL -- FortiOS SSL VPN 2FA bypass by changing username case An improper authentication vulnerability in SSL VPN in FortiOS may result in a user being able to log in successfully without being prompted for the	FGT-97-root-207	-125	Failed	

Result	Failed
Severity	Critical
Severity Weight	50
Security Score Impact	-125

FAIL -- FortiOS SSL VPN 2FA bypass by changing username case

An improper authentication vulnerability in SSL VPN in FortiOS may result in a user being able to log in successfully without being prompted for the second factor of authentication (FortiToken) if they changed the case of their username.This happens when two-factor authentication is enabled in the "user local" setting, and that user authentication type is set to a remote authentication method (eg: ldap).The issue exists because of inconsistent case sensitive matching among the local and remote authentication.A new CLI attribute called "username-case-sensitivity" was added in "user local" CLI settings, and is now available when remote and two-factor authentication are both enabled:config user localedit [name]set type ldap /* ldap as remote authentication */set two-factor fortitoken /* fortitoken as 2FA auth method */set username-case-sensitivity enable*|disable /* newly added, set to 'enable' by default */nextusername-case-sensitivity is enabled by default; this is consistent with the default behavior on previous versions (local and remote username case must match). To

The *Recommendations* section includes a link to the *System* > *Fabric Management* page to update the firmware.



Grades

D	Fabric Security Hardening	A	Endpoint Management
B	Audit Logging & Monitoring	A	Firmware & Subscriptions
D	Threat & Vulnerability Management	D	FortiGuard Outbreak Detection

Report Details

Score	369.53
Last Ran	2 minutes and 43 seconds ago
Endpoints	8

Trends

High	369.53
Low	369.53
Change	0.00%

Search

Security Control	Device	Score	Result	Compliance
Failed 40				
PSIRT FAIL -- FortiOS SSL VPN 2FA bypass by changing username case An improper authentication vulnerability in SSL VPN in FortiOS may result in a user being able to log in successfully without being prompted for the	FGT-97-root-207	-125	Failed	
Log Capacity Management (Local Device) Local device log settings should be configured to support the target volume and data retention period.	FGT-97-root-207 EZ	-50	Failed	FSBP AL05.1
Automatic FortiGuard Update FortiGates should be configured to check for FortiGuard signature and database updates at least once a day.	FGT-97-root-207 EZ	-50	Failed	FSBP TV07.2
⊞ Default Port HTTPS HTTPS should not use the default port.	2 Devices	-60	Failed	FSBP SH01.8
Default Port SSH SSH should not use the default port.	FGT-97-root-207	-30	Failed	FSBP SH01.10

set to 'enable' by default */nextusername-case-sensitivity is enabled by default; this is consistent with the default behavior on previous versions (local and remote username case must match). To avoid the second factor of authentication bypass issue, administrators must manually disable username-case-sensitivity.

Category

Threat and Vulnerability Management (TV)

Recommendations

FGT-97-root-207 -125

Upgrade firmware version to: [redacted]

Visit the following page(s) to remediate:

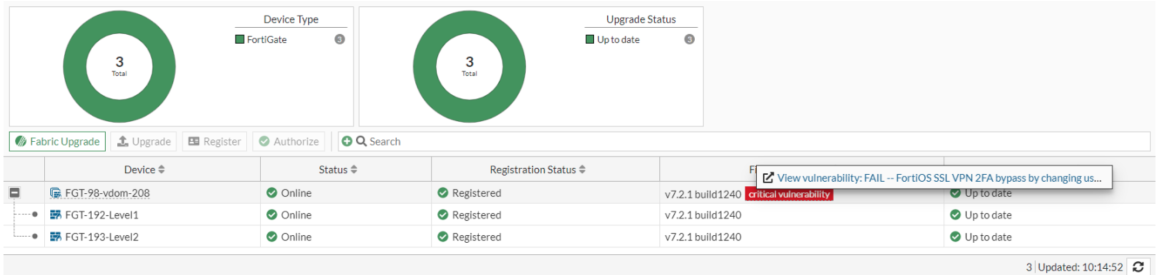
System > Fabric Management

Total Score: -125

In the search bar, use PSIRT keywords to filter for PSIRT vulnerabilities.

Tooltip

A tooltip for the *critical vulnerability* label on the *System > Fabric Management* page lists the vulnerability, and it links to the *Security Fabric > Security Rating* page where more details about the vulnerability are displayed.



Device	Status	Registration Status	F	
FGT-98-vdom-208	✓ Online	✓ Registered	v7.2.1 build1240 critical vulnerability	✓ Up to date
FGT-192-Level1	✓ Online	✓ Registered	v7.2.1 build1240	✓ Up to date
FGT-193-Level2	✓ Online	✓ Registered	v7.2.1 build1240	✓ Up to date

Network

This section includes information about network related new features:

SD-WAN

This section includes information about SD-WAN related new features:

Allow application category as an option for SD-WAN rule destination

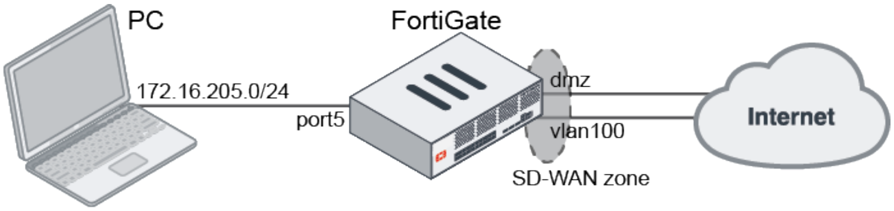
An application category can be selected as an SD-WAN service rule destination criterion. Previously, only application groups or individual applications could be selected.

```
config system sdwan
    config service
        edit <id>
            set internet-service enable
            set internet-service-app-ctrl-category <id_1> <id_2> ... <id_n>
        next
    end
end
```

To view the detected application categories details based on category ID, use `diagnose sys sdwan internet-service-app-ctrl-category-list <id>`.

Example

In this example, traffic steering is applied to traffic detected as video/audio (category ID 5) or email (category ID 21) and applies the lowest cost (SLA) strategy to this traffic. When costs are tied, the priority goes to member 1, dmz.



To configure application categories as an SD-WAN rule destination in the CLI:

1. Configure the SD-WAN settings:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "dmz"
            set gateway 172.16.208.2
        next
        edit 2
            set interface "vlan100"
            set gateway 172.16.206.2
        next
    end
    config health-check
        edit "1"
            set server "8.8.8.8"
            set protocol dns
            set members 0
            config sla
                edit 1
                next
            end
        next
    end
end
```

2. Configure the SD-WAN rule to use application categories 5 and 21:

```
config system sdwan
    config service
        edit 1
            set name "1"
            set mode sla
            set src "172.16.205.0"
            set internet-service enable
            set internet-service-app-ctrl-category 5 21
            config sla
                edit "1"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr 172.16.205.0
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "g-default"
    next
end
```

4. Verify that the traffic is sent over dmz:

```
# diagnose firewall proute list
list route policy info(vf=root):
id=2133590017(0x7f2c0001) vwl_service=1(1) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2) oif=5(dmz)
oif=95(vlan100)
source(1): 172.16.205.0-172.16.205.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): (null)(0,5,0,0,0) (null)(0,21,0,0,0)
hit_count=469 last_used=2021-12-15 15:06:05
```

5. View some videos and emails on the PC, then verify the detected application details for each category:

```
# diagnose sys sdwan internet-service-app-ctrl-category-list 5
YouTube(31077 4294838537): 142.250.217.110 6 443 Wed Dec 15 15:39:50 2021
YouTube(31077 4294838537): 173.194.152.89 6 443 Wed Dec 15 15:37:20 2021
YouTube(31077 4294838537): 173.194.152.170 6 443 Wed Dec 15 15:37:37 2021
YouTube(31077 4294838537): 209.52.146.205 6 443 Wed Dec 15 15:37:19 2021
```

```
# diagnose sys sdwan internet-service-app-ctrl-category-list 21
Gmail(15817 4294836957): 172.217.14.197 6 443 Wed Dec 15 15:39:47 2021
```

6. Verify that the captured email traffic is sent over dmz:

```
# diagnose sniffer packet any 'host 172.217.14.197' 4
interfaces=[any]
filters=[host 172.217.14.197]
5.079814 dmz out 172.16.205.100.60592 -> 172.217.14.197.443: psh 2961561240 ack
2277134591
```

7. Edit the SD-WAN rule so that dmz has a higher cost and vlan100 is preferred.

8. Verify that the traffic is now sent over vlan100:

```
# diagnose firewall proute list
list route policy info(vf=root):
id=2134048769(0x7f330001) vwl_service=1(1) vwl_mbr_seq=2 1 dscp_tag=0xff 0xff flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2) oif=95
(vlan100) oif=5(dmz)
source(1): 172.16.205.0-172.16.205.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): (null)(0,5,0,0,0) (null)(0,21,0,0,0)
hit_count=635 last_used=2021-12-15 15:55:43
```

```
# diagnose sniffer packet any 'host 172.217.14.197' 4
interfaces=[any]
filters=[host 172.217.14.197]
304.625168 vlan100 in 172.16.205.100.60592 -> 172.217.14.197.443: psh 2961572711 ack
2277139565
```

To configure application categories as an SD-WAN rule destination in the GUI:

This functionality is available in FortiOS 7.2.1 and later. Prior to 7.2.1, individual applications can be selected in SD-WAN rules by default.

After upgrading to 7.2.1 or later, the GUI functionality is available if applications are already configured in SD-WAN rules prior to upgrading. Otherwise, by default, individual applications and application groups cannot be selected in SD-WAN rules. To enable this functionality, see step 1 in the following procedure.

1. Enable the feature visibility:
   a. Go to *System > Feature Visibility*.
   b. In the *Additional Features* section, enable *Application Detection Based SD-WAN*.
   c. Click *Apply*.

   To enable GUI visibility of application detection based SD-WAN in the CLI:

   ```
   config system global
       set gui-app-detection-sdwan enable
   end
   ```

2. Configure the SD-WAN members:
   a. Go to *Network > SD-WAN*, select the *SD-WAN Zones* tab, and click *Create New > SD-WAN Member*.
   b. Set the *Interface* to *dmz*, and set the *Gateway* to *172.16.208.2*.
   c. Click *OK*.
   d. Repeat these steps to create another member for the *vlan100* interface with gateway *172.16.206.2*.
3. Configure the performance SLA (health check):
   a. Go to *Network > SD-WAN*, and select the *Performance SLAs* tab, and click *Create New*.
   b. Configure the following settings:

Name	*1*
Protocol	*DNS*

Server	*8.8.8.8*
SLA Target	Enable

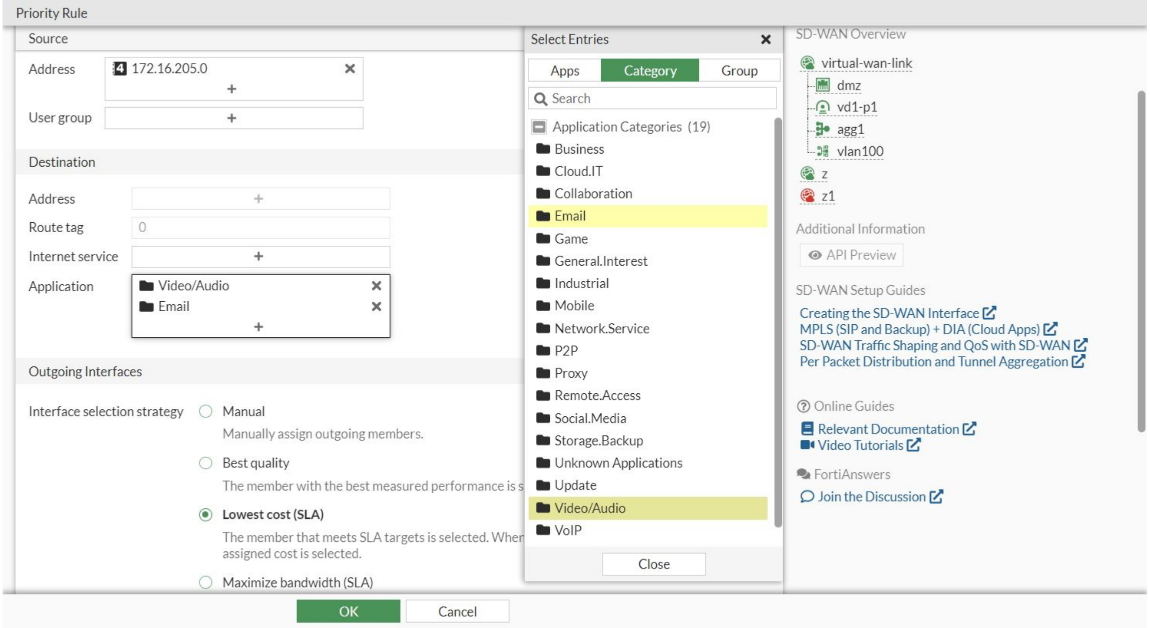
c. Click *OK*.

4. Configure the SD-WAN rule to use the video/audio and email application categories:

   a. Go to *Network > SD-WAN*, select the *SD-WAN Rules* tab, and click *Create New*.

   b. In the *Destination* section, click the + in the *Application* field.

   c. Click *Category*, and select *Video/Audio* and *Email*.



Priority Rule

Source
Address: 172.16.205.0
User group

Destination
Address
Route tag: 0
Internet service
Application: Video/Audio, Email

Outgoing Interfaces
Interface selection strategy:
○ Manual — Manually assign outgoing members.
○ Best quality — The member with the best measured performance is s
● Lowest cost (SLA) — The member that meets SLA targets is selected. When assigned cost is selected.
○ Maximize bandwidth (SLA)

   d. Configure the other settings as needed.

   e. Click *OK*.

5. Configure the firewall policy:

   a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.

   b. Configure the following settings:

Incoming Interface	*port5*
Outgoing Interface	*virtual-wan-link*
Source	*172.16.205.0*
Destination	*all*
Schedule	*always*
Service	*ALL*
Action	*ACCEPT*
Application Control	*g-default*
SSL Inspection	*certificate-inspection*

   c. Click *OK*.

Add mean opinion score calculation and logging in performance SLA health checks

The mean opinion score (MOS) is a method of measuring voice quality using a formula that takes latency, jitter, packet loss, and the codec into account to produce a score from zero to five (0 - 5). The G.711, G.729, and G.722 codecs can be selected in the health check configurations, and an MOS threshold can be entered to indicate the minimum MOS score for the SLA to pass. The maximum MOS score will depend on which codec is used, since each codec has a theoretical maximum limit.

```
config system sdwan
    config health-check
          edit <name>
            set mos-codec {g711 | g729 | g722}
            config sla
                edit <id>
                    set link-cost-factor {latency jitter packet-loss mos}
                    set mos-threshold <value>
                next
            end
        next
    end
end
```

`mos-codec {g711 | g729 | g722}`	Set the VoIP codec to use for the MOS calculation (default = g711).
`link-cost-factor {latency jitter packet-loss mos}`	Set the criteria to base the link selection on.
`mos-threshold <value>`	Set the minimum MOS for the SLA to be marked as pass (1.0 - 5.0, default = 3.6).

To configure a health check to calculate the MOS:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "dmz"
            set gateway 172.16.208.2
        next
        edit 2
            set interface "port15"
            set gateway 172.16.209.2
        next
    end
    config health-check
        edit "Test_MOS"
            set server "2.2.2.2"
            set sla-fail-log-period 30
            set sla-pass-log-period 30
            set members 0
            set mos-codec g729
            config sla
                edit 1
                    set link-cost-factor mos
                    set mos-threshold "4.0"
                next
            end
        next
    end
end
```

To use an MOS SLA to steer traffic in an SD-WAN rule:

```
config system sdwan
    config service
        edit 1
            set name "MOS_traffic_steering"
            set mode sla
            set dst "HQ_LAN"
            set src "Branch_LAN"
            config sla
                edit "Test_MOS"
                    set id 1
                next
            end
            set priority-members 0
        next
    end
end
```

The MOS currently cannot be used to steer traffic when the `mode` is set to `priority`.

To verify the MOS calculation results:

1. Verify the health check diagnostics:

   ```
   # diagnose sys sdwan health-check
   Health Check(Test_MOS):
   Seq(1 dmz): state(alive), packet-loss(0.000%) latency(0.114), jitter(0.026), mos(4.123),
   bandwidth-up(999999), bandwidth-dw(999997), bandwidth-bi(1999996) sla_map=0x1
   Seq(2 port15): state(alive), packet-loss(0.000%) latency(0.100), jitter(0.008), mos
   (4.123), bandwidth-up(999999), bandwidth-dw(999999), bandwidth-bi(1999998) sla_map=0x1
   ```

   ```
   # diagnose sys sdwan sla-log Test_MOS 1
   Timestamp: Tue Jan  4 11:23:06 2022, vdom root, health-check Test_MOS, interface: dmz,
   status: up, latency: 0.151, jitter: 0.040, packet loss: 0.000%, mos: 4.123.
   Timestamp: Tue Jan  4 11:23:07 2022, vdom root, health-check Test_MOS, interface: dmz,
   status: up, latency: 0.149, jitter: 0.041, packet loss: 0.000%, mos: 4.123.
   ```

   ```
   # diagnose sys sdwan sla-log Test_MOS 2
   Timestamp: Tue Jan  4 11:25:09 2022, vdom root, health-check Test_MOS, interface:
   port15, status: up, latency: 0.097, jitter: 0.009, packet loss: 0.000%, mos: 4.123.
   Timestamp: Tue Jan  4 11:25:10 2022, vdom root, health-check Test_MOS, interface:
   port15, status: up, latency: 0.097, jitter: 0.008, packet loss: 0.000%, mos: 4.123.
   ```

2. Change the `mos-codec` to `g722`. The diagnostics will now display different MOS values:

   ```
   # diagnose sys sdwan health-check
   Health Check(Test_MOS):
   Seq(1 dmz): state(alive), packet-loss(0.000%) latency(0.150), jitter(0.031), mos(4.453),
   bandwidth-up(999999), bandwidth-dw(999997), bandwidth-bi(1999996) sla_map=0x1
   Seq(2 port15): state(alive), packet-loss(0.000%) latency(0.104), jitter(0.008), mos
   (4.453), bandwidth-up(999999), bandwidth-dw(999999), bandwidth-bi(1999998) sla_map=0x1
   ```

3. Increase the latency on the link in port15. The calculated MOS value will decrease accordingly. In this example, port15 is out of SLA since its MOS value is now less than the 4.0 minimum:

   ```
   # diagnose sys sdwan  health-check
   Health Check(Test_MOS):
   Seq(1 dmz): state(alive), packet-loss(0.000%) latency(0.106), jitter(0.022), mos(4.453),
   bandwidth-up(999999), bandwidth-dw(999997), bandwidth-bi(1999996) sla_map=0x1
   Seq(2 port15): state(alive), packet-loss(0.000%) latency(300.119), jitter(0.012), mos
   (3.905), bandwidth-up(999999), bandwidth-dw(999999), bandwidth-bi(1999998) sla_map=0x0
   ```

Sample logs

```
date=2022-01-04 time=11:57:54 eventtime=1641326274876828300 tz="-0800" logid="0113022933"
type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN SLA notification"
eventtype="SLA" healthcheck="Test_MOS" slatargetid=1 interface="port15" status="up"
latency="300.118" jitter="0.013" packetloss="0.000" mos="3.905"
inbandwidthavailable="1000.00Mbps" outbandwidthavailable="1000.00Mbps"
bibandwidthavailable="2.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps"
bibandwidthused="0kbps" slamap="0x0" metric="mos" msg="Health Check SLA status. SLA failed
due to being over the performance metric threshold."

date=2022-01-04 time=11:57:24 eventtime=1641326244286635920 tz="-0800" logid="0113022923"
type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status"
eventtype="Health Check" healthcheck="Test_MOS" slatargetid=1 oldvalue="2" newvalue="1"
msg="Number of pass member changed."

date=2022-01-04 time=11:57:24 eventtime=1641326244286627260 tz="-0800" logid="0113022923"
type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status"
eventtype="Health Check" healthcheck="Test_MOS" slatargetid=1 member="2" msg="Member status
changed. Member out-of-sla."

date=2022-01-04 time=11:57:02 eventtime=1641326222516756500 tz="-0800" logid="0113022925"
type="event" subtype="sdwan" level="information" vd="root" logdesc="SDWAN SLA information"
eventtype="SLA" healthcheck="Test_MOS" slatargetid=1 interface="port15" status="up"
latency="0.106" jitter="0.007" packetloss="0.000" mos="4.453"
inbandwidthavailable="1000.00Mbps" outbandwidthavailable="1000.00Mbps"
bibandwidthavailable="2.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps"
bibandwidthused="0kbps" slamap="0x1" msg="Health Check SLA status."
```

Multiple members per SD-WAN neighbor configuration

SD-WAN BGP neighbor configurations are used to define the SLA health check in which an SD-WAN member must meet to qualify as being up. When the SD-WAN member meets the SLA threshold, the FortiGate will apply the route map defined in the BGP neighbor's `route-map-out-preferable` option. If the SD-WAN member fails to meet the SLA, the FortiGate will apply the route map defined in the BGP neighbor's `route-map-out` option instead. This allows the FortiGate to advertise the health of the SD-WAN member to its BGP neighbor by advertising different community strings based on its SLA status.

For more information, refer to the following BGP examples in the FortiOS Administration Guide: Controlling traffic with BGP route mapping and service rules and Applying BGP route-map to multiple BGP neighbors.

In this enhancement, instead of selecting only one SD-WAN member per neighbor, multiple SD-WAN members can be selected. This allows the SD-WAN neighbor feature to support topologies where there are multiple SD-WAN overlays and/or underlays to a neighbor. The `minimum-sla-meet-members` option is used to configure the minimum number of members that must be in an SLA per neighbor for the preferable route map to be used.

```
config system sdwan
    config neighbor
        edit <ip>
            set member {<seq-num_1>} [<seq-num_2>] ... [<seq-num_n>]
            set minimum-sla-meet-members <integer>
        next
    end
end
```

`member {<seq-num_1>} [<seq-num_2>] ... [<seq-num_n>]`	Enter the member sequence number list. Multiple members can be defined.
`minimum-sla-meet-members <integer>`	Set the minimum number of members that meet SLA when the neighbor is preferred (1 - 255, default = 1). • If the number of in SLA members is less than the `minimum-sla-meet-members` value, the default route map will be used. • If the number of in SLA members is equal or larger than the `minimum-sla-meet-members` value, the preferable route map will be used.

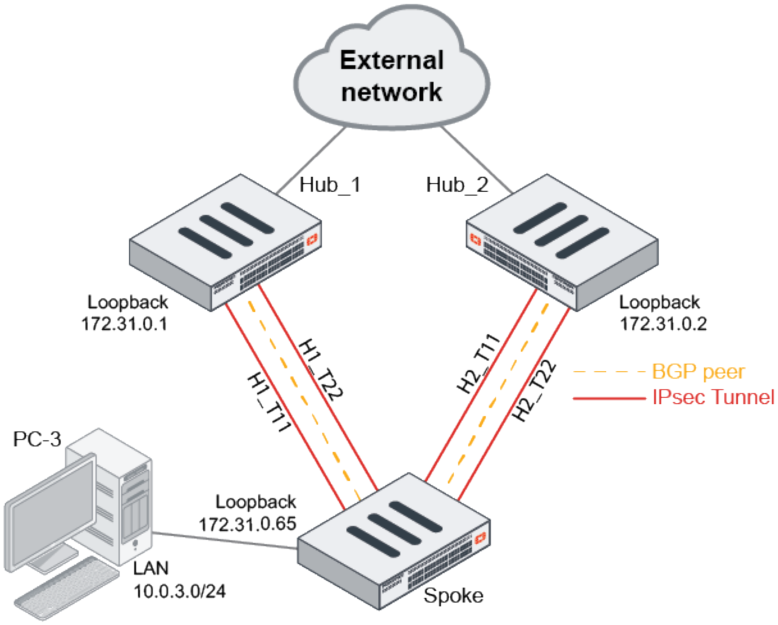
Example

In the following example, the spoke FortiGate has four tunnels: two tunnels to Hub_1 and two tunnels to Hub_2. The spoke has two BGP neighbors: one to Hub_1 and one to Hub-2. BGP neighbors are established on loopback IPs.

The SD-WAN neighbor plus `route-map-out-preferable`configuration is deployed on the spoke to achieve the following:

- If any tunnel to Hub_1 or Hub_2 is in SLA, the preferable route map will be applied on the BGP neighbor to Hub_1 or Hub_2.
- If both tunnels to Hub_1 or Hub_2 are out of SLA, the default route map will be applied on the BGP neighbor to Hub_1 or Hub_2.

The preferable route map and default route map are used to set different custom BGP communities as the spoke advertises its LAN routes to the hub. Each hub can translate communities into different BGP MED or AS prepends and signal them to the external peers to manipulate inbound traffic, thereby routing traffic to the spoke only when the SLAs are met on at least one of two VPN overlays. In this example, community string 10:1 signals to the neighbor that SLAs are met, and 10:2 signals that SLAs are not met.



To configure the BGP route maps and neighbors:

1. Configure an access list of prefixes to be matched:

```
config router access-list
    edit "net10"
        config rule
            edit 1
                set prefix 10.0.3.0 255.255.255.0
            next
        end
    next
end
```

2. Configure route maps for neighbors in SLA (preferable) and out of SLA (default):

```
config router route-map
    edit "in_sla"
        config rule
            edit 1
                set match-ip-address "net10"
                set set-community "10:1"
            next
        end
    next
    edit "out_sla"
        config rule
            edit 1
                set match-ip-address "net10"
                set set-community "10:2"
            next
        end
    next
end
```

3. Configure the BGP neighbors:

```
config router bgp
    set router-id 172.31.0.65
    config neighbor
        edit "172.31.0.1"
            set route-map-out "out_sla"
            set route-map-out-preferable "in_sla"
            set update-source "Loopback0"
        next
        edit "172.31.0.2"
            set route-map-out "out_sla"
            set route-map-out-preferable "in_sla"
            set update-source "Loopback0"
        next
    end
    config network
        edit 1
            set prefix 10.0.3.0 255.255.255.0
        next
    end
end
```

To configure SD-WAN:

1. Configure the SD-WAN members:

```
config system sdwan
    set status enable
    config members
        edit 1
            set interface "H1_T11"
            set source 172.31.0.65
        next
        edit 4
            set interface "H1_T22"
            set source 172.31.0.65
        next
        edit 6
            set interface "H2_T11"
            set source 172.31.0.65
        next
        edit 9
            set interface "H2_T22"
            set source 172.31.0.65
        next
    end
end
```

2. Configure the health check that must be met:

```
config system sdwan
    config health-check
        edit "HUB"
            set server "172.31.100.100"
            set members 0
            config sla
```

```
                edit 1
                    set link-cost-factor latency
                    set latency-threshold 100
                next
            end
        next
    end
end
```

3. Configure the SD-WAN neighbors:

```
config system sdwan
    config neighbor
        edit "172.31.0.1"
            set member 1 4
            set health-check "HUB"
            set sla-id 1
            set minimum-sla-meet-members 1
        next
        edit "172.31.0.2"
            set member 6 9
            set health-check "HUB"
            set sla-id 1
            set minimum-sla-meet-members 1
        next
    end
end
```

To verify that when two members to Hub_1/Hub_2 are in SLA, the preferable route map is be applied on BGP neighbors to Hub_1/Hub_2:

```
Branch1_A_FGT (root) # diagnose sys sdwan health-check
Health Check(HUB):
Seq(1 H1_T11): state(alive), packet-loss(0.000%) latency(0.209), jitter(0.017), mos(4.404),
bandwidth-up(999999), bandwidth-dw(999999), bandwidth-bi(1999998) sla_map=0x1
Seq(4 H1_T22): state(alive), packet-loss(0.000%) latency(0.171), jitter(0.004), mos(4.404),
bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x1
Seq(6 H2_T11): state(alive), packet-loss(0.000%) latency(0.175), jitter(0.014), mos(4.404),
bandwidth-up(999999), bandwidth-dw(999999), bandwidth-bi(1999998) sla_map=0x1
Seq(9 H2_T22): state(alive), packet-loss(0.000%) latency(0.176), jitter(0.019), mos(4.404),
bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x1
```

```
# diagnose sys sdwan neighbor
Neighbor(172.31.0.1): member(1 4 )role(standalone)
        Health-check(HUB:1)  sla-pass selected alive
Neighbor(172.31.0.2): member(6 9 )role(standalone)
        Health-check(HUB:1)  sla-pass selected alive
```

On Hub_1 and Hub_2, the expected communities have been attached into the spoke's LAN route:

```
Hub_1_FGT (root) # get router info bgp network 10.0.3.0/24
VRF 0 BGP routing table entry for 10.0.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  Local, (Received from a RR-client)
    172.31.0.65 from 172.31.0.65 (172.31.0.65)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Community: 10:1
      Last update: Wed Dec 29 22:38:29 2021
```

```
Hub_2_FGT (root) # get router info bgp network 10.0.3.0/24
VRF 0 BGP routing table entry for 10.0.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  Local, (Received from a RR-client)
    172.31.0.65 from 172.31.0.65 (172.31.0.65)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Community: 10:1

      Last update: Wed Dec 29 22:43:10 2021
```

If one member for each neighbor becomes out of SLA, the preferable route map is still applied:

```
Branch1_A_FGT (root) # diagnose sys sdwan health-check
Health Check(HUB):
Seq(1 H1_T11): state(alive), packet-loss(0.000%) latency(120.207), jitter(0.018), mos
(4.338), bandwidth-up(999999), bandwidth-dw(999997), bandwidth-bi(1999996) sla_map=0x0
Seq(4 H1_T22): state(alive), packet-loss(0.000%) latency(0.182), jitter(0.008), mos(4.404),
bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x1
Seq(6 H2_T11): state(alive), packet-loss(0.000%) latency(120.102), jitter(0.009), mos
(4.404), bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x0
Seq(9 H2_T22): state(alive), packet-loss(0.000%) latency(0.176), jitter(0.009), mos(4.404),
bandwidth-up(999999), bandwidth-dw(999997), bandwidth-bi(1999996) sla_map=0x1
```

```
# diagnose sys sdwan neighbor
Neighbor(172.31.0.1): member(1 4 )role(standalone)
        Health-check(HUB:1)  sla-pass selected alive
Neighbor(172.31.0.2): member(6 9 )role(standalone)
        Health-check(HUB:1)  sla-pass selected alive
```

```
Hub_1_FGT (root) # get router info bgp network 10.0.3.0/24
VRF 0 BGP routing table entry for 10.0.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  Local, (Received from a RR-client)
    172.31.0.65 from 172.31.0.65 (172.31.0.65)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Community: 10:1
      Last update: Thu Dec 30 10:44:47 2021
```

```
Hub_2_FGT (root) # get router info bgp network 10.0.3.0/24
VRF 0 BGP routing table entry for 10.0.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  Local, (Received from a RR-client)
    172.31.0.65 from 172.31.0.65 (172.31.0.65)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Community: 10:1
      Last update: Wed Dec 29 22:43:10 2021
```

If both members for Hub_1 become out of SLA, the default route map is applied:

```
Branch1_A_FGT (root) # diagnose sys sdwan health-check
Health Check(HUB):
Seq(1 H1_T11): state(alive), packet-loss(0.000%) latency(120.194), jitter(0.018), mos
(4.338), bandwidth-up(999999), bandwidth-dw(999997), bandwidth-bi(1999996) sla_map=0x0
Seq(4 H1_T22): state(alive), packet-loss(0.000%) latency(120.167), jitter(0.006), mos
(4.338), bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x0
Seq(6 H2_T11): state(alive), packet-loss(0.000%) latency(120.180), jitter(0.012), mos
(4.338), bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x0
Seq(9 H2_T22): state(alive), packet-loss(0.000%) latency(0.170), jitter(0.005), mos(4.404),
bandwidth-up(999999), bandwidth-dw(999997), bandwidth-bi(1999996) sla_map=0x1
```

```
# diagnose sys sdwan  neighbor
Neighbor(172.31.0.1): member(1 4 )role(standalone)
        Health-check(HUB:1)  sla-fail alive
Neighbor(172.31.0.2): member(6 9 )role(standalone)
        Health-check(HUB:1)  sla-pass selected alive
```

```
Hub_1_FGT (root) # get router info bgp network 10.0.3.0/24
VRF 0 BGP routing table entry for 10.0.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  Local, (Received from a RR-client)
    172.31.0.65 from 172.31.0.65 (172.31.0.65)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Community: 10:2
      Last update: Thu Dec 30 10:57:33 2021
```

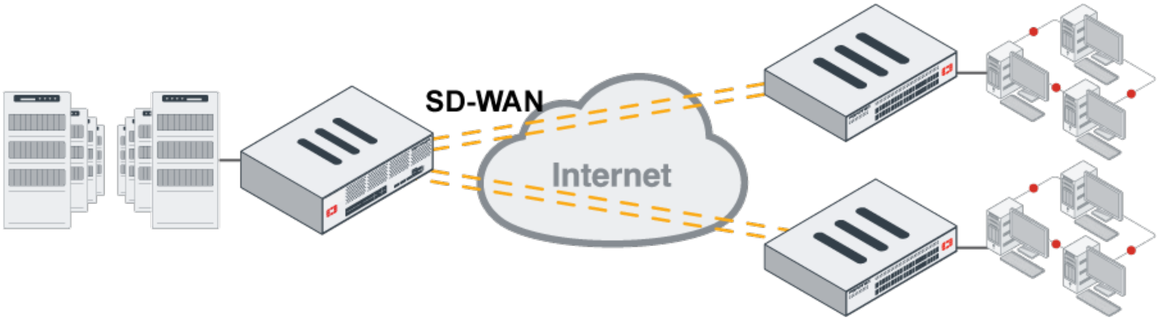
```
Hub_2_FGT (root) # get router info bgp network 10.0.3.0/24
VRF 0 BGP routing table entry for 10.0.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  Local, (Received from a RR-client)
    172.31.0.65 from 172.31.0.65 (172.31.0.65)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Community: 10:1
      Last update: Wed Dec 29 22:43:10 2021
```

Duplication on-demand when SLAs in the configured service are matched

SD-WAN packet duplication can be configured to be performed on-demand only when SLAs in the configured service are matched. When enabled, only the SLA health checks and targets that are used in the service rule are used to trigger the packet duplication.

```
config system sdwan
    config duplication
        edit 1
            set service-id 1
            set packet-duplication on-demand
            set sla-match-service {enable | disable}
        next
    end
end
```

`sla-match-service {enable | disable}`	Enable/disable packet duplication matching health check SLAs in service rules (matching all SLAs of the current defined service).



In this example, two performance SLA health checks are configured, health1 and health2. The health1 SLA is used in an SD-WAN service rule called rule1. Packet duplication uses on-demand mode, so packets for duplication are matched based on rule1. It triggers duplication based on the status of the health checks.

Results are shown for various combinations of health check statuses when the SLA match service is enabled or disabled.

To configure SD-WAN:

```
config system sdwan
    set status enable
    set load-balance-mode usage-based
    config zone
        edit "virtual-wan-link"
        next
        edit "SASE"
        next
    end
    config members
        edit 1
            set interface "port5"
            set gateway 10.100.1.1
        next
        edit 2
            set interface "port4"
        next
    end
    config health-check
        edit "health1"
            set server "10.100.2.22"
            set members 0
            config sla
                edit 1
                next
            end
        next
        edit "health2"
            set server "10.100.2.23"
            set members 0
            config sla
                edit 1
                next
            end
        next
    end
    config service
        edit 1
            set name "rule1"
            set mode sla
            set dst "10.100.20.0"
            config sla
                edit "health1"
                    set id 1
                next
            end
            set priority-members 2 1
        next
    end
    config duplication
        edit 1
            set service-id 1
            set packet-duplication on-demand
            set sla-match-service enable
        next
    end
end
```

Results

- When health1 (used in rule1) is out of SLA (`sla_map=0x0`) and health2 (not used) is in SLA (`sla_map=0x1`), the packet is duplicated (`dup=0x1(dup)`):

```
# diagnose sys sdwan health-check
Health Check(health1):
Seq(1 port5): state(alive), packet-loss(6.000%) latency(5.718), jitter(0.086), mos
(4.404), bandwidth-up(99995), bandwidth-dw(99995), bandwidth-bi(199990) sla_map=0x0
Seq(2 port4): state(alive), packet-loss(3.000%) latency(7.242), jitter(0.025), mos
(4.404), bandwidth-up(99998), bandwidth-dw(99999), bandwidth-bi(199997) sla_map=0x0
Health Check(health2):
Seq(1 port5): state(alive), packet-loss(0.000%) latency(0.700), jitter(0.075), mos
(4.404), bandwidth-up(99995), bandwidth-dw(99995), bandwidth-bi(199990) sla_map=0x1
Seq(2 port4): state(alive), packet-loss(0.000%) latency(0.244), jitter(0.021), mos
(4.404), bandwidth-up(99998), bandwidth-dw(99999), bandwidth-bi(199997) sla_map=0x1
```

```
# diagnose firewall proute list
id=2135031809(0x7f420001) vwl_service=1(rule1) vwl_mbr_seq=2 1 dscp_tag=0xfc 0xfc
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=12(port4) measure=0x0(not measured) dup=0x1(dup) oif=13(port5) measure=0x0(not
measured) dup=0x1(dup)
destination(1): 10.100.20.0-10.100.20.255
source wildcard(1): 0.0.0.0/0.0.0.0
```

The sniffer output shows packets leaving from both interfaces in the zone:

```
# diagnose sniffer packet any "port 90" 4
interfaces=[any]
filters=[port 90]
```

```
2.403506 port2 in 172.16.205.11.59624 -> 10.100.20.33.90: syn 2098685816
2.403522 port5 out 10.100.1.250.59624 -> 10.100.20.33.90: syn 2098685816
2.403523 port4 out 10.100.1.250.59624 -> 10.100.20.33.90: syn 2098685816
```

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(2 port4), alive, sla(0x0), gid(0), cfg_order(0), cost(0), selected
    2: Seq_num(1 port5), alive, sla(0x0), gid(0), cfg_order(1), cost(0), selected
  Dst address(1):
        10.100.20.0-10.100.20.255
```

- When health1 (used in rule1) is in SLA (`sla_map=0x1`) and health2 (not used) is out of SLA (`sla_map=0x0`), the packet is not duplicated (`dup=0x0(not dup)`):

```
# diagnose sys sdwan health-check
Health Check(health1):
Seq(1 port5): state(alive), packet-loss(0.000%) latency(0.684), jitter(0.064), mos
(4.404), bandwidth-up(99995), bandwidth-dw(99995), bandwidth-bi(199990) sla_map=0x1
Seq(2 port4): state(alive), packet-loss(0.000%) latency(0.222), jitter(0.015), mos
(4.404), bandwidth-up(99998), bandwidth-dw(99999), bandwidth-bi(199997) sla_map=0x1
Health Check(health2):
Seq(1 port5): state(alive), packet-loss(6.000%) latency(2.911), jitter(2.328), mos
(1.787), bandwidth-up(99995), bandwidth-dw(99996), bandwidth-bi(199990) sla_map=0x0
Seq(2 port4): state(alive), packet-loss(6.000%) latency(2.566), jitter(2.307), mos
(1.786), bandwidth-up(99998), bandwidth-dw(99999), bandwidth-bi(199997) sla_map=0x0
```

```
# diagnose firewall proute list
id=2135031809(0x7f420001) vwl_service=1(rule1) vwl_mbr_seq=2 1 dscp_tag=0xfc 0xfc
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=12(port4) measure=0x0(not measured) dup=0x0(not dup) oif=13(port5) measure=0x0(not
measured) dup=0x0(not dup)
destination(1): 10.100.20.0-10.100.20.255
source wildcard(1): 0.0.0.0/0.0.0.0
```

The sniffer output shows packets leaving from only one interface:

```
# diagnose sniffer packet any "port 90" 4
interfaces=[any]
filters=[port 90]
3.330376 port2 in 172.16.205.11.38318 -> 10.100.21.33.90: syn 381919014
3.330395 port5 out 10.100.1.2.38318 -> 10.100.21.33.90: syn 381919014
4.327851 port2 in 172.16.205.11.38318 -> 10.100.21.33.90: syn 381919014
4.327855 port5 out 10.100.1.2.38318 -> 10.100.21.33.90: syn 381919014
```

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(2 port4), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected
    2: Seq_num(1 port5), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  Dst address(1):
        10.100.20.0-10.100.20.255
```

- When the SLA match service is disabled, packets are only duplicated with all of the health checks are out of SLA:

```
config system sdwan
    config duplication
        edit 1
            set service-id 1
            set packet-duplication on-demand
            set sla-match-service disable
        next
    end
end
```

  - When health1 is out of SLA (`sla_map=0x0`) and health2 is in SLA (`sla_map=0x1`), the packet is not duplicated (`dup=0x0(not dup)`):

```
# diagnose sys sdwan health-check
Health Check(health1):
Seq(1 port5): state(alive), packet-loss(5.000%) latency(6.587), jitter(0.096), mos
(4.404), bandwidth-up(99995), bandwidth-dw(99995), bandwidth-bi(199990) sla_map=0x0
Seq(2 port4): state(alive), packet-loss(3.000%) latency(3.365), jitter(0.085), mos
(4.404), bandwidth-up(99998), bandwidth-dw(99999), bandwidth-bi(199997) sla_map=0x0
Health Check(health2):
Seq(1 port5): state(alive), packet-loss(0.000%) latency(0.837), jitter(0.192), mos
(4.404), bandwidth-up(99995), bandwidth-dw(99995), bandwidth-bi(199990) sla_map=0x1
Seq(2 port4): state(alive), packet-loss(0.000%) latency(0.330), jitter(0.081), mos
(4.404), bandwidth-up(99998), bandwidth-dw(99999), bandwidth-bi(199997) sla_map=0x1
```

```
# diagnose firewall proute list
list route policy info(vf=root):

id=2135097345(0x7f430001) vwl_service=1(rule1) vwl_mbr_seq=2 1 dscp_tag=0xfc 0xfc
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=12(port4) measure=0x0(not measured) dup=0x0(not dup) oif=13(port5) measure=0x0
(not measured) dup=0x0(not dup)
destination(1): 10.100.20.0-10.100.20.255
source wildcard(1): 0.0.0.0/0.0.0.0
```

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(2 port4), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected
    2: Seq_num(1 port5), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  Dst address(1):
        10.100.20.0-10.100.20.255
```

  - When both health1 and health2 are out of SLA (`sla_map=0x0`), the packet is duplicated (`dup=0x1(dup)`).

If there are multiple targets in a performance SLA health check, and only one of the targets is used in the service that is defined in the duplication rule, and the SLA match service is disabled, then only that target triggers packet duplication. It is note required for all of the targets in the health check to miss SLA.

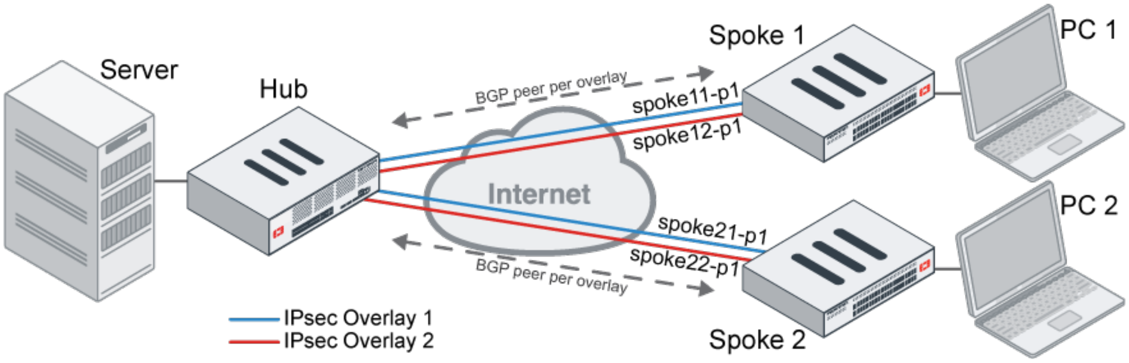
SD-WAN in large scale deployments

SD-WAN with ADVPN configurations in large-scale deployments is improved.

- Phase 2 selectors can be used to inject IKE routes on the ADVPN shortcut tunnel.

  When configuration method (`mode-cfg`) is enabled in IPsec phase 1 configuration, enabling `mode-cfg-allow-client-selector` allows custom phase 2 selectors to be configured. By also enabling the addition of a route to the peer destination selector (`add-route`) in the phase 1 configuration, IKE routes based on the phase 2 selectors can be injected. This means that routes do not need to be reflected on the hub to propagate them between spokes, avoiding possible BGP daemon process load issues and improving network scalability in a large-scale ADVPN network.
- Route map rules can apply priorities to BGP routes.

  On the hub, priorities can be set in a route map's rules, and the route map can be applied on BGP routes. This allows the hub to mark the preferred path learned from the spokes with a priority value (lower priority is preferred), instead of using multiple SD-WAN policy routes on the hub. When a preferred outbound route map (`route-map-out-preferable`) is also configured in an SD-WAN neighbor on the spoke, deploying SD-WAN rules on the hub to steer traffic from the hub to a spoke is unnecessary.
- SD-WAN members' local cost can be exchanged on the ADVPN shortcut tunnel so that spokes can use the remote cost as tiebreak to select a preferred shortcut. If multiple shortcuts originate from the same member to different members on the same remote spoke, then the remote cost on the shortcuts is used as the tiebreak to decide which shortcut is preferred.



In this example, SD-WAN is configured on an ADVPN network with a BGP neighbor per overlay.

Instead of reflecting BGP routes with the route-reflector on the hub, when the shortcuts are triggered, IKE routes on the shortcuts are directly injected based on the configured phase 2 selectors to allow routes to be exchanged between spokes.

Routes between the hub and the spokes are exchanged by BGP, and the spokes use the default route to send spoke-to-spoke traffic to the hub and trigger the shortcuts.

Instead of configuring SD-WAN rules on the hub, different priorities are configured on the BGP routes by matching different BGP communities to steer traffic from the hub to the spokes.

To configure Spoke 1:

1. Configure phase 1:

```
config vpn ipsec phase1-interface
    edit "spoke11-p1"
        ...
        set ike-version 2
        set net-device enable
        set add-route enable
        set mode-cfg enable
        set auto-discovery-receiver enable
        set mode-cfg-allow-client-selector enable
        ...
    next
    edit "spoke12-p1"
       ...
        set ike-version 2
        set net-device enable
        set add-route enable
        set mode-cfg enable
        set auto-discovery-receiver enable
        set mode-cfg-allow-client-selector enable
    next
end
```

2. Configure phase 2:

```
config vpn ipsec phase2-interface
    edit "spoke11-p2"
        ...
        set src-name "LAN_Net"
        set dst-name "all"
    next
    edit "spoke12-p2"
        ...
        set src-name "LAN_Net"
        set dst-name "all"
    next
end
```

3. Configure an address group:
   Spoke 1 uses LAN subnet 10.1-3.100.0/24.

```
config firewall addrgrp
    edit "LAN_Net"
        set member "10.1.100.0" "10.2.100.0" "10.3.100.0"
    next
end
```

4. Configure route maps:
   - If overlay 1 to the hub is in SLA, attach "65000:1" to the BGP routes advertised to the hub over overlay 1.
   - If overlay 2 to the hub is in SLA, attach "65000:2" to the BGP routes advertised to the hub over overlay 2.
   - If any overlay to the hub is out of SLA, attach "65000:9999" to the BGP routes advertised to the hub over any overlay.

```
config router route-map
    edit "HUB_CARRIER1"
        config rule
            edit 1
                set set-community "65000:1"
                ...
            next
        end
```

```
            ...
        next
        edit "HUB_CARRIER2"
            config rule
                edit 1
                    set set-community "65000:2"
                    ...
                next
            end
            ...
        next
        edit "HUB_BAD"
            config rule
                edit 1
                    set set-community "65000:9999"
                    ...
                next
            end
            ...
        next
    end
```

5. Configure BGP and SD-WAN members and neighbors:

```
config router bgp
    set as 65412
    config neighbor
        edit "10.10.15.253"
            set remote-as 65412
            set route-map-out "HUB_BAD"
            set route-map-out-preferable "HUB_CARRIER1"
            ...
        next
        edit "10.10.16.253"
            set remote-as 65412
            set route-map-out "HUB_BAD"
            set route-map-out-preferable "HUB_CARRIER2"
            ...
        next
    end
end
```

```
config system sdwan
    config members
        edit 1
            set interface "spoke11-p1"
        next
        edit 2
            set interface "spoke12-p1"
        next
    end
    config neighbor
        edit "10.10.15.253"
            set member 1
            set health-check "1"
            set sla-id 1
        next
        edit "10.10.16.253"
            set member 2
            set health-check "11"
            set sla-id 1
        next
    end
end
```

To configure Spoke 2:

1. Configure phase 1:

```
config vpn ipsec phase1-interface
    edit "spoke21-p1"
        ...
        set ike-version 2
        set net-device enable
        set add-route enable
        set mode-cfg enable
        set auto-discovery-receiver enable
        set mode-cfg-allow-client-selector enable
        ...
    next
    edit "spoke22-p1"
       ...
        set ike-version 2
        set net-device enable
        set add-route enable
        set mode-cfg enable
        set auto-discovery-receiver enable
        set mode-cfg-allow-client-selector enable
    next
end
```

2. Configure phase 2:

```
config vpn ipsec phase2-interface
    edit "spoke21-p2"
        ...
        set src-name "LAN_Net"
        set dst-name "all"
    next
    edit "spoke22-p2"
        ...
        set src-name "LAN_Net"
        set dst-name "all"
    next
end
```

3. Configure an address group:
   Spoke 2 uses LAN subnet 192.168.5-7.0/24.

```
config firewall addrgrp
    edit "LAN_Net"
        set member "192.168.5.0" "192.168.6.0" "192.168.7.0"
    next
end
```

4. Configure route maps:
   - If overlay 1 to the hub is in SLA, attach "65000:1" to the BGP routes advertised to the hub over overlay 1.
   - If overlay 2 to the hub is in SLA, attach "65000:2" to the BGP routes advertised to the hub over overlay 2.
   - If any overlay to the hub is out of SLA, attach "65000:9999" to the BGP routes advertised to the hub over any overlay.

```
config router route-map
    edit "HUB_CARRIER1"
        config rule
            edit 1
                set set-community "65000:1"
                ...
            next
        end
        ...
    next
    edit "HUB_CARRIER2"
        config rule
            edit 1
                set set-community "65000:2"
                ...
            next
        end
        ...
    next
    edit "HUB_BAD"
        config rule
            edit 1
                set set-community "65000:9999"
                ...
            next
        end
        ...
    next
end
```

5. Configure BGP and SD-WAN members and neighbors:

```
config router bgp
    set as 65412
    config neighbor
        edit "10.10.15.253"
            set remote-as 65412
            set route-map-out "HUB_BAD"
            set route-map-out-preferable "HUB_CARRIER1"
            ...
        next
        edit "10.10.16.253"
            set remote-as 65412
            set route-map-out "HUB_BAD"
            set route-map-out-preferable "HUB_CARRIER2"
            ...
        next
    end
end
```

```
config system sdwan
    config members
        edit 1
            set interface "spoke21-p1"
            set cost 100
        next
        edit 2
            set interface "spoke22-p1"
            set cost 200
        next
    end
    config neighbor
        edit "10.10.15.253"
            set member 1
            set health-check "1"
            set sla-id 1
        next
        edit "10.10.16.253"
            set member 2
            set health-check "11"
            set sla-id 1
        next
    end
end
```

To configure the hub:

1. Configure the route maps:
    - Set the priority to 100 for routes with community 65000:1, indicating that they are in SLA for overlay 1.
    - Set the priority to 200 for routes with community 65000:2, indicating that they are in SLA for overlay 2.
    - Set the priority to 9999 for routes with community 65000:9999, indicating that they are out of SLA for any overlay.

```
config router route-map
     edit "Set_Pri"
        config rule
            edit 1
                set match-community "comm_65000:1"
                set set-priority 100
            next
            edit 2
                set match-community "comm_65000:2"
                set set-priority 200
            next
            edit 3
                set match-community "comm_65000:9999"
                set set-priority 9999
            next
        end
    next
end
```

2. Configure BGP:

```
config router bgp
    set as 65412
    config neighbor-group
        edit "advpn"
            set remote-as 65412
            set route-map-in "Set_Pri"
            ...
        next
        edit "advpn2"
            set remote-as 65412
            set route-map-in "Set_Pri"
            ...
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.15.0 255.255.255.0
            set neighbor-group "advpn"
        next
        edit 2
            set prefix 10.10.16.0 255.255.255.0
            set neighbor-group "advpn2"
        next
    end
end
```

To test the configuration:

1. Check the routing tables on the spokes:

   Spoke 1:

```
spoke-1 (root) # get router info routing-table all
B*      0.0.0.0/0 [200/0] via 10.10.15.253 (recursive is directly connected, spoke11-
p1), 00:01:17, [1/0]         // default route to hub
                         [200/0] via 10.10.16.253 (recursive is directly connected,
spoke12-p1), 00:01:17, [1/0]
B       9.0.0.0/24 [200/0] via 10.10.15.253 (recursive is directly connected, spoke11-
p1), 00:01:17, [1/0]        // route to the server behind hub
                          [200/0] via 10.10.16.253 (recursive is directly connected,
spoke12-p1), 00:01:17, [1/0]
C       10.1.100.0/24 is directly connected, port2             // route to PC 1
C       10.10.15.0/24 is directly connected, spoke11-p1        // overlay 1
C       10.10.15.1/32 is directly connected, spoke11-p1
C       10.10.16.0/24 is directly connected, spoke12-p1        // overlay 2
C       10.10.16.1/32 is directly connected, spoke12-p1
```

   Spoke 2:

```
spoke-2 (root) # get router info routing-table all
B*      0.0.0.0/0 [200/0] via 10.10.15.253 (recursive is directly connected, spoke21-
p1), 00:46:14, [1/0]         // default route to hub
                         [200/0] via 10.10.16.253 (recursive is directly connected,
spoke22-p1), 00:46:14, [1/0]
B       9.0.0.0/24 [200/0] via 10.10.15.253 (recursive is directly connected, spoke21-
p1), 00:46:18, [1/0]        // route to the server behind hub
                          [200/0] via 10.10.16.253 (recursive is directly connected,
spoke22-p1), 00:46:18, [1/0]
C       10.10.15.0/24 is directly connected, spoke21-p1        // overlay 1
C       10.10.15.2/32 is directly connected, spoke21-p1
```

```
C       10.10.16.0/24 is directly connected, spoke22-p1        // overlay 2
C       10.10.16.2/32 is directly connected, spoke22-p1
C       192.168.5.0/24 is directly connected, port2            // route to PC 2
```

2. Send traffic from PC 1 to PC 2 and trigger the shortcut:

   The IKE routes on the shortcut are directly injected based on the phase 2 selectors, and spoke-to-spoke traffic then goes directly through the shortcut instead of going through the hub.

   Spoke 1:

```
spoke-1 (root) # get router info routing-table static
S       192.168.5.0/24 [15/0] via spoke11-p1_0 tunnel 172.16.200.4 vrf 0, [1/0]
S       192.168.6.0/24 [15/0] via spoke11-p1_0 tunnel 172.16.200.4 vrf 0, [1/0]
S       192.168.7.0/24 [15/0] via spoke11-p1_0 tunnel 172.16.200.4 vrf 0, [1/0]
```

```
spoke-1 (root) # diagnose sniffer packet any 'host 192.168.5.44' 4
interfaces=[any]
filters=[host 192.168.5.44]
1.446306 port2 in 10.1.100.22 -> 192.168.5.44: icmp: echo request
1.446327 spoke11-p1_0 out 10.1.100.22 -> 192.168.5.44: icmp: echo request
1.446521 spoke11-p1_0 in 192.168.5.44 -> 10.1.100.22: icmp: echo reply
1.446536 port2 out 192.168.5.44 -> 10.1.100.22: icmp: echo reply
```

   Spoke 2:

```
spoke-2 (root) # get router info routing-table static
S       10.1.100.0/24 [15/0] via spoke21-p1_0 tunnel 10.10.15.1 vrf 0, [1/0]
S       10.2.100.0/24 [15/0] via spoke21-p1_0 tunnel 10.10.15.1 vrf 0, [1/0]
S       10.3.100.0/24 [15/0] via spoke21-p1_0 tunnel 10.10.15.1 vrf 0, [1/0]
```

3. Confirm that the overlays are in SLA on the spokes:

   Spoke 1:

```
spoke-1 (root) # diagnose sys sdwan  neighbor
Neighbor(10.10.15.253): member(1)role(standalone)
        Health-check(1:1)  sla-pass selected alive
Neighbor(10.10.16.253): member(2)role(standalone)
        Health-check(11:1)  sla-pass selected alive
```

   Spoke 2:

```
spoke-2 (root) # diagnose sys sdwan neighbor
Neighbor(10.10.15.253): member(1)role(standalone)
        Health-check(1:1)  sla-pass selected alive
Neighbor(10.10.16.253): member(2)role(standalone)
        Health-check(11:1)  sla-pass selected alive
```

4. On the hub, check that the routes received from the spokes have the expected priorities:

```
hub (root) # diagnose ip route list | grep proto=11
tab=254 vf=0 scope=0 type=1 proto=11 prio=100 0.0.0.0/0.0.0.0/0->10.1.100.0/24
pref=0.0.0.0 gwy=10.10.15.1 dev=101(hub-phase1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=200 0.0.0.0/0.0.0.0/0->10.1.100.0/24
pref=0.0.0.0 gwy=10.10.16.1 dev=102(hub2-phase1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=100 0.0.0.0/0.0.0.0/0->192.168.5.0/24
pref=0.0.0.0 gwy=10.10.15.2 dev=101(hub-phase1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=200 0.0.0.0/0.0.0.0/0->192.168.5.0/24
pref=0.0.0.0 gwy=10.10.16.2 dev=102(hub2-phase1)
```

The priority set by the hub's route map is based on the community string received from the spoke. The route with a lower priority value is selected, so traffic to Spoke 1 goes out on the hub-phase1 tunnel:

```
hub (root) # diagnose sniffer packet any 'host 9.0.0.2' 4
interfaces=[any]
filters=[host 9.0.0.2]
2.735456 R190 in 9.0.0.2 -> 10.1.100.22: icmp: echo request
2.735508 hub-phase1 out 9.0.0.2 -> 10.1.100.22: icmp: echo request
2.735813 hub-phase1 in 10.1.100.22 -> 9.0.0.2: icmp: echo reply
2.735854 R190 out 10.1.100.22 -> 9.0.0.2: icmp: echo reply
```

5. If overlay 1 goes out of SLA, the priorities of the routes on the hub are updated and traffic from the hub to Spoke 1 goes through overlay 2:

   Spoke 1:

   ```
   spoke-1 (root) # diagnose sys sdwan  neighbor
   Neighbor(10.10.15.253): member(1)role(standalone)
           Health-check(1:1)  sla-fail alive
   Neighbor(10.10.16.253): member(2)role(standalone)
           Health-check(11:1)  sla-pass selected alive
   ```

   Spoke 2:

   ```
   spoke-2 (root) # diagnose sys sdwan neighbor
   Neighbor(10.10.15.253): member(1)role(standalone)
           Health-check(1:1)  sla-fail alive
   Neighbor(10.10.16.253): member(2)role(standalone)
           Health-check(11:1)  sla-pass selected alive
   ```

   Hub:

   ```
   hub (root) # diagnose ip route list | grep proto=11
   tab=254 vf=0 scope=0 type=1 proto=11 prio=200 0.0.0.0/0.0.0.0/0->10.1.100.0/24
   pref=0.0.0.0 gwy=10.10.16.1 dev=102(hub2-phase1)
   tab=254 vf=0 scope=0 type=1 proto=11 prio=9999 0.0.0.0/0.0.0.0/0->10.1.100.0/24
   pref=0.0.0.0 gwy=10.10.15.1 dev=101(hub-phase1)
   tab=254 vf=0 scope=0 type=1 proto=11 prio=200 0.0.0.0/0.0.0.0/0->192.168.5.0/24
   pref=0.0.0.0 gwy=10.10.16.2 dev=102(hub2-phase1)
   tab=254 vf=0 scope=0 type=1 proto=11 prio=9999 0.0.0.0/0.0.0.0/0->192.168.5.0/24
   pref=0.0.0.0 gwy=10.10.15.2 dev=101(hub-phase1)
   ```

   ```
   hub (root) # diagnose sniffer packet any 'host 9.0.0.2' 4
   interfaces=[any]
   filters=[host 9.0.0.2]
   3.550181 R190 in 9.0.0.2 -> 10.1.100.22: icmp: echo request
   3.550234 hub2-phase1 out 9.0.0.2 -> 10.1.100.22: icmp: echo request
   3.550713 hub2-phase1 in 10.1.100.22 -> 9.0.0.2: icmp: echo reply
   3.550735 R190 out 10.1.100.22 -> 9.0.0.2: icmp: echo reply
   ```

6. Trigger shortcuts between Spoke 1 and Spoke 2:
   - Shortcuts spoke11-p1_1 and spoke11-p1_0 originate from spoke11-p1.
   - spoke11-p1_1 corresponds to spoke21-p1_0 on Spoke 2.
   - spoke11-p1_0 corresponds to spoke22-p1_0 on Spoke 2.

   Spoke 1:

   ```
   spoke-1 (root) # diagnose sys sdwan service

   Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
   ```

```
 Tie break: cfg
  Gen(12), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-number
  Service role: standalone
  Member sub interface(4):
    3: seq_num(1), interface(spoke11-p1):
       1: spoke11-p1_0(75)
       2: spoke11-p1_1(76)
  Members(4):
    1: Seq_num(1 spoke11-p1_1), alive, sla(0x1), gid(0), remote cost(100), cfg_order(0),
local cost(0), selected
    2: Seq_num(1 spoke11-p1_0), alive, sla(0x1), gid(0), remote cost(200), cfg_order(0),
local cost(0), selected
    3: Seq_num(1 spoke11-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0),
selected
    4: Seq_num(2 spoke12-p1), alive, sla(0x2), gid(0), cfg_order(1), local cost(0),
selected
  Src address(1):
        10.1.100.0-10.1.100.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

Spoke 2:

```
spoke-2 (root) # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(9), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-number
  Service role: standalone
  Member sub interface(4):
    2: seq_num(1), interface(spoke21-p1):
       1: spoke21-p1_0(68)
    4: seq_num(2), interface(spoke22-p1):
       1: spoke22-p1_0(67)
  Members(4):
    1: Seq_num(1 spoke21-p1_0), alive, sla(0x1), gid(0), cfg_order(0), local cost(100),
selected
    2: Seq_num(1 spoke21-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(100),
selected
    3: Seq_num(2 spoke22-p1_0), alive, sla(0x2), gid(0), cfg_order(1), local cost(200),
selected
    4: Seq_num(2 spoke22-p1), alive, sla(0x2), gid(0), cfg_order(1), local cost(200),
selected
  Src address(1):
        192.168.5.0-192.168.5.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

7. On Spoke 2, increase the cost of spoke21-p1_0 to 300.

```
spoke-2 (root) # config system sdwan
    config members
        edit 1
            set interface "spoke21-p1"
            set cost 300
        next
    end
end
```

The new cost is learned by the spoke11-p1_1 shortcut on Spoke 1, and that shortcut is no longer preferred due to its higher remote cost:

Spoke 1:

```
spoke-1 (root) # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(13), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-number
  Service role: standalone
  Member sub interface(4):
    3: seq_num(1), interface(spoke11-p1):
       1: spoke11-p1_0(78)
       2: spoke11-p1_1(79)
  Members(4):
    1: Seq_num(1 spoke11-p1_0), alive, sla(0x1), gid(0), remote cost(200), cfg_order(0),
local cost(0), selected
    2: Seq_num(1 spoke11-p1_1), alive, sla(0x1), gid(0), remote cost(300), cfg_order(0),
local cost(0), selected
    3: Seq_num(1 spoke11-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0),
selected
    4: Seq_num(2 spoke12-p1), alive, sla(0x2), gid(0), cfg_order(1), local cost(0),
selected
  Src address(1):
        10.1.100.0-10.1.100.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

Spoke 2:

```
spoke-2 (root) # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-number
  Service role: standalone
  Member sub interface(4):
    2: seq_num(2), interface(spoke22-p1):
       1: spoke22-p1_0(70)
    4: seq_num(1), interface(spoke21-p1):
       1: spoke21-p1_0(71)
  Members(4):
    1: Seq_num(2 spoke22-p1_0), alive, sla(0x2), gid(0), cfg_order(1), local cost(200),
selected
    2: Seq_num(2 spoke22-p1), alive, sla(0x2), gid(0), cfg_order(1), local cost(200),
selected
    3: Seq_num(1 spoke21-p1_0), alive, sla(0x1), gid(0), cfg_order(0), local cost(300),
selected
    4: Seq_num(1 spoke21-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(300),
selected
  Src address(1):
        192.168.5.0-192.168.5.255
```

```
      Dst address(1):
            0.0.0.0-255.255.255.255
```

SD-WAN segmentation over a single overlay

SD-WAN, VPN, and BGP configurations support L3 VPN segmentation over a single overlay. In these configurations, a hub and spoke SD-WAN deployment requires that branch sites, or spokes, are able to accommodate multiple companies or departments, and each company's subnet is separated by a different VRF. A subnet on one VRF cannot communicate with a subnet on another VRF between different branches, but can communicate with the same VRF.

New SD-WAN options

VRF-aware SD-WAN health checks

SD-WAN on the originating spoke can tag the health check probes with the correct VRF when transmitting to a multi-VRF tunnel. The hub can then forward the probes to the correct health check server in the same VRF as the hub.

```
config system sdwan
   config health-check
       edit <name>
           set vrf <vrf id>
           set source <address>
       next
   end
end
```

`vrf <vrf id>`	Virtual Routing Forwarding ID.
`source <address>`	Source IP address used in the health-check packet to the server.

Overlay stickiness

When a hub has multiple overlays, traffic received on one overlay should egress on the same overlay when possible. The `service-sla-tie-break` option ensures overlay stickiness. In SD-WAN service rules, options are available to ensure that traffic received in a zone stays in that zone.

```
config system sdwan
    config zone
        edit <name>
            set service-sla-tie-break input-device
        next
    end
    config service
        edit <id>
            set input-zone <zone>
            set tie-break input-device
        next
    end
end
```

`service-sla-tie-break input-device`	Members that meet the SLA are selected by matching the input device.
`input-zone <zone>`	Source input-zone name.
`tie-break input-device`	Members that meet the SLA are selected by matching the input device.

New IPsec options

Configurable rate limit for shortcut offers sent by the hub

By default, the hub sends a shortcut offer to a spoke every five seconds. If the hub continues to send offers that keep failing, and there are a large number of spokes, this can cause a high load on the hub. This setting makes the interval between shortcut offers configurable.

```
config vpn ipsec phase1-interface
    edit <name>
        set auto-discovery-offer-interval <interval>
    next
end
```

`auto-discovery-offer-interval <interval>`	Interval between shortcut offer messages, in seconds (1 - 300, default = 5).

Segmentation over a single overlay

Segmentation requires that VRF info is encapsulated within the IPsec VPN tunnel. This setting enables multi-VRF IPSEC tunnels.

```
config vpn ipsec phase1-interface
    edit <name>
        set encapsulation vpn-id-ipip
    next
end
```

`encapsulation vpn-id-ipip`	VPN ID with IPIP encapsulation.

New VPN configuration for BGP

The role of a VRF can be specified, along with other VRF details. In FortiOS 7.2.0 to 7.2.3, up to 64 VRFs can be configured per VDOM for any device. In FortiOS 7.2.4, up to 252 VRFs can be configured per VDOM for any device.

```
config router bgp
    config vrf
        edit <vrf>
            set role {standalone | ce | pe}
            set rd <string>
            set export-rt <route_target>
            set import-rt <route_target>
            set import-route-map <route_map>
            config leak-target
                edit <vrf>
                    set route-map <route-map>
                    set interface <interface>
                next
            end
        next
    end
end
```

`role {standalone | ce | pe}`	VRF role: standalone, customer edge (CE), or provider edge (PE).
`rd <string>`	Route Distinguisher: AA|AA:NN. This option is only available when the role is CE.
`export-rt <route_target>`	List of export route target. This option is only available when the role is CE.
`import-rt <route_target>`	List of import route target. This option is only available when the role is CE.
`import-route-map <route_map>`	Import route map. This option is only available when the role is CE.
`route-map <route-map>`	Route map of VRF leaking.
`interface <interface>`	Interface that is used to leak routes to the target VRF.

In FortiOS 7.0, `config vrf` was `config vrf-leak`, and `config leak-target` was `config target`.

Display BGP routes by VRF and neighbor

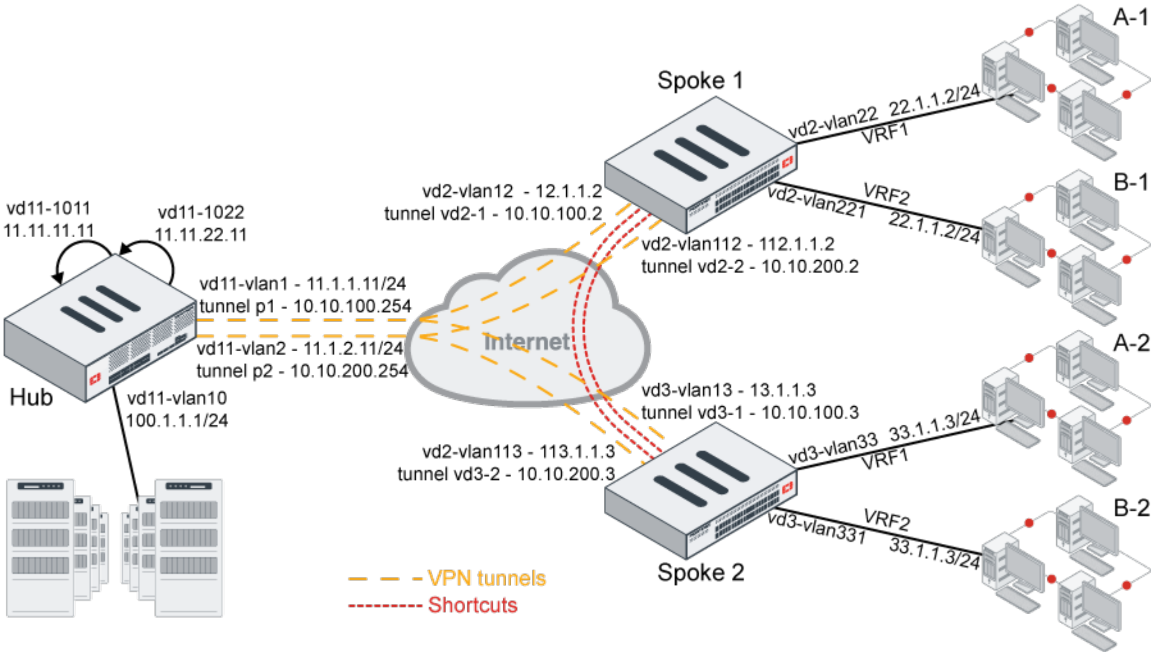
```
# diagnose ip router bgp set-filter vrf <vrf>
# diagnose ip router bgp set-filter neighbor <neighbor address>
# diagnose ip router bgp set-filter reset
# execute router clear bgp vpnv4 unicast soft {in | out}
# get router info filter show
# get router info filter vrf {vrf | all}
```

Examples

In example 1, multiple companies (or departments of a company) share the ADVPN. Company A and company B each have two branches in two different locations. Company A's branches (A-1 and A-2) can talk to each other using the VPN shortcut, but not to company B's branches (B-1 and B-2). Likewise, company B's branches can talk to each other using the VPN shortcut, but not to company A's branches. Traffic can share the tunnels and shortcuts, but cannot be mixed up.

Example 2 shows that performance SLA health checks can be sent from a spoke's VRF to the loopback on the hub that is in the same VRF.

Example 3 shows that when traffic is ingress on the hub on one overlay, it will preferably egress on the same overlay.



Example 1

In this example, two spokes each have two tunnels to the hub.

- Each spoke has two VRFs behind it that can use the same IP address or subnets.
- The computers in VRF1 behind spoke 1 can talk to the computers in VRF1 behind spoke 2, but not to any of the computers in the VRF2s behind either spoke.
- The computers in VRF2 behind spoke 1 can talk to the computers in VRF2 behind spoke 2, but not to any of the computers in the VRF1s behind either spoke.

To configure the hub:

```
config router bgp
    set as 65505
    set router-id 11.11.11.11
    set ibgp-multipath enable
    set additional-path enable
    set additional-path-vpnv4 enable
    set cluster-id 11.12.13.14
    set additional-path-select 3
    config neighbor-group
        edit "gr1"
            set capability-graceful-restart enable
            set capability-default-originate enable
            set next-hop-self-rr enable
            set soft-reconfiguration-vpnv4 enable
            set remote-as 65505
            set additional-path both
            set additional-path-vpnv4 both
            set adv-additional-path 3
            set route-reflector-client enable
            set route-reflector-client-vpnv4 enable
        next
        edit "gr2"
            set capability-graceful-restart enable
            set capability-default-originate enable
            set next-hop-self-rr enable
            set soft-reconfiguration-vpnv4 enable
            set remote-as 65505
            set additional-path both
            set additional-path-vpnv4 both
            set adv-additional-path 3
            set route-reflector-client enable
            set route-reflector-client-vpnv4 enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.100.0 255.255.255.0
            set neighbor-group "gr1"
        next
        edit 2
            set prefix 10.10.200.0 255.255.255.0
            set neighbor-group "gr2"
        next
    end
    config network
        edit 12
            set prefix 11.11.11.11 255.255.255.255
        next
        edit 22
            set prefix 11.11.22.11 255.255.255.255
        next
        edit 10
            set prefix 100.1.1.0 255.255.255.0
        next
        edit 33
            set prefix 11.1.1.0 255.255.255.0
        next
    end
    config vrf
        edit "0"
            set role pe
        next
        edit "1"
            set role ce
            set rd "1:1"
            set export-rt "1:1"
            set import-rt "1:1"
        next
        edit "2"
            set role ce
            set rd "2:1"
            set export-rt "2:1"
            set import-rt "2:1"
        next
    end
end
```

```
config vpn ipsec phase1-interface
    edit "p1"
        set type dynamic
        set interface "vd11-vlan1"
        set peertype any
        set net-device disable
        set proposal aes128-sha1
        set add-route disable
        set dpd on-idle
        set dhgrp 5
        set auto-discovery-sender enable
        set auto-discovery-offer-interval 10
        set encapsulation vpn-id-ipip
        set psksecret **********
        set dpd-retryinterval 60
    next
    edit "p2"
        set type dynamic
        set interface "vd11-vlan2"
        set peertype any
        set net-device disable
        set proposal aes128-sha1
        set add-route disable
        set dpd on-idle
        set dhgrp 5
        set auto-discovery-sender enable
        set auto-discovery-offer-interval 10
        set encapsulation vpn-id-ipip
        set psksecret **********
        set dpd-retryinterval 60
    next
end
```

```
config vpn ipsec phase2-interface
    edit "p1"
        set phase1name "p1"
        set proposal aes128-sha1
        set dhgrp 5
    next
    edit "p2"
        set phase1name "p2"
        set proposal aes128-sha1
        set dhgrp 5
    next
end
```

To configure a spoke:

```
config router bgp
    set as 65505
    set router-id 2.2.2.2
    set ebgp-multipath enable
    set ibgp-multipath enable
    set network-import-check disable
    set additional-path enable
    set additional-path6 enable
    set additional-path-vpnv4 enable
    set recursive-next-hop enable
    set graceful-restart enable
    set additional-path-select 4
    config neighbor
        edit "10.10.100.254"
            set capability-dynamic enable
            set capability-graceful-restart-vpnv4 enable
            set soft-reconfiguration enable
            set soft-reconfiguration-vpnv4 enable
            set remote-as 65505
            set additional-path both
            set additional-path-vpnv4 both
            set adv-additional-path 3
        next
        edit "10.10.200.254"
            set capability-dynamic enable
            set capability-graceful-restart-vpnv4 enable
            set soft-reconfiguration enable
            set soft-reconfiguration-vpnv4 enable
            set remote-as 65505
            set additional-path both
            set additional-path-vpnv4 both
            set adv-additional-path 3
        next
    end
    config network
        edit 3
            set prefix 22.1.1.0 255.255.255.0
        next
        edit 4
            set prefix 12.12.12.0 255.255.255.0
        next
    end
    config vrf
        edit "0"
            set role pe
        next
        edit "1"
            set role ce
            set rd "1:1"
            set export-rt "1:1"
            set import-rt "1:1"
        next
        edit "2"
            set role ce
            set rd "2:1"
            set export-rt "2:1"
            set import-rt "2:1"
        next
    end
end
```

```
config vpn ipsec phase1-interface
    edit "vd2-1"
        set interface "vd2-vlan12"
        set peertype any
        set net-device enable
        set proposal aes128-sha1
        set add-route disable
        set dhgrp 5
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set encapsulation vpn-id-ipip
        set remote-gw 11.1.1.11
        set psksecret **********
    next
    edit "vd2-2"
        set interface "vd2-vlan112"
        set peertype any
        set net-device enable
        set proposal aes128-sha1
        set add-route disable
        set dhgrp 5
        set auto-discovery-receiver enable
        set encapsulation vpn-id-ipip
        set remote-gw 11.1.2.11
        set psksecret **********
    next
end
```

```
config vpn ipsec phase2-interface
    edit "vd2-1"
        set phase1name "vd2-1"
        set proposal aes128-sha1
        set dhgrp 5
        set auto-negotiate enable
    next
    edit "vd2-2"
        set phase1name "vd2-2"
        set proposal aes128-sha1
        set dhgrp 5
        set auto-negotiate enable
    next
end
```

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "SASE"
        next
        edit "zon2"
        next
    end
    config members
        edit 1
            set interface "vd2-1"
            set cost 10
        next
        edit 2
            set interface "vd2-2"
            set cost 20
        next
    end
    config health-check
        edit "ping"
            set server "11.11.11.11"
            set members 1 2
            config sla
                edit 1
                    set latency-threshold 200
                    set jitter-threshold 50
                next
            end
        next
        edit "1"
            set server "22.1.1.2"
            set vrf 1
            set members 1 2
        next
    end
    config service
        edit 2
            set mode sla
            set dst "100-200"
            config sla
                edit "ping"
                    set id 1
                next
            end
            set priority-members 2
            set use-shortcut-sla disable
        next
        edit 1
            set name "test-tag"
            set mode sla
            set dst "001-100"
            config sla
                edit "ping"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
```

To check the spoke 1 routes:

```
# get router info routing-table bgp
Routing table for VRF=0
B*      0.0.0.0/0 [200/0] via 10.10.100.254 (recursive via vd2-1 tunnel 11.1.1.11 vrf 0),
04:42:57, [1/0]
                  [200/0] via 10.10.200.254 (recursive via vd2-2 tunnel 11.1.2.11 vrf 0),
04:42:57, [1/0]
B       1.1.1.1/32 [200/0] via 11.1.1.1 [2] (recursive via 12.1.1.1, vd2-vlan12), 04:42:57,
[1/0]
B       1.222.222.222/32 [200/0] via 11.1.1.1 [2] (recursive via 12.1.1.1, vd2-vlan12),
04:42:57, [1/0]
B       11.11.11.11/32 [200/0] via 10.10.100.254 (recursive via vd2-1 tunnel 11.1.1.11 vrf
0), 04:42:57, [1/0]
                       [200/0] via 10.10.200.254 (recursive via vd2-2 tunnel 11.1.2.11 vrf
0), 04:42:57, [1/0]
B       33.1.1.0/24 [200/0] via 10.10.100.254 [2] (recursive via vd2-1 tunnel 11.1.1.11 vrf
0), 04:42:57, [1/0]
                    [200/0] via 10.10.200.254 [2] (recursive via vd2-2 tunnel 11.1.2.11 vrf
0), 04:42:57, [1/0]
B       100.1.1.0/24 [200/0] via 10.10.100.254 (recursive via vd2-1 tunnel 11.1.1.11 vrf 0),
04:42:57, [1/0]
                     [200/0] via 10.10.200.254 (recursive via vd2-2 tunnel 11.1.2.11 vrf 0),
04:42:57, [1/0]

Routing table for VRF=1
B V     33.1.1.0/24 [200/0] via 10.10.100.3 [2] (recursive via vd2-1 tunnel 11.1.1.11 vrf
0), 04:42:57, [1/0]
                    [200/0] via 10.10.200.3 [2] (recursive is directly connected, vd2-2_0),
04:42:57, [1/0]

Routing table for VRF=2
B V     33.1.1.0/24 [200/0] via 10.10.100.3 [2] (recursive via vd2-1 tunnel 11.1.1.11 vrf
0), 04:42:56, [1/0]
                    [200/0] via 10.10.200.3 [2] (recursive is directly connected, vd2-2_0),
04:42:56, [1/0]
```

VRF1 routes:

```
# get router info filter vrf 1
# get router info routing-table bgp
Routing table for VRF=1
B V     33.1.1.0/24 [200/0] via 10.10.100.3 [2] (recursive via vd2-1 tunnel 11.1.1.11 vrf
0), 04:44:11, [1/0]
                    [200/0] via 10.10.200.3 [2] (recursive is directly connected, vd2-2_0),
04:44:11, [1/0]
```

To test the configuration on shortcut 1:

1. From VRF1 of spoke 1 ping VRF1 of spoke 2 and from VRF2 of spoke 1 ping VRF2 spoke 2. Both VRF1 and VRF2 source and destination IP addresses are the same, so you can see how the traffic is isolated
2. Check sessions on spoke 1:

   The output `vd=<vdom ID>:<VRF ID>` indicates that sessions are created in and stay in the corresponding VRFs.

   - User at 22.1.1.22 in VRF1 on spoke 1 pings 33.1.1.33 in VRF1 on spoke2.

     ```
     # diagnose sys session list
     session info: proto=1 proto_state=00 duration=21 expire=42 timeout=0 flags=00000000
     socktype=0 sockport=0 av_idx=0 use=3
     origin-shaper=
     reply-shaper=
     per_ip_shaper=
     class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
     state=may_dirty
     statistic(bytes/packets/allow_err): org=420/5/1 reply=420/5/1 tuples=2
     tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
     orgin->sink: org pre->post, reply pre->post dev=89->131/131->89
     gwy=10.10.200.3/22.1.1.22
     ```

```
hook=pre dir=org act=noop 22.1.1.22:48417->33.1.1.33:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.33:48417->22.1.1.22:0(0.0.0.0:0)
src_mac=02:4c:a5:fc:6a:7f
misc=0 policy_id=1 pol_uuid_idx=566 auth_info=0 chk_client_info=0 vd=1:1
serial=00092eee tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=1
rpdb_link_id=ff000001 ngfwid=n/a
npu_state=0x5040001 no_offload
no_ofld_reason:  disabled-by-policy non-npu-intf
```

- User at 22.1.1.22 in VRF2 on spoke 1 pings 33.1.1.33 in VRF2 on spoke2:

```
# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=56 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 39/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=113->131/131->113
gwy=10.10.200.3/22.1.1.22
hook=pre dir=org act=noop 22.1.1.22:55841->33.1.1.33:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.33:55841->22.1.1.22:0(0.0.0.0:0)
src_mac=02:4c:a5:fc:6a:7f
misc=0 policy_id=1 pol_uuid_idx=566 auth_info=0 chk_client_info=0 vd=1:2
serial=00092f77 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=1
rpdb_link_id=ff000001 ngfwid=n/a
npu_state=0x5040001 no_offload
no_ofld_reason:  disabled-by-policy non-npu-intf
```

3. Check sessions on spoke 2:

   The output `vd=<vdom ID>:<VRF ID>` indicates that sessions are created in and stay in the corresponding VRFs.

   - User at 22.1.1.22 in VRF1 on spoke 1 pings 33.1.1.33 in VRF1 on spoke 2:

```
# diagnose sys session list
session info: proto=1 proto_state=00 duration=11 expire=49 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 14/0 rx speed(Bps/kbps): 14/0
orgin->sink: org pre->post, reply pre->post dev=132->92/92->132
gwy=33.1.1.33/10.10.200.2
hook=pre dir=org act=noop 22.1.1.22:27733->33.1.1.33:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.33:27733->22.1.1.22:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=630 auth_info=0 chk_client_info=0 vd=6:1
serial=000a29fd tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000001 no_offload
```

```
npu info: flag=0x00/0x82, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  disabled-by-policy
```

- User at 22.1.1.22 in VRF2 on spoke 1 pings 33.1.1.33 in VRF2 on spoke 2:

```
# diagnose sys session list
session info: proto=1 proto_state=00 duration=17 expire=43 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 9/0 rx speed(Bps/kbps): 9/0
orgin->sink: org pre->post, reply pre->post dev=132->115/115->132
gwy=33.1.1.33/10.10.200.2
hook=pre dir=org act=noop 22.1.1.22:24917->33.1.1.33:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.33:24917->22.1.1.22:0(0.0.0.0:0)
dst_mac=02:4c:a5:fc:6a:7f
misc=0 policy_id=1 pol_uuid_idx=630 auth_info=0 chk_client_info=0 vd=6:2
serial=000a29ca tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000001 no_offload
npu info: flag=0x00/0x82, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  disabled-by-policy
```

To test the configuration on shortcut 2:

1. From VRF1 of spoke 1 ping VRF1 of spoke 2 and from VRF2 of spoke 1 ping VRF2 spoke 2. Both VRF1 and VRF2 source and destination IP addresses are the same, so you can see how the traffic is isolated
2. Check sessions on spoke 1:

   The output `vd=<vdom ID>:<VRF ID>` indicates that sessions are created in and stay in the corresponding VRFs.

   - User at 22.1.1.22 in VRF1 on spoke 1 pings 33.1.1.133 in VRF1 on spoke 2:

```
# diagnose sys session listsession info: proto=1 proto_state=00 duration=17 expire=45
timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=336/4/1 reply=336/4/1 tuples=2
tx speed(Bps/kbps): 19/0 rx speed(Bps/kbps): 19/0
orgin->sink: org pre->post, reply pre->post dev=89->137/137->89
gwy=10.10.200.3/22.1.1.22
hook=pre dir=org act=noop 22.1.1.22:25968->33.1.1.133:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.133:25968->22.1.1.22:0(0.0.0.0:0)
src_mac=02:4c:a5:fc:6a:7f
misc=0 policy_id=1 pol_uuid_idx=566 auth_info=0 chk_client_info=0 vd=1:1
serial=000aa475 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=2
```

```
rpdb_link_id=ff000002 ngfwid=n/a
npu_state=0x5040001 no_offload
no_ofld_reason:  disabled-by-policy non-npu-intf
```

- User at 22.1.1.22 in VRF2 on spoke 1 pings 33.1.1.133 in VRF2 on spoke 2:

```
# diagnose sys session listsession info: proto=1 proto_state=00 duration=8 expire=53
timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=252/3/1 reply=252/3/1 tuples=2
tx speed(Bps/kbps): 30/0 rx speed(Bps/kbps): 30/0
orgin->sink: org pre->post, reply pre->post dev=113->137/137->113
gwy=10.10.200.3/22.1.1.22
hook=pre dir=org act=noop 22.1.1.22:28528->33.1.1.133:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.133:28528->22.1.1.22:0(0.0.0.0:0)
src_mac=02:4c:a5:fc:6a:7f
misc=0 policy_id=1 pol_uuid_idx=566 auth_info=0 chk_client_info=0 vd=1:2
serial=000aa49f tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=2
rpdb_link_id=ff000002 ngfwid=n/a
npu_state=0x5040001 no_offload
no_ofld_reason:  disabled-by-policy non-npu-intf
```

3. Check sessions on spoke 2:

   The output `vd=<vdom ID>:<VRF ID>` indicates that sessions are created in and stay in the corresponding VRFs.

   - User at 22.1.1.22 in VRF1 on spoke 1 pings 33.1.1.133 in VRF1 on spoke 2:

```
# diagnose sys session list
session info: proto=1 proto_state=00 duration=24 expire=38 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=336/4/1 reply=336/4/1 tuples=2
tx speed(Bps/kbps): 13/0 rx speed(Bps/kbps): 13/0
orgin->sink: org pre->post, reply pre->post dev=138->92/92->138
gwy=33.1.1.133/10.10.200.2
hook=pre dir=org act=noop 22.1.1.22:25968->33.1.1.133:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.133:25968->22.1.1.22:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=630 auth_info=0 chk_client_info=0 vd=6:1
serial=000aa476 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000001 no_offload
npu info: flag=0x00/0x82, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  disabled-by-policy
```

   - User at 22.1.1.22 in VRF2 on spoke 1 pings 33.1.1.133 in VRF2 on spoke2:

```
# diagnose sys session list
session info: proto=1 proto_state=00 duration=15 expire=46 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=252/3/1 reply=252/3/1 tuples=2
tx speed(Bps/kbps): 16/0 rx speed(Bps/kbps): 16/0
orgin->sink: org pre->post, reply pre->post dev=138->115/115->138
gwy=33.1.1.133/10.10.200.2
hook=pre dir=org act=noop 22.1.1.22:28528->33.1.1.133:8(0.0.0.0:0)
hook=post dir=reply act=noop 33.1.1.133:28528->22.1.1.22:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=630 auth_info=0 chk_client_info=0 vd=6:2
serial=000aa4a0 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000001 no_offload
npu info: flag=0x00/0x82, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  disabled-by-policy
```

Example 2

In this example, SLA health checks are sent from a spoke's VRF to the loopback on the hub that is in the same VRF.

To configure the health check:

```
config system sdwan
    config health-check
        edit "1"
            set server "11.11.22.11"
            set vrf 1
            set source 22.1.1.2
            set members 1 2
            config sla
                edit 1
                    set latency-threshold 200
                    set jitter-threshold 50
                next
            end
        next
    end
end
```

To check the health check status:

```
# diagnose sys sdwan health-check status  1
Health Check(1):
Seq(1 vd2-1): state(alive), packet-loss(0.000%) latency(0.023), jitter(0.002), mos(4.404),
bandwidth-up(0), bandwidth-dw(0), bandwidth-bi(0) sla_map=0x1
Seq(2 vd2-2): state(alive), packet-loss(0.000%) latency(0.022), jitter(0.002), mos(4.404),
bandwidth-up(0), bandwidth-dw(0), bandwidth-bi(0) sla_map=0x1
```

Example 3

In this example, when traffic from spoke 1 arrives at the hub on tunnel 1, it will egress the hub on tunnel 1 to go to other spokes. If traffic arrives on tunnel 2, it will egress on tunnel 2, and not tunnel 1.

To configure SD-WAN on the hub:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
            set service-sla-tie-break input-device
        next
    end
    config members
        edit 1
            set interface "p1"
        next
        edit 2
            set interface "p2"
        next
    end
    config health-check
        edit "1"
            set server "22.1.1.2"
            set members 1 2
            config sla
                edit 1
                next
            end
        next
    end
    config service
        edit 1
            set mode sla
            set dst "all"
            config sla
                edit "1"
                    set id 1
                next
            end
            set priority-members 1 2
            set tie-break input-device
        next
    end
end
```

To verify that traffic stays in the same overlay on ingress and egress on the hub:

1. Confirm that the SD-WAN service rule has `Tie break` set to `input-device` so that, when SLAs are met on all of the members, traffic prefers to egress on the same member as the input device:

   ```
   # diagnose sys sdwan service

   Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
   ```

```
Tie break: input-device
 Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
 Members(2):
   1: Seq_num(1 p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
   2: Seq_num(2 p2), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
 Dst address(1):
       0.0.0.0-255.255.255.255
```

2. Use `diagnose sniffer packet` commands to verify that traffic ingress and egress are on the same overlay.

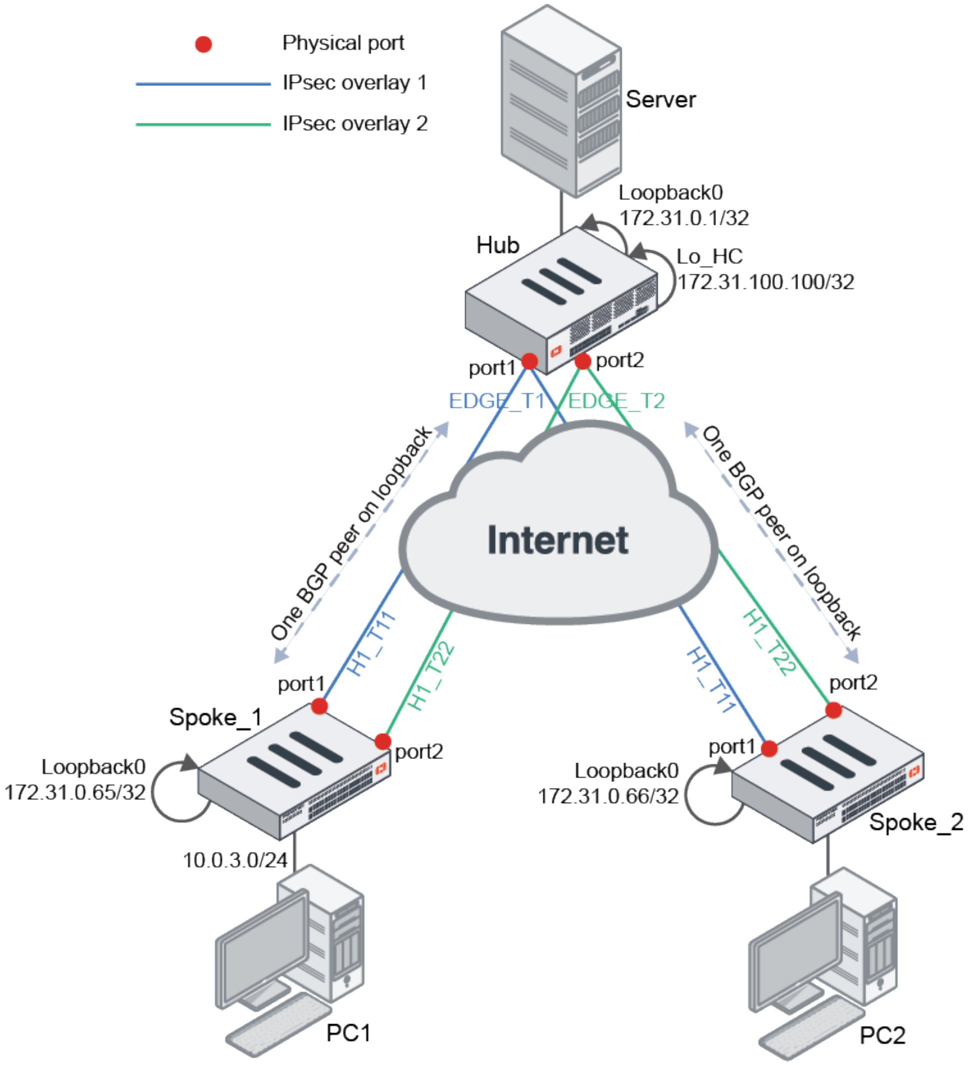
Embedded SD-WAN SLA information in ICMP probes - 7.2.1

In the hub and spoke SD-WAN design, in order for traffic to pass symmetrically from spoke to hub and hub to spoke, it is essential for the hub to know which IPsec overlay is in SLA and out of SLA. Prior to introducing embedded SLA information in ICMP probes, it is common practice for spokes to use the SD-WAN neighbor feature and `route-map-out-preferable` setting to signal the health of each overlay to the hub. However, this requires BGP to be configured per overlay, and to manipulate BGP routes using custom BGP communities.

With embedded SLA information in ICMP probes, spokes can communicate their SLA for each overlay directly through ICMP probes to the hub. The hub learns these SLAs and maps the status for each spoke and its corresponding overlays.

The hub uses the SLA status to apply priorities to the IKE routes, giving routes over IPsec overlays that are within SLAs a lower priority value and routes over overlays out of SLAs a higher priority value. If BGP is used, recursively resolved BGP routes can inherit the priority from its parent.

Embedded SLA information in ICMP probes allows hub and spoke SD-WAN to be designed with a BGP on loopback topology, or without BGP at all. The following topology outlines an example of the BGP on loopback design where each spoke is peered with the hub and route reflector on the loopback interface.



In this topology, each FortiGate's BGP router ID is based on its Loopback0 interface. Each spoke has SLA health checks defined to send ICMP probes to the server's Lo_HC interface on 172.31.100.100. The ICMP probes include embedded SLA information for each SD-WAN overlay member.

Related SD-WAN settings:

```
config system sdwan
    config health-check
        edit <name>
            set detect-mode {active | passive | prefer-passive | remote}
            set embed-measured-health {enable | disable}
            config sla
                edit <id>
                    set priority-in-sla <integer>
                    set priority-out-sla <integer>
                next
            end
            set sla-id-redistribute <id>
        next
    end
end
```

`detect-mode {active | passive | prefer-passive | remote}`	Set the mode that determines how to detect the server: • `active`: the probes are sent actively (default). • `passive`: the traffic measures health without probes. • `prefer-passive`: the probes are sent in case of no new traffic. • `remote`: the link health is obtained from remote peers.
`embed-measured-health {enable | disable}`	Enable/disable embedding SLA information in ICMP probes (default = disable).
`set priority-in-sla <integer>`	Set the priority that will be set to the IKE route when the corresponding overlay is in SLA (0 - 65535).
`set priority-out-sla <integer>`	Set the priority that will be set to the IKE route when the corresponding overlay is out of SLA (0 - 65535).
`sla-id-redistribute <id>`	Set the SLA entry (ID) that will be applied to the IKE routes (0 - 32, default = 0).

Related BGP setting:

```
config router bgp
    set recursive-inherit-priority {enable | disable}
end
```

`recursive-inherit-priority {enable | disable}`	Enable/disable allowing recursive resolved BGP routes to inherit priority from its parent (default = disable).

Example with BGP on loopback SD-WAN

This example demonstrates the configurations needed to configure the SD-WAN and BGP settings for the preceding topology. It is assumed that IPsec VPN overlays are already configured per the topology, and that loopback interfaces are already configured on each FortiGate.

Configuring the Spoke_1 FortiGate

In the SD-WAN settings, note the following requirements:

1. Configure the SD-WAN zones and members. For each SD-WAN member, define the source of its probes to be the Loopback0 interface IP.
2. Configure the SLA health check to point to the Hub's Lo_HC interface and IP. Enable `embed-measured-health`.
3. Configure an SD-WAN service rule to route traffic based on the maximize bandwidth (SLA) algorithm to prefer member H1_T11 over H1_T22.
4. Configure `set exchange-interface-ip enable` and `set exchange-ip-addr4` to the Loopback0 interface IP. The `exchange-interface-ip option` is automatically turned on when ADVPN has already been configured. If ADVPN has not been configured, then `set exchange-interface-ip enable` must be configured before `set exchange-ip-addr4` can be configured.

To configure the SD-WAN settings:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "overlay"
        next
    end
    config members
        edit 1
            set interface "H1_T11"
            set zone "overlay"
            set source 172.31.0.65
        next
        edit 4
            set interface "H1_T22"
            set zone "overlay"
            set source 172.31.0.65
        next
    end
    config health-check
        edit "HUB"
            set server "172.31.100.100"
            set embed-measured-health enable
            set members 0
            config sla
                edit 1
                    set link-cost-factor latency
                    set latency-threshold 100
                next
            end
        next
    end
    config service
        edit 1
            set mode sla
            set dst "CORP_LAN"
            set src "CORP_LAN"
            config sla
                edit "HUB"
                    set id 1
                next
            end
            set priority-members 1 4
        next
    end
end
```

To configure the BGP settings:

```
config router bgp
    set as 65001
    set router-id 172.31.0.65
    config neighbor
```

```
        edit "172.31.0.1"
            set remote-as 65001
            set update-source "Loopback0"
        next
    end
    config network
        edit 1
            set prefix 10.0.3.0 255.255.255.0
        next
    end
end
```

To add the loopback IP to the IPsec interface settings:

```
config vpn ipsec phase1-interface
    edit "H1_T11"
        set exchange-interface-ip enable
        set exchange-ip-addr4 172.31.0.65
    next
    edit "H1_T22"
        set exchange-interface-ip enable
        set exchange-ip-addr4 172.31.0.65
    next
end
```

Configuring the hub FortiGate

In the SD-WAN settings, note the following requirements:

1. Configure the SD-WAN zone and members.
2. Configure the SLA health checks to detect SLAs based on the remote site (spoke). This must be defined for each SD-WAN member:
   a. For the SLA, specify the same link cost factor and metric as the spoke (100).
   b. Define the IKE route priority for in and out of SLA. Lower priority values have higher priority than higher priority values.
3. Define the SLA entry ID that will be applied to the IKE routes.
4. Configure `set exchange-interface-ip enable` and `set exchange-ip-addr4` to the Loopback0 interface IP. The `exchange-interface-ip option` is automatically turned on when ADVPN has already been configured. If ADVPN has not been configured, then `set exchange-interface-ip enable` must be configured before `set exchange-ip-addr4` can be configured.

To configure the SD-WAN settings:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "EDGE_T1"
        next
        edit 2
```

```
            set interface "EDGE_T2"
        next
    end
    config health-check
        edit "1"
            set detect-mode remote
            set sla-id-redistribute 1
            set members 1
            config sla
                edit 1
                    set link-cost-factor latency
                    set latency-threshold 100
                    set priority-in-sla 10
                    set priority-out-sla 20
                next
            end
        next
        edit "2"
            set detect-mode remote
            set sla-id-redistribute 1
            set members 2
            config sla
                edit 1
                    set link-cost-factor latency
                    set latency-threshold 100
                    set priority-in-sla 15
                    set priority-out-sla 25
                next
            end
        next
    end
end
```

In the BGP settings, note the following requirements:

1. Enable `recursive-inherit-priority` to inherit the route priority from its parent, which is the priority defined in the health check SLA settings.
2. Configure the other BGP settings similar to a regular BGP hub.

To configure the BGP settings:

```
config router bgp
    set as 65001
    set router-id 172.31.0.1
    set recursive-inherit-priority enable
    config neighbor-group
        edit "EDGE"
            set remote-as 65001
            set update-source "Loopback0"
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 172.31.0.64 255.255.255.192
            set neighbor-group "EDGE"
        next
    end
end
```

To add the loopback IP to the IPsec interface settings:

```
config vpn ipsec phase1-interface
    edit "EDGE_T1"
        set exchange-interface-ip enable
        set exchange-ip-addr4 172.31.0.1
    next
    edit "EDGE_T2"
        set exchange-interface-ip enable
        set exchange-ip-addr4 172.31.0.1
    next
end
```

Testing and verification

Once the hub and spokes are configured, verify that SLA statuses are passed from the spoke to the hub.

To verify that the SLA statuses are passed from the spoke to the hub:

1. On Spoke_1, display the status of the health-checks for H1_T11 and H1_T22:

```
# diagnose sys sdwan  health-check
Health Check(HUB):
Seq(1 H1_T11): state(alive), packet-loss(0.000%) latency(0.228), jitter(0.018), mos
(4.404), bandwidth-up(999999), bandwidth-dw(1000000), bandwidth-bi(1999999) sla_map=0x1
Seq(4 H1_T22): state(alive), packet-loss(0.000%) latency(0.205), jitter(0.007), mos
(4.404), bandwidth-up(999998), bandwidth-dw(1000000), bandwidth-bi(1999998) sla_map=0x1
```

2. On Spoke_1, display the status and order of the overlays in the SD-WAN service rule:

```
# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(1 H1_T11), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected

    2: Seq_num(4 H1_T22), alive, sla(0x1), gid(0), cfg_order(3), local cost(0), selected

  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        10.0.0.0-10.255.255.255
```

   Both overlays are within SLA, so H1_T11 is preferred due to its `cfg-order`.

   Spoke_1's SLA information for H1_T11 and H1_T22 is embedded into the ICMP probes destined for the hub's Lo_HC interface. The hub receives this information and maps the SLAs correspondingly per spoke and overlay based on the same SLA targets.

   As a result, since all SLAs are within target, the hub sets the routes over each overlay as follows:

Hub SD-WAN member	Overlay	SLA status	Priority for IKE routes
1	EDGE_T1	0x1 – within SLA	10
2	EDGE_T2	0x1 – within SLA	15

Simultaneously, BGP recursive routes inherit the priority based on the parent IKE routes. The recursively resolved BGP routes that pass through EDGE_T1 will have a priority of 10, and routes that pass through EDGE_T2 will have a priority of 15. Therefore, traffic from the hub to spoke will be routed to EDGE_T1.

3. Verify the routing tables.
   a. Static:

```
# get router info routing-table static
Routing table for VRF=0
S       172.31.0.65/32 [15/0] via EDGE_T1 tunnel 10.0.0.69 vrf 0, [10/0]
                                  [15/0] via EDGE_T2 tunnel 172.31.0.65 vrf 0, [15/0]
```

   b. BGP:

```
# get router info routing-table bgp
Routing table for VRF=0
B       10.0.3.0/24 [200/0] via 172.31.0.65 (recursive via EDGE_T1 tunnel 10.0.0.69
vrf 0 [10]), 04:32:53
                                            (recursive via EDGE_T2 tunnel 172.31.0.65
vrf 0 [15]), 04:32:53, [1/0]
```

Next, test by making the health checks over the spokes' H1_T11 tunnel out of SLA. This should trigger traffic to start flowing from the spokes' H1_T22 tunnel. Consequently, the SLA statuses are passed from the spoke to the hub, and the hub will start routing traffic to EDGE_T2.

To verify that the hub will start routing traffic to EDGE_T2 when the spoke H1_T11 tunnel is out of SLA:

1. On Spoke_1, display the status of the health checks for H1_T11 and H1_T22:

```
# diagnose sys sdwan health-check
Health Check(HUB):
Seq(1 H1_T11): state(alive), packet-loss(0.000%) latency(120.228), jitter(0.013), mos
(4.338), bandwidth-up(999999), bandwidth-dw(1000000), bandwidth-bi(1999999) sla_map=0x0
Seq(4 H1_T22): state(alive), packet-loss(0.000%) latency(0.220), jitter(0.008), mos
(4.404), bandwidth-up(999998), bandwidth-dw(1000000), bandwidth-bi(1999998) sla_map=0x1
```

2. Verify the routing tables.
   a. Static:

```
# get router info routing-table static
Routing table for VRF=0
S       172.31.0.65/32 [15/0] via EDGE_T2 tunnel 172.31.0.65 vrf 0, [15/0]
                       [15/0] via EDGE_T1 tunnel 10.0.0.69 vrf 0, [20/0]
```

   The priority for EDGE_T1 has changed from 10 to 20.

   b. BGP:

```
# get router info routing-table bgp
Routing table for VRF=0
B       10.0.3.0/24 [200/0] via 172.31.0.65 (recursive via EDGE_T2 tunnel 172.31.0.65
vrf 0 [15]), 00:01:19
```

```
                                                   (recursive via EDGE_T1 tunnel 10.0.0.69
        vrf 0 [20]), 00:01:19, [1/0]
```

EDGE_T2 is now preferred. The priority for EDGE_T1 has changed from 10 to 20.

Spoke_1's SLA information for H1_T11 embedded into the ICMP probes has now changed.

As a result, the hub sets the routes over each overlay as follows:

Hub SD-WAN member	Overlay	SLA status	Priority for IKE routes
1	EDGE_T1	0x0 – out of SLA	20
2	EDGE_T2	0x1 – within SLA	15

The BGP recursive routes inherit the priority based on the parent IKE routes. Since priority for IKE routes on EDGE_T1 has changed to 20, recursively resolved BGP routes passing through EDGE_T1 has also dropped to 20. As a result, hub to spoke_1 traffic will go over EDGE_T2.

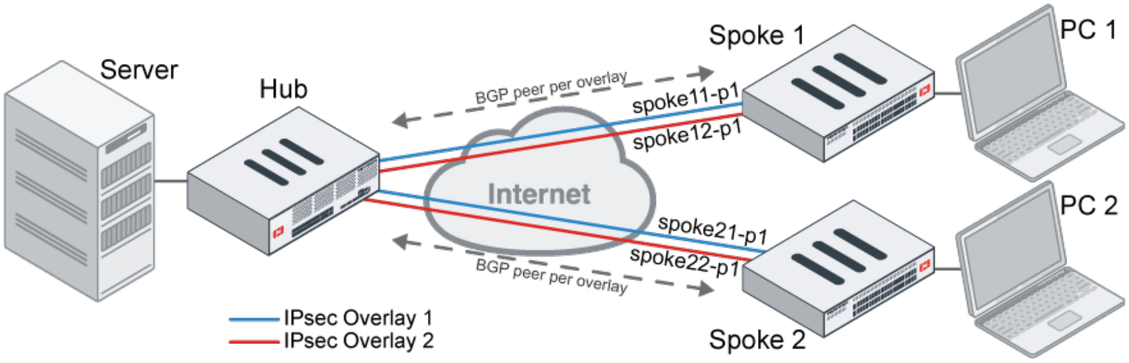
Exchange underlay link cost property with remote peer in IPsec VPN phase 1 negotiation - 7.2.1

The underlay link cost property has been added to the IPsec VPN tunnel phase 1 configuration and enhances the IPsec VPN to exchange the link cost with a remote peer as a private notify payload in IKEv1 and IKEv2 phase 1 negotiations. This avoids possible health check daemon process load issues in the previous implementation of the link cost exchange feature, and it improves network scalability in a large-scale SD-WAN network with ADVPN.

```
config vpn ipsec phase1-interface
    edit <name>
        set link-cost <integer>
    next
end
```

`link-cost <integer>`	Set the VPN underlay link cost (0 - 255, default = 0).

If multiple shortcuts originate from the same SD-WAN member to different members on the same remote spoke, learned remote IPsec link costs on shortcuts will be used as a tie-breaker to decide which shortcut is preferred.



In this example, SD-WAN is configured on an ADVPN network with a BGP neighbor per overlay.

Instead of reflecting BGP routes with the route-reflector on the hub, when the shortcuts are triggered, IKE routes on the shortcuts are directly injected based on the configured phase 2 selectors to allow routes to be exchanged between spokes.

Routes between the hub and the spokes are exchanged by BGP, and the spokes use the default route to send spoke-to-spoke traffic to the hub and trigger the shortcuts.

To configure Spoke 1:

1. Configure the VPN remote gateway:

```
config vpn ipsec phase1-interface
    edit "spoke11-p1"
        ...
        set mode-cfg-allow-client-selector enable
        set link-cost 11
    next
    edit "spoke12-p1"
        ...
        set mode-cfg-allow-client-selector enable
        set link-cost 21
    next
end
```

2. Configure the SD-WAN settings:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "spoke11-p1"
            set cost 10
        next
        edit 2
            set interface "spoke12-p1"
            set cost 20
        next
    end
    config health-check
        edit "1"
            set server "9.0.0.1"
            set members 0
            config sla
                edit 1
                next
            end
        next
    end
    config service
        edit 1
            set name "1"
            set mode sla
            set dst "all"
            set src "10.1.100.0"
            config sla
                edit "1"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
```

To configure Spoke 2:

1. Configure the VPN remote gateway:

```
config vpn ipsec phase1-interface
    edit "spoke21-p1"
        ...
        set link-cost 101
    next
    edit "spoke22-p1"
        ...
        set link-cost 201
    next
end
```

2. Configure the SD-WAN settings:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "spoke21-p1"
            set cost 10
        next
        edit 2
            set interface "spoke22-p1"
            set cost 20
        next
    end
    config health-check
        edit "1"
            set server "9.0.0.1"
            set members 0
            config sla
                edit 1
                next
            end
        next
    end
    config service
        edit 1
            set name "1"
```

```
                set mode sla
                set dst "all"
                set src "192.168.5.0"
                config sla
                    edit "1"
                        set id 1
                    next
                end
                set priority-members 1 2
            next
        end
    end
```

To test the configuration:

1. Verify the service diagnostics on Spoke 1:

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(1 spoke11-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(10),
selected
    2: Seq_num(2 spoke12-p1), alive, sla(0x1), gid(0), cfg_order(1), local cost(20),
selected
  Src address(1):
        10.1.100.0-10.1.100.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

2. Verify the service diagnostics on Spoke 2:

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(1 spoke21-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(10),
selected
    2: Seq_num(2 spoke22-p1), alive, sla(0x1), gid(0), cfg_order(1), local cost(20),
selected
  Src address(1):
        192.168.5.0-192.168.5.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

3. Trigger shortcuts between Spoke 1 and Spoke 2:
   - Shortcuts spoke11-p1_1 and spoke11-p1_0 originate from spoke11-p1.
   - spoke11-p1_1 corresponds to spoke21-p1_0 on Spoke 2.
   - spoke11-p1_0 corresponds to spoke22-p1_0 on Spoke 2.

   Spoke 1:

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(11), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Member sub interface(4):
    3: seq_num(1), interface(spoke11-p1):
       1: spoke11-p1_0(80)
       2: spoke11-p1_1(81)
  Members(4):
    1: Seq_num(1 spoke11-p1_1), alive, sla(0x1), gid(0), remote cost(101), cfg_order(0),
local cost(10), selected
    2: Seq_num(1 spoke11-p1_0), alive, sla(0x1), gid(0), remote cost(201), cfg_order(0),
local cost(10), selected
    3: Seq_num(1 spoke11-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(10),
selected
    4: Seq_num(2 spoke12-p1), alive, sla(0x1), gid(0), cfg_order(1), local cost(20),
selected
  Src address(1):
        10.1.100.0-10.1.100.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

Spoke 2:

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(15), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Member sub interface(4):
    2: seq_num(1), interface(spoke21-p1):
       1: spoke21-p1_0(75)
    4: seq_num(2), interface(spoke22-p1):
       1: spoke22-p1_0(74)
  Members(4):
    1: Seq_num(1 spoke21-p1_0), alive, sla(0x1), gid(0), remote cost(11), cfg_order(0),
local cost(10), selected
    2: Seq_num(1 spoke21-p1), alive, sla(0x1), gid(0), cfg_order(0), local cost(10),
selected
    3: Seq_num(2 spoke22-p1_0), alive, sla(0x1), gid(0), remote cost(11), cfg_order(1),
local cost(20), selected
    4: Seq_num(2 spoke22-p1), alive, sla(0x1), gid(0), cfg_order(1), local cost(20),
selected
  Src address(1):
        192.168.5.0-192.168.5.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

The spoke11-p1_1 shortcut on Spoke 1 is preferred over spoke11-p1_0 due to the lower remote link cost of 101 when they have the same local SD-WAN member cost of 10.

4. Verify the policy route list on Spoke 1:

```
# diagnose firewall proute list
list route policy info(vf=root):
```

```
id=2131755009(0x7f100001) vwl_service=1(1) vwl_mbr_seq=1 1 1 2 dscp_tag=0xfc 0xfc
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path
(4) oif=81(spoke11-p1_1) oif=80(spoke11-p1_0) oif=54(spoke11-p1) oif=55(spoke12-p1)
source(1): 10.1.100.0-10.1.100.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=176 last_used=2022-07-12 11:56:08
```

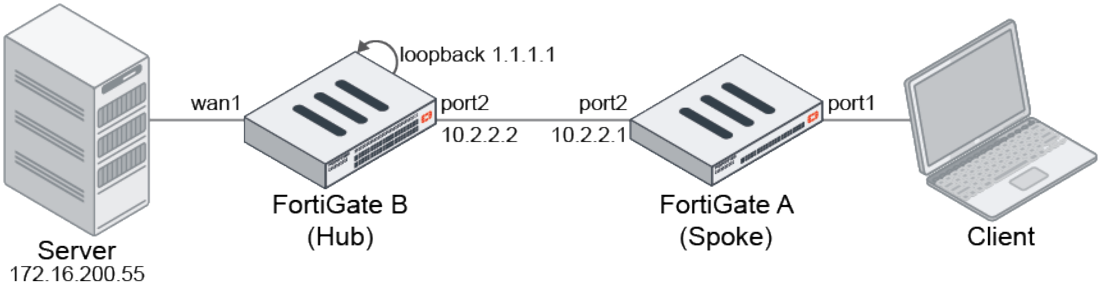
Copying the DSCP value from the session original direction to its reply direction - 7.2.1

In an SD-WAN scenario when DSCP tags are used to mark traffic from the spoke to the hub, it is sometimes desirable for the hub to mark the reply traffic with the same DSSP tags. The `diffserv-copy` setting in firewall policy configurations allows the DSCP tag to be copied to the reply direction.

```
config firewall policy
    edit <id>
        set diffserv-copy {enable | disable}
    next
end
```

Example

The use cases in this example are for a hub and spoke SD-WAN deployment. Traffic from the spoke (either real traffic or SLA health check probes) can be marked with a certain DSCP tag when leaving the spoke. QoS may be applied by an upstream device based on the DSCP tag. When the traffic arrives on the hub, the hub may also want to mark the reply traffic to the spoke with the same DSCP tag. This would allow QoS to be applied to the traffic in the reply direction as well, which is traffic in the hub to spoke direction associated with the same session in the spoke to hub direction.



While this topology simplifies the SD-WAN deployment into a single hub and spoke, this feature applies to the following configurations:

- Multiple spokes (branch sites)
- One or more hubs (data center sites)
- Multiple overlays connecting spokes to hubs
- SD-WAN configured on spokes to pick the best overlay

Use case 1: typical forwarding traffic

Traffic originates from the spoke and is destined for a server behind the hub. The spoke marks the traffic with a DSCP tag of 101010. This is done by enabling `diffserv-foward` on the spoke firewall policy. It can also be accomplished by enabling `dscp-forward` in an SD-WAN rule.

The hub allows the traffic in through a firewall policy. By enabling `diffserv-copy` on the firewall policy, it will mark the reply traffic on the corresponding sessions with the same DSCP tag in which it came.

To configure the FortiGates:

1. Configure the firewall policy on the spoke (FortiGate A):

```
config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all6"
        set dstaddr6 "all6"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set diffserv-forward enable
        set diffservcode-forward 101010
    next
end
```

2. Configure the firewall policy on the hub (FortiGate B):

```
config firewall policy
    edit 3
        set srcintf "virtual-wan-link"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
        set diffserv-copy enable
    next
end
```

To test the configuration:

1. Generate some forwarding traffic.
2. Verify that the session's `tos` value from the original direction is applied to the reply direction:

```
# diagnose sys session filter policy 3
# diagnose sys session filter dst 172.16.200.55
# diagnose sys session list

session info: proto=1 proto_state=00 duration=35 expire=59 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
```

```
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=3024/36/1 reply=3024/36/1 tuples=2
tx speed(Bps/kbps): 82/0 rx speed(Bps/kbps): 82/0
orgin->sink: org pre->post, reply pre->post dev=20->17/17->20 gwy=172.16.200.55/10.2.2.1
hook=post dir=org act=snat 10.2.2.1:25290->172.16.200.55:8(172.16.200.2:25290)
hook=pre dir=reply act=dnat 172.16.200.55:25290->172.16.200.2:0(10.2.2.1:25290)
misc=0 policy_id=3 pol_uuid_idx=1097 auth_info=0 chk_client_info=0 vd=3
serial=0000a018 tos=6a/6a app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000001 no_offload
no_ofld_reason:  disabled-by-policy
total session 1
```

Use case 2: local-in traffic destined to a loopback interface

SLA health checks from the spoke are destined for a loopback interface on the hub. The health check is marked with a DSCP tag of 000001 by the spoke. When the hub receives the probes to its loopback, it will mark the replies with the same DSCP tags in which it came.

To configure the FortiGates:

1. Configure the health check on the spoke (FortiGate A):

```
config system sdwan
    config health-check
        edit "ping"
            set server "1.1.1.1"
            set diffservcode 000001
        set members 0
    next
end
```

2. Configure the loopback interface on the hub (FortiGate B):

```
config system interface
    edit "loopback"
        set vdom "vdom1"
        set ip 1.1.1.1 255.255.255.255
        set allowaccess ping https ssh  http telnet
        set type loopback
        set role lan
        set snmp-index 35
    next
end
```

3. Configure the firewall policy on the hub:

```
config firewall policy
    edit 1
        set srcintf "virtual-wan-link"
        set dstintf "loopback"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
        set diffserv-copy enable
    next
end
```

To test the configuration:

1. Generate some local-in traffic.
2. Verify that the session's `tos` value from the original direction is applied to the reply direction:

```
# diagnose sys session list

session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log local may_dirty
statistic(bytes/packets/allow_err): org=80/2/1 reply=80/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->in, reply out->post dev=20->42/42->20 gwy=1.1.1.1/0.0.0.0
hook=pre dir=org act=noop 10.2.2.1:15->1.1.1.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 1.1.1.1:15->10.2.2.1:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=3
serial=0001a846 tos=41/41 app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x000001 no_offload
no_ofld_reason:  local disabled-by-policy
total session 1
```

Capture packets can also be used verify that the DSCP value from the original direction is applied to the reply direction.

Matching BGP extended community route targets in route maps - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Matching BGP extended community route targets in route maps

BGP extended community route targets can be matched in route maps. This can be applied in a scenario where the BGP route reflector receives routes from many VRFs, and instead of reflecting all routes from all VRFs, users only want to reflect routes based on a specific extended community route target.

To configure the extended community list:

```
config router extcommunity-list
    edit <name>
        set type {standard | expanded}
        config rule
            edit <id>
                set action {deny | permit}
                set type {rt | soo}
                set match <extended_community_specifications>
                set regexp <ordered_list_of_attributes>
            next
        end
    next
end
```

`type {standard | expanded}`	Set the extended community list type (standard or expanded).
`action {deny | permit}`	Deny or permit route-based operations based on the route's extended community attribute.
`type {rt | soo}`	Set the extended community type: • rt: route target • soo: site of origin
`match <extended_community_specifications>`	Set the extended community specifications for matching a reserved extended community (community number in AA:NN format; use quotation marks complex expressions, "`123:234 345:456`").
`regexp <ordered_list_of_attributes>`	Set the ordered list of extended community attributes as a regular expression.

To configure the BGP extended community list in the route map:

```
config router route-map
    edit <name>
        config rule
            edit <id>
                set match-extcommunity <list>
                set match-extcommunity-exact {enable | disable}
            next
        end
    next
end
```

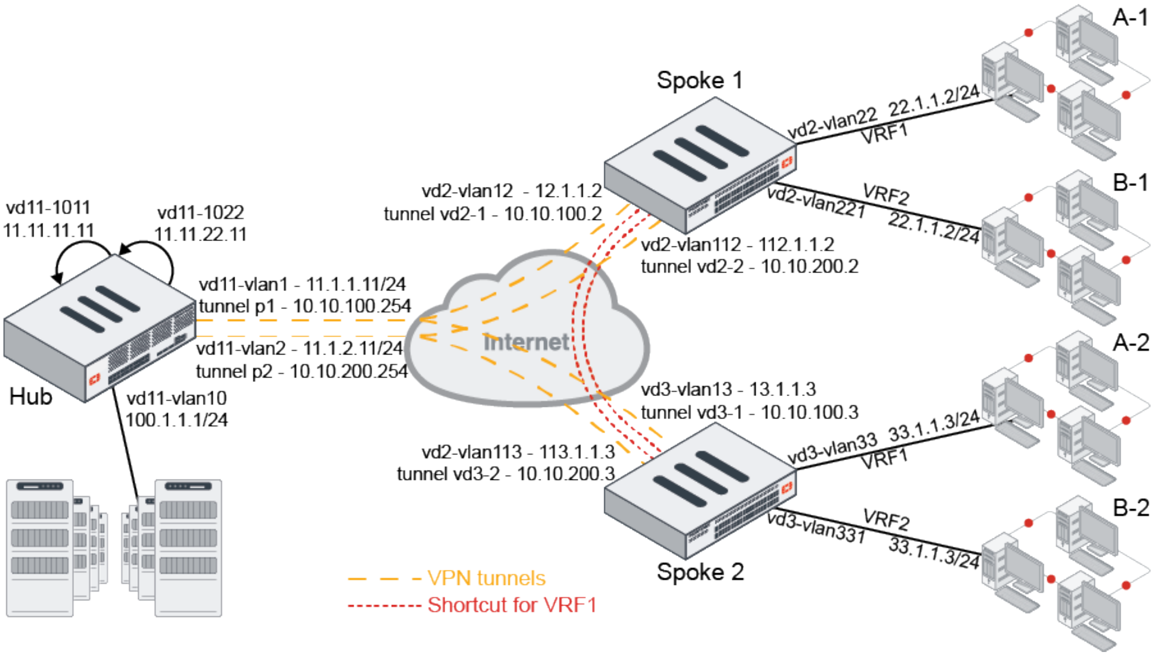
`match-extcommunity <list>`	Set the BGP extended community list to match to.
`match-extcommunity-exact {enable | disable}`	Enable/disable exact matching of extended communities.

Example

In this example, multiple companies (or departments of a company) share the same hub and spoke VPN infrastructure. Company A and company B each have two branches in two different locations. The goal is for company A's branches (A-

1 and A-2) to be able to communicate only with each other over VPN but not with company B’s branches. Likewise, company B’s branches (B-1 and B-2) can only communicate with each other over VPN but not with company A’s. This is accomplished by placing each branch VLAN into their respective VRFs (VRF1 and VRF2), and encapsulating the VRF information within the VPN tunnel. The hub forms BGP peering with its neighbors, spoke 1 and spoke 2, over each IPsec overlay. The hub’s BGP route reflector reflects the routes to the corresponding VRFs, allowing each spoke to form ADVPN shortcuts with the other spoke for each VRF.

However, in this scenario, we want A-1 and A-2 to use an ADVPN shortcut, but we do not want B-1 and B-2 to use ADVPN. A route map is configured on the hub to match the desired extended community route target number where only this route target is permitted, and others are denied. This allows the hub’s BGP route reflector to only reflect routes associated with VRF1, allowing the spokes to form an ADVPN shortcut for VRF1. Routes associated with VRF2 are not reflected, and each spoke must route traffic through the hub to reach VRF2 on the other spoke.



Configure the topology by following the instructions of Example 1 in *SD-WAN segmentation over a single overlay*. Note that when checking the spoke 1 routes in example 1, there is a VRF2 route:

```
Spoke 1 # get router info routing-table bgp
…
Routing table for VRF=2
B V     33.1.1.0/24 [200/0] via 10.10.100.3 [2] (recursive via vd2-1 tunnel 11.1.1.11),
00:00:20, [1/0]
                    [200/0] via 10.10.200.3 [2] (recursive via vd2-2 tunnel 11.1.2.11),
00:00:20, [1/0]
```

The following procedure applies a route map on the hub’s BGP configurations to limit route reflection to only routes matching the external community target of 1:1. This external community target corresponds to BGP paths for VRF1 learned from spoke 1 and spoke 2. The external community target of 2:1 corresponds to BGP paths for VRF2. By not explicitly permitting this target (2:1) in the community list and denying everything other than the permitted target (1:1) in the route map, the VRF2 BGP paths are essentially omitted from being reflected to the spokes.

To configure BGP filtering for an extended community route target on the hub:

1. Identify the external community target of VRF1 to be permitted:

```
# get router info bgp network 33.1.1.0/24
VRF 0 BGP routing table entry for 33.1.1.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   11.1.1.1
  Advertised to peer-groups:
  gr1 gr2
…
VRF 1 BGP routing table entry for 33.1.1.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0 external duplicated
  Local, (Received from a RR-client)
    0.0.0.0 from 10.10.100.3 (3.3.3.3)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      Receive Path ID: 1
      Advertised Path ID: 1
       Last update: Wed Aug 17 10:31:02 2022
  Original VRF 0 external duplicated
  Local, (Received from a RR-client)
    0.0.0.0 from 10.10.200.3 (3.3.3.3)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      Receive Path ID: 1
      Advertised Path ID: 2
       Last update: Wed Aug 17 10:31:02 2022
VRF 2 BGP routing table entry for 33.1.1.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0 external duplicated
  Local, (Received from a RR-client)
    0.0.0.0 from 10.10.100.3 (3.3.3.3)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Extended Community: RT:2:1
      Receive Path ID: 1
      Advertised Path ID: 1
       Last update: Wed Aug 17 10:31:02 2022
  Original VRF 0 external duplicated
  Local, (Received from a RR-client)
    0.0.0.0 from 10.10.200.3 (3.3.3.3)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Extended Community: RT:2:1
      Receive Path ID: 1
      Advertised Path ID: 2
       Last update: Wed Aug 17 10:31:02 2022
```

2. Configure the extended community list:

```
config router extcommunity-list
    edit "extcomm1"
        config rule
            edit 1
```

```
                set action permit
                set match "1:1"
                set type rt
            next
        end
    next
end
```

3. Apply the extended community list to the route map:

```
config router route-map
    edit "rmp11"
        config rule
            edit 1
                set match-extcommunity "extcomm1"
            next
            edit 2
                set action deny
            next
        end
    next
end
```

4. Update the related BGP neighbor group settings:

```
config router bgp
    config neighbor-group
        edit "gr1"
            set route-map-out-vpnv4 "rmp11"
        next
        edit "gr2"
            set route-map-out-vpnv4 "rmp11"
        next
    end
end
```

5. Refresh the routes:

```
# execute router clear bgp all vpnv4 unicast out
```

6. Check the spoke 1 routes. Since the extended community route target is applied, the VFR2 route does not appear in the BGP routing table:

```
# get router info routing-table bgp
Routing table for VRF=0
B*      0.0.0.0/0 [200/0] via 10.10.100.254 (recursive via vd2-1 tunnel 11.1.1.11),
03:47:50, [1/0]
                  [200/0] via 10.10.200.254 (recursive via vd2-2 tunnel 11.1.2.11),
03:47:50, [1/0]
B       1.1.1.1/32 [200/0] via 11.1.1.1 [2] (recursive via 12.1.1.1, vd2-vlan12),
03:47:50, [1/0]
B       1.222.222.222/32 [200/0] via 11.1.1.1 [2] (recursive via 12.1.1.1, vd2-vlan12),
03:47:50, [1/0]
B       11.11.11.11/32 [200/0] via 10.10.100.254 (recursive via vd2-1 tunnel 11.1.1.11),
03:47:50, [1/0]
                       [200/0] via 10.10.200.254 (recursive via vd2-2 tunnel 11.1.2.11),
03:47:50, [1/0]
B       33.1.1.0/24 [200/0] via 10.10.100.254 [2] (recursive via vd2-1 tunnel
11.1.1.11), 03:47:21, [1/0]
                    [200/0] via 10.10.200.254 [2] (recursive via vd2-2 tunnel
11.1.2.11), 03:47:21, [1/0]

Routing table for VRF=1
B V     11.11.22.11/32 [200/0] via 10.10.100.254 (recursive via vd2-1 tunnel 11.1.1.11),
03:47:50, [1/0]
                       [200/0] via 10.10.200.254 (recursive via vd2-2 tunnel 11.1.2.11),
03:47:50, [1/0]
B V     33.1.1.0/24 [200/0] via 10.10.100.3 [2] (recursive via vd2-1 tunnel 11.1.1.11),
03:47:21, [1/0]
                    [200/0] via 10.10.200.3 [2] (recursive via vd2-2 tunnel 11.1.2.11),
03:47:21, [1/0]
B V     100.1.1.0/24 [200/0] via 10.10.100.254 (recursive via vd2-1 tunnel 11.1.1.11),
03:47:50, [1/0]
                     [200/0] via 10.10.200.254 (recursive via vd2-2 tunnel 11.1.2.11),
03:47:50, [1/0]
```

SD-WAN application monitor using FortiMonitor - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- SD-WAN application monitor using FortiMonitor

The agent-based health check detection mode works with FortiMonitor to provide more accurate user level performance statistics. FortiMonitor acts as an agent and sends health check probes on behalf of the monitored FortiGate interface. FortiMonitor mimics a real user, and the probes return a more accurate application level performance. The SLA information collected from FortiMonitor is sent back to the FortiGate as the monitored interface's SLA information. These statistics can be used to gain a deeper insight into the SD-WAN traffic performance.

```
config system sdwan
    config health-check
        edit <name>
            set detect-mode agent-based
        next
    end
    config service
        edit <id>
            set agent-exclusive {enable | disable}
        next
    end
end
```

The following diagnostic commands can be used to view agent related metrics:

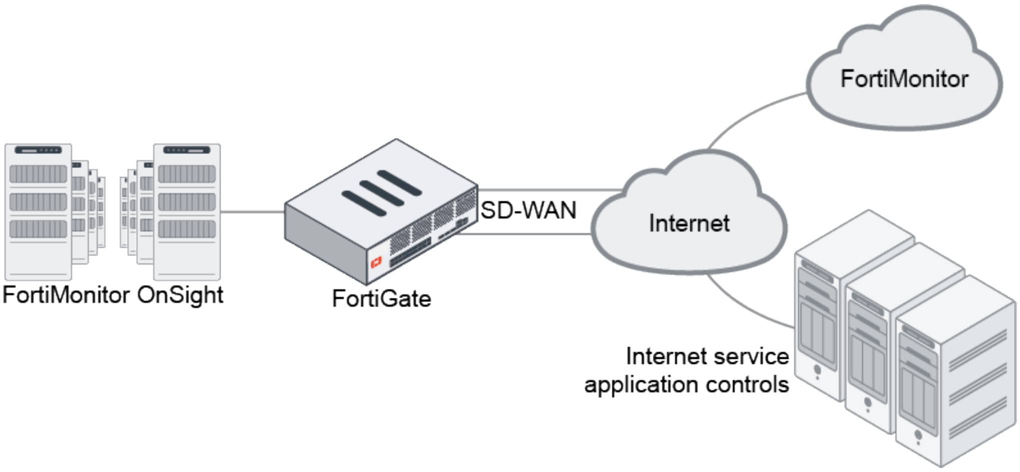
```
# diagnose sys link-monitor-passive agent <option>
```

list	List all the collected reports.
list-app	List the details of each application.
flush	Flush all the collected reports.

flush-app	Flush the details of all the applications.
agent-oif-map	List the agent and interface maps.

Example

In this example, routing is achieved through SD-WAN rules. The agent-based health check detection mode creates the FortiMonitor IP address and FortiGate SD-WAN interface map.



This example assumes that the FortiMonitor has already been added to the Security Fabric (see Configuring FortiMonitor in the FortiOS Administration Guide for detailed instructions). The FortiMonitor OnSight (client) can be configured for two or more IP addresses, and each IP address is capable of sending application probes to user-specified applications.

Specific routing is implemented on the FortiGate to ensure each FortiMonitor client collects performance statistics for only one SD-WAN member interface. The FortiMonitor is configured to send application-specific probes to measure that application's performance on a given SD-WAN member. The FortiGate uses the FortiMonitor performance statistics to determine link quality based on application performance by mapping the health check. The link quality for a given application can then be used to steer the matching application traffic with greater accuracy.

To configure the FortiGate:

1. Configure the address objects for each FortiMonitor client:

```
config firewall address
    edit "FMR_OnSight1"
        set subnet 10.2.1.80 255.255.255.255
    next
    edit "MR_OnSight2"
        set subnet 10.2.1.81 255.255.255.255
    next
end
```

2. Configure the SD-WAN rules to ensure each OnSight client uses only one SD-WAN member, and map the FortiMonitor IP to an SD-WAN member (interface):

```
config system sdwan
    config service
```

```
        edit 1
            set dst "all"
            set src "FMR_OnSight1"
            set priority-members 1
            set agent-exclusive enable
        next
        edit 2
            set dst "all"
            set src "FMR_OnSight2"
            set priority-members 2
            set agent-exclusive enable
        next
    end
end
```

3. Configure the SD-WAN health check:

```
config health-check
    edit "FMR"
        set detect-mode agent-based
        set members 1 2
        config sla
            edit 1
            next
        end
    next
end
```

To verify the SD-WAN member performance:

1. Verify the health check diagnostics:

```
# diagnose sys sdwan health-check
Health Check(FMR):
Seq(1 v1236): state(alive), packet-loss(0.000%) latency(183.214), jitter(0.124), mos
(4.225), bandwidth-up(999992), bandwidth-dw(999976), bandwidth-bi(1999968) sla_map=0x0
Seq(2 v1237): state(alive), packet-loss(0.000%) latency(182.946), jitter(0.100), mos
(4.226), bandwidth-up(999998), bandwidth-dw(999993), bandwidth-bi(1999991) sla_map=0x0
```

2. Verify the collected reports:

```
# diagnose sys link-monitor-passive agent list
       v1236( 23) | src=10.2.1.80 | latency=183.2   20:27:24 | jitter=0.1     20:27:24 |
pktloss=0.0  % 20:27:24
       v1237( 24) | src=10.2.1.81 | latency=182.9   20:27:24 | jitter=0.1     20:27:24 |
pktloss=0.0  % 20:27:24
```

3. Verify the details of each application:

```
# diagnose sys link-monitor-passive agent list-app
app_id=0x00000000, app=fortinet.com, dev=v1236(23)
        latency=183.2, jitter=0.1, pktloss=0.0,ntt=99.2,srt=384.8,app_err=0.0, 20:28:25
app_id=0x00000000, app=fortinet.com, dev=v1237(24)
        latency=183.1, jitter=0.5, pktloss=0.0,ntt=104.4,srt=377.8,app_err=0.0, 20:28:25
```

4. Verify the agent and interface maps:

```
# diagnose sys link-monitor-passive agent agent-oif-map
oif=v1236(23), src=10.2.1.80
oif=v1237(24), src=10.2.1.81
```

Add Fabric Overlay Orchestrator for SD-WAN overlay configurations - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Fabric Overlay Orchestrator

The Fabric Overlay Orchestrator feature is an easy-to-use GUI wizard that simplifies the process of configuring a self-orchestrated SD-WAN overlay within a single Security Fabric. This feature is self-orchestrated since no additional tool or device, aside from the FortiGates themselves, is required to orchestrate this configuration. An SD-WAN overlay configuration consists of IPsec and BGP configuration settings.

Currently, the Fabric Overlay Orchestrator supports a single hub architecture and builds upon an existing Security Fabric configuration. This feature configures the root FortiGate as the SD-WAN overlay hub and the downstream first-level FortiGates as the spokes.

After configuring the Fabric Overlay, you can complete the SD-WAN deployment by configuring SD-WAN rules.

If you cannot view the *VPN > Fabric Overlay Orchestrator* tree menu, configure the FortiGate as a root or a downstream device in the Security Fabric. See Configuring the root FortiGate and downstream FortiGates in the FortiOS Administration Guide for more details.

The Fabric Overlay Orchestrator does not work when VDOM mode is enabled.

Prerequisites

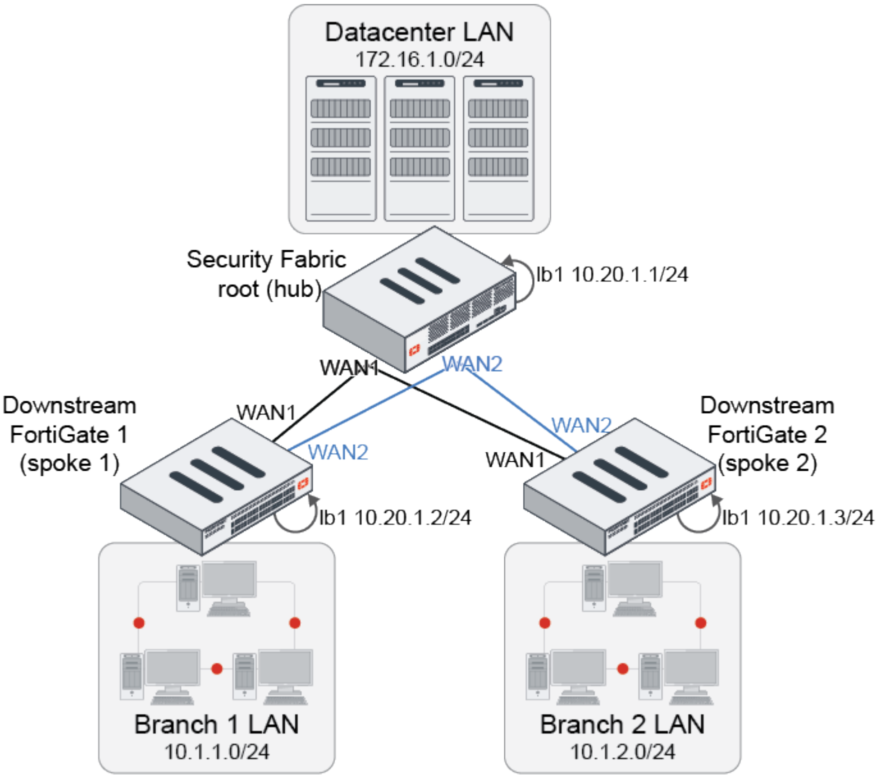
Create a single Fortinet Security Fabric with the following components:

- A root FortiGate and one or more downstream FortiGates all running FortiOS 7.2.4 or later
- A FortiAnalyzer, or cloud logging using FortiAnalyzer Cloud or FortiGate Cloud
  - For FortiGate Cloud, all downstream devices must belong to the same FortiCloud account

  For more information about configuring these components, see Configuring the root FortiGate and downstream FortiGates, Configuring FortiAnalyzer, and Configuring cloud logging in the FortiOS Administration Guide.

Network topology

The Fabric Overlay Orchestrator supports configuring an overlay for the following hub and spoke topology using ADVPN and a single hub.



This topology corresponds to the single datacenter (active-passive gateway) design using the IPsec overlay design of one-to-one overlay mapping per underlay. For more details on these topics, see the SD-WAN Architectures for Enterprise guide.

In this topology, the datacenter FortiGate (Security Fabric root FortiGate) is the hub, and the branch FortiGates (Security Fabric downstream FortiGates) are the spokes. Each FortiGate has a distinctly defined LAN subnet and loopback interface (lb1) with an IP address within the 10.20.1.0/24 subnet.

The Fabric Overlay Orchestrator creates loopbacks to act as health check servers that are always up, and they can be accessed by adjacent Fabric devices. When configuring the policy creation option of either automatic or health check on the hub, the Fabric Overlay Orchestrator configures performance SLAs from the hub to the health check servers on 10.20.1.2 and 10.20.1.3 corresponding to the spoke 1 and spoke 2 FortiGates respectively. Likewise, when the Fabric Overlay Orchestrator runs on each spoke, it creates a performance SLA to the hub using its loopback address of 10.20.1.1.

Instead of using loopbacks, any business-critical applications and resources connected to the LAN of each device can be used as health check servers for performance SLAs.

Using the Fabric Overlay Orchestrator

The following steps should be used to configure a self-orchestrated SD-WAN overlay within a single Security Fabric. These steps must be followed in order, and assume that the prerequisites and network topology are in place.

1. Configure the root FortiGate using the Fabric Overlay Orchestrator.
2. Configure one or more downstream FortiGates using the Fabric Overlay Orchestrator.
3. Configure an overlay on the spoke for an additional incoming interface on the hub (if applicable).
4. Verify the firewall policies on the hub FortiGate.

5. Verify the Fabric Overlay created by the Fabric Overlay Orchestrator:
   1. Verify the IPsec VPN tunnels on the hub FortiGate.
   2. Verify BGP routing on the hub FortiGate.
   3. Verify the performance SLAs on the hub FortiGate.
   4. Verify the firewall policies on a spoke FortiGate.
   5. Verify the IPsec VPN tunnels on a spoke FortiGate.
   6. Verify BGP routing on a spoke FortiGate.
   7. Verify the performance SLAs on a spoke FortiGate.
   8. Verify the spoke-to-spoke ADVPN communication.
6. Configure SD-WAN rules on the hub FortiGate.
7. Configure SD-WAN rules on the spoke FortiGates.

When configuring the root and downstream FortiGates, the Fabric Overlay Orchestrator configures the following settings in the background:

- IPsec overlay configuration (hub and spoke ADVPN tunnels)
- BGP configuration
- Policy routing
- SD-WAN zones
- SD-WAN performance SLAs

The FortiGate’s role in the SD-WAN overlay is automatically determined by its role in the Security Fabric. The Fabric root will be the hub, and any first-level downstream devices from the Fabric root will be spokes.

After using the Fabric Overlay Orchestrator on all FortiGates and verifying the overlay settings, complete the SD-WAN deployment configuration using steps 3 (if applicable), and steps 6 and 7. See SD-WAN rules in the FortiOS Administration Guide for more information.

For a detailed example configuration, see Using the Fabric Overlay Orchestrator in the FortiOS Administration Guide.

Creating firewall policies

The Fabric Overlay Orchestrator can create firewall policies to allow all traffic through the SD-WAN overlay, or firewall policies to just allow health check traffic through it instead. When the Fabric Overlay Orchestrator is enabled on the root FortiGate, there are three *Policy creation* options:

- *Automatic*: automatically create policies for the loopback interface and tunnel overlays.
- *Health check*: automatically create a policy for the loopback interface so the SD-WAN health checks are functional.
- *Manual*: no policies are automatically created.

The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. For some cases, these policies do not provide the necessary granularity to restrict overlay traffic to specific subnets or hosts.

When the Fabric Overlay Orchestrator is configured on a device, changing the policy creation rule will create new policies based on the rule, but it will not delete existing policies. Deleting existing policies must be performed manually.

Improve client-side settings for SD-WAN network monitor - 7.2.6

This information is also available in the FortiOS 7.2 Administration Guide:

- Speed test examples

Improvements have been made to the client-side settings of the SD-WAN network bandwidth monitoring service to increase the flexibility of the speed tests, and to optimize the settings to produce more accurate measurements. The changes include:

- Support UDP speed tests.
- Support multiple TCP connections to the server instead of a single connection.
- Measure the latency to speed test servers and select the server with the smallest latency to perform the test.
- Support the auto mode speed test, which selects either UDP or TCP testing automatically based on the latency threshold.

For more information about this feature, see Improve client-side settings for SD-WAN network monitor.

General

This section includes information about general network related new features:

- Add NetFlow fields to identify class of service on page 162
- OSPF graceful restart on topology change on page 164
- OSPFv3 graceful restart for OSPF6 on page 168
- BFD for multihop path for BGP on page 172
- Configuring the FortiGate to act as an 802.1X supplicant on page 177
- Support 802.1X on virtual switch for certain NP6 platforms on page 179
- SNMP OIDs for port block allocations IP pool statistics on page 181
- Increase the number of VRFs per VDOM on page 184
- GUI support for advanced BGP options 7.2.1 on page 188
- Support BGP AS number input in asdot and asdot+ format 7.2.1 on page 191
- SNMP OIDs with details about authenticated users 7.2.1 on page 193
- Add new IPAM GUI page 7.2.1 on page 197
- Assign multiple IP pools and subnets using IPAM Rules 7.2.1 on page 200
- Add VCI pattern matching as a condition for IP or DHCP option assignment 7.2.1 on page 203
- Support cross-VRF local-in and local-out traffic for local services 7.2.1 on page 205
- FortiGate as FortiGate LAN extension 7.2.1 on page 207
- Allow VLAN sub-interfaces to be used in virtual wire pairs 7.2.4 on page 212
- Add static route tag and BGP neighbor password 7.2.4 on page 214

- DHCP enhancements 7.2.4 on page 217
- Improve DVLAN QinQ performance for NP7 platforms 7.2.5 on page 222

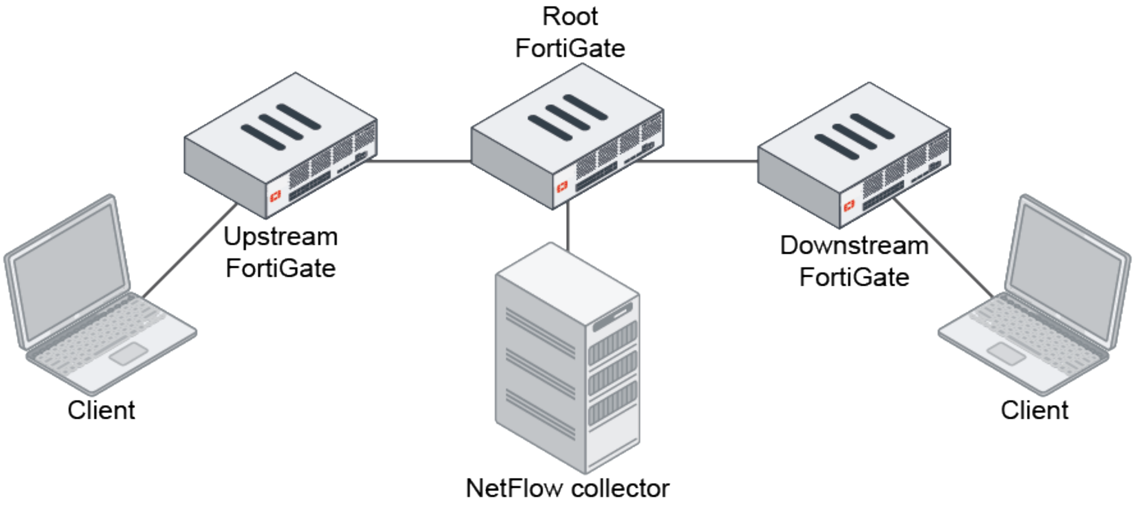
Add NetFlow fields to identify class of service

The new Netflow fields, ipClassOfService and postIpClassOfService, for identifying class of service in traffic flows are supported in FortiOS. The FortiGate reads the TOS(IPv4)/Traffic Class(IPv6) fields from the first packet of incoming traffic flow for the ipClassOfService value, and the first packet of outgoing traffic flow for postIpClassOfService value. These fields were added to NetFlow template ID 262.

Example

In this example, a device behind the downstream FortiGate sends traffic to a device behind the upstream FortiGate. In the direction of downstream FortiGate > root FortiGate > upstream FortiGate, the downstream FortiGate tags the traffic with DSCP 110000. The downstream FortiGate pads two 00s to the 6-bit binary to produce the TOS value of 11000000, which equals 0xc0 in hexadecimal. The flow in that direction will have an ipClassOfService/IP_TOS (TOS value of first inbound packet) of 0xc0, and a postIpClassOfService/DST_TOS (TOS value of first outbound) of the same 0xc0 value.

In the opposite direction, a device behind the upstream FortiGate sends traffic to device the downstream FortiGate. In the direction of upstream FortiGate > root FortiGate > downstream FortiGate, the upstream FortiGate tags the traffic with DSCP 111000. The upstream FortiGate pads two 00s to the 6-bit binary to produce the TOS value of 11100000, which equals 0xe0 in hexadecimal. The flow in that direction will have an ipClassOfService/IP_TOS (TOS value of first inbound packet) of 0xe0, and a postIpClassOfService/DST_TOS (TOS value of first outbound) of the same 0xe0 value.



Wireshark is used to analyze the packets. For more information about configuring NetFlow in FortiOS, refer to the Administration Guide.

Wireshark captures

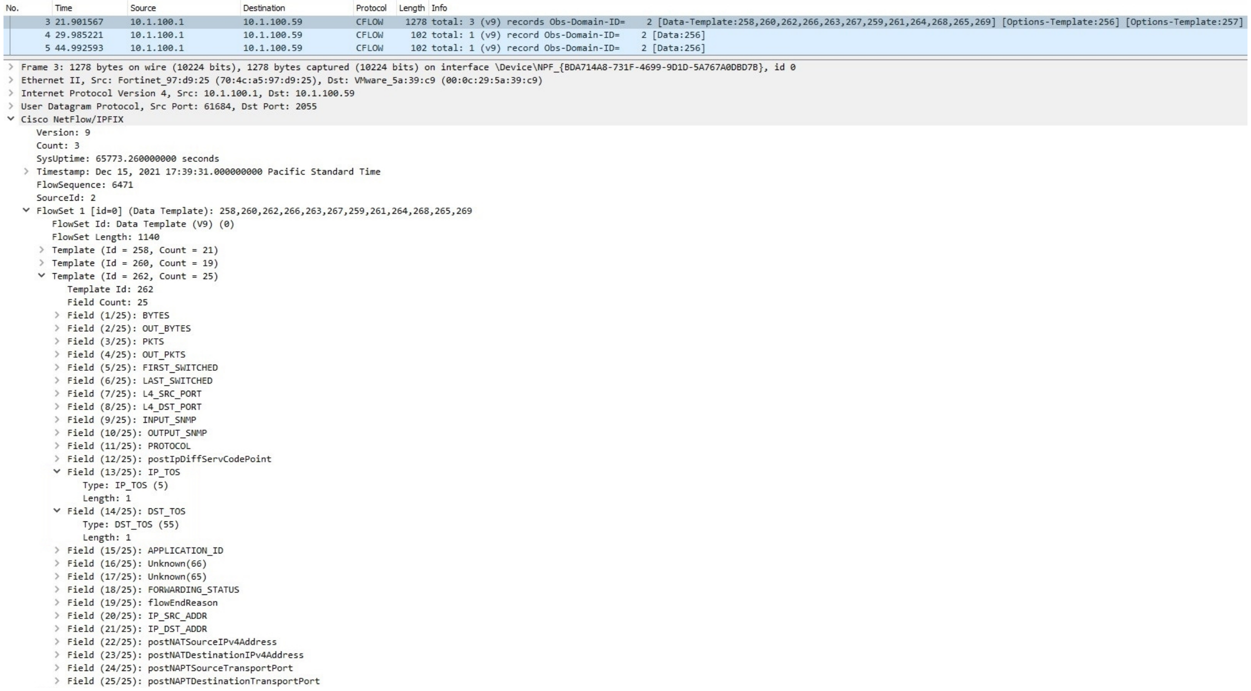
In the following capture of the NetFlow packet sent from the FortiGate to the NetFlow collector:

- The FortiGate sends NetFlow data template IDs 258 to 269, and option template IDs 256 and 257 to the NetFlow collector containing the fields in each template (see NetFlow templates for more information).

- Inside data template ID 262, two new fields are added, which correspond to field numbers 13 and 14 of the template.

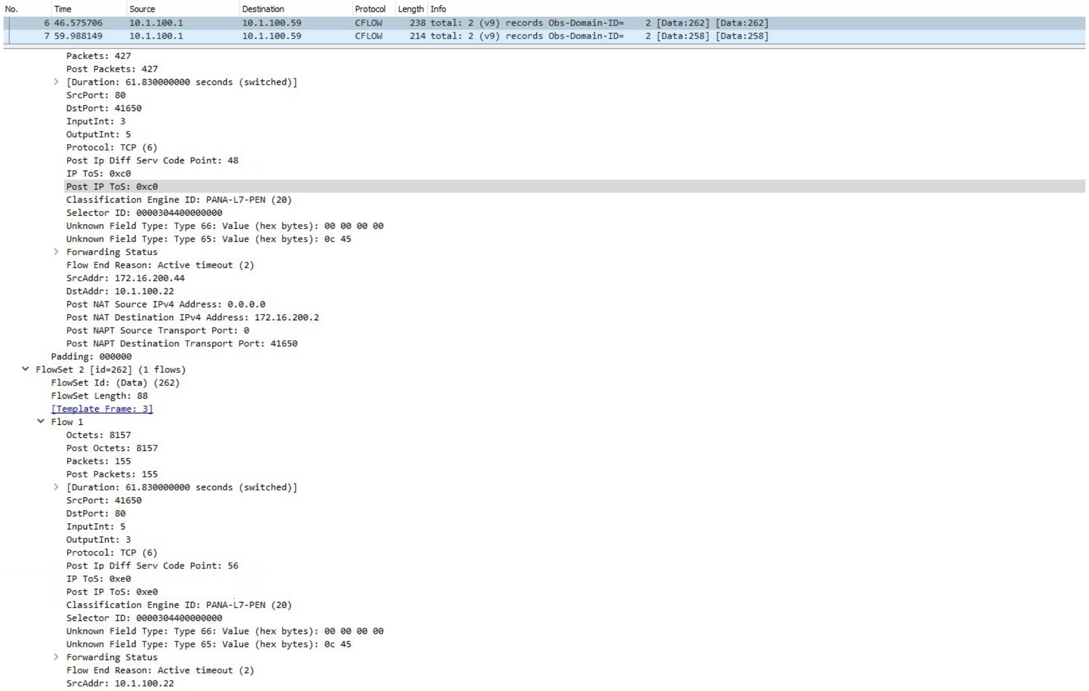
Field #	Type	Element ID
13	IP_TOS/ipClassOfService	5
14	DST_TOS/postIpClassOfService	55

Refer to IP Flow Information Export (IPFIX) Entities for more information.



```
No.   Time        Source        Destination    Protocol  Length Info
    3 21.901567   10.1.100.1    10.1.100.59    CFLOW      1278 total: 3 (v9) records Obs-Domain-ID=    2 [Data-Template:258,260,262,266,263,267,259,261,264,268,265,269] [Options-Template:256] [Options-Template:257]
    4 29.985221   10.1.100.1    10.1.100.59    CFLOW       102 total: 1 (v9) record Obs-Domain-ID=    2 [Data:256]
    5 44.992593   10.1.100.1    10.1.100.59    CFLOW       102 total: 1 (v9) record Obs-Domain-ID=    2 [Data:256]

> Frame 3: 1278 bytes on wire (10224 bits), 1278 bytes captured (10224 bits) on interface \Device\NPF_{BDA714A8-731F-4699-9D1D-5A767A0DBD7B}, id 0
> Ethernet II, Src: Fortinet_97:d9:25 (70:4c:a5:97:d9:25), Dst: VMware_5a:39:c9 (00:0c:29:5a:39:c9)
> Internet Protocol Version 4, Src: 10.1.100.1, Dst: 10.1.100.59
> User Datagram Protocol, Src Port: 61684, Dst Port: 2055
v Cisco NetFlow/IPFIX
    Version: 9
    Count: 3
    SysUptime: 65773.260000000 seconds
  > Timestamp: Dec 15, 2021 17:39:31.000000000 Pacific Standard Time
    FlowSequence: 6471
    SourceId: 2
  v FlowSet 1 [id=0] (Data Template): 258,260,262,266,263,267,259,261,264,268,265,269
      FlowSet Id: Data Template (V9) (0)
      FlowSet Length: 1140
    > Template (Id = 258, Count = 21)
    > Template (Id = 260, Count = 19)
    v Template (Id = 262, Count = 25)
        Template Id: 262
        Field Count: 25
      > Field (1/25): BYTES
      > Field (2/25): OUT_BYTES
      > Field (3/25): PKTS
      > Field (4/25): OUT_PKTS
      > Field (5/25): FIRST_SWITCHED
      > Field (6/25): LAST_SWITCHED
      > Field (7/25): L4_SRC_PORT
      > Field (8/25): L4_DST_PORT
      > Field (9/25): INPUT_SNMP
      > Field (10/25): OUTPUT_SNMP
      > Field (11/25): PROTOCOL
      > Field (12/25): postIpDiffServCodePoint
      v Field (13/25): IP_TOS
          Type: IP_TOS (5)
          Length: 1
      v Field (14/25): DST_TOS
          Type: DST_TOS (55)
          Length: 1
      > Field (15/25): APPLICATION_ID
      > Field (16/25): Unknown(66)
      > Field (17/25): Unknown(65)
      > Field (18/25): FORWARDING_STATUS
      > Field (19/25): flowEndReason
      > Field (20/25): IP_SRC_ADDR
      > Field (21/25): IP_DST_ADDR
      > Field (22/25): postNATSourceIPv4Address
      > Field (23/25): postNATDestinationIPv4Address
      > Field (24/25): postNAPTSourceTransportPort
      > Field (25/25): postNAPTDestinationTransportPort
```

The following capture shows two flow sets corresponding to each traffic direction. Each flow set has the TOS value corresponding to the DSCP tag applied in that direction: 0xc0 for downstream FortiGate > root FortiGate > upstream FortiGate, and 0xe0 for upstream FortiGate > root FortiGate > downstream FortiGate.



```
No.     Time        Source        Destination    Protocol  Length Info
      6 46.575706   10.1.100.1    10.1.100.59    CFLOW        238 total: 2 (v9) records Obs-Domain-ID=    2 [Data:262] [Data:262]
      7 59.988149   10.1.100.1    10.1.100.59    CFLOW        214 total: 2 (v9) records Obs-Domain-ID=    2 [Data:258] [Data:258]
            Packets: 427
            Post Packets: 427
          > [Duration: 61.830000000 seconds (switched)]
            SrcPort: 80
            DstPort: 41650
            InputInt: 3
            OutputInt: 5
            Protocol: TCP (6)
            Post Ip Diff Serv Code Point: 48
            IP ToS: 0xc0
            Post IP ToS: 0xc0
            Classification Engine ID: PANA-L7-PEN (20)
            Selector ID: 0000304400000000
            Unknown Field Type: Type 66: Value (hex bytes): 00 00 00 00
            Unknown Field Type: Type 65: Value (hex bytes): 0c 45
          > Forwarding Status
            Flow End Reason: Active timeout (2)
            SrcAddr: 172.16.200.44
            DstAddr: 10.1.100.22
            Post NAT Source IPv4 Address: 0.0.0.0
            Post NAT Destination IPv4 Address: 172.16.200.2
            Post NAPT Source Transport Port: 0
            Post NAPT Destination Transport Port: 41650
         Padding: 000000
   v FlowSet 2 [id=262] (1 flows)
         FlowSet Id: (Data) (262)
         FlowSet Length: 88
         [Template Frame: 3]
       v Flow 1
            Octets: 8157
            Post Octets: 8157
            Packets: 155
            Post Packets: 155
          > [Duration: 61.830000000 seconds (switched)]
            SrcPort: 41650
            DstPort: 80
            InputInt: 5
            OutputInt: 3
            Protocol: TCP (6)
            Post Ip Diff Serv Code Point: 56
            IP ToS: 0xe0
            Post IP ToS: 0xe0
            Classification Engine ID: PANA-L7-PEN (20)
            Selector ID: 0000304400000000
            Unknown Field Type: Type 66: Value (hex bytes): 00 00 00 00
            Unknown Field Type: Type 65: Value (hex bytes): 0c 45
          > Forwarding Status
            Flow End Reason: Active timeout (2)
            SrcAddr: 10.1.100.22
```

OSPF graceful restart on topology change

In OSPF graceful restart mode, the `restart-on-topology-change` option can be used to keep restarting the router in graceful restart mode when a topology change is detected during a restart.

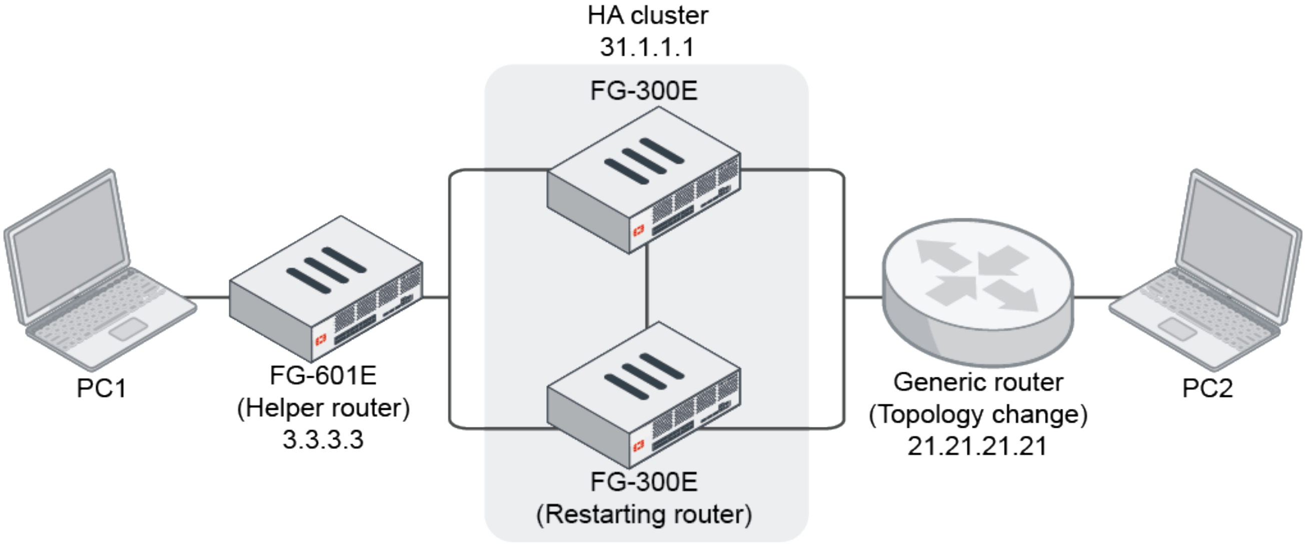
```
config router ospf
    set restart-on-topology-change {enable | disable}
end
```

Example

In this example, a restarting router (one of the FG-300Es in the HA cluster) informs its neighbors using grace LSAs before restarting its OSPF process. When the helper router (the FG-601E) receives the grace LSAs, it enters helper mode to help with the graceful restart until the graceful period expires. It will act as though there are no changes on the restarting router (FG-300E). A generic router simulates a topology change during the restart event.

If `restart-on-topology-change` is enabled on the restarting router, it will not exit the graceful restart mode even when a topology change is detected.

If `restart-on-topology-change` is disabled on the restarting router, it will exit graceful restart mode when a topology change is detected.



To configure the restarting router:

```
config router ospf
    set router-id 31.1.1.1
    set restart-mode graceful-restart
    set restart-period 180
    set restart-on-topology-change enable
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 172.16.200.0 255.255.255.0
        next
        edit 2
            set prefix 31.1.1.1 255.255.255.255
        next
    end
end
```

To configure the restarting helper router:

```
config router ospf
    set router-id 3.3.3.3
    set restart-mode graceful-restart
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 172.16.200.0 255.255.255.0
        next
        edit 2
            set prefix 3.3.3.3 255.255.255.255
        next
    end
end
```

Testing the configuration

Topology change with continuing graceful restart enabled:

When `restart-on-topology-change` is enabled and there is a topology change during the HA OSPF graceful restart, the graceful restart will continue. The routes on the helper router (FG-601E) are still there and no traffic will drop.

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:14:47*   172.16.200.31   port1

# get router info routing-table ospf
Routing table for VRF=0
O       21.21.21.21/32 [110/300] via 172.16.200.31, port1, 00:09:55
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:55:31
O       100.21.1.0/24 [110/200] via 172.16.200.31, port1, 00:12:31

# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:14:47*   172.16.200.31   port1

# get router info routing-table ospf
Routing table for VRF=0
O       21.21.21.21/32 [110/300] via 172.16.200.31, port1, 00:10:07
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:55:43
O       100.21.1.0/24 [110/200] via 172.16.200.31, port1, 00:12:43

# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:14:38*   172.16.200.31   port1

# get router info routing-table ospf
Routing table for VRF=0
O       21.21.21.21/32 [110/300] via 172.16.200.31, port1, 00:10:17
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:55:53
O       100.21.1.0/24 [110/200] via 172.16.200.31, port1, 00:12:53

# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:00:38    172.16.200.31   port1

# get router info routing-table ospf
Routing table for VRF=0
O       21.21.21.21/32 [110/300] via 172.16.200.31, port1, 00:10:37
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:56:13
O       100.21.1.0/24 [110/200] via 172.16.200.31, port1, 00:13:13
```

Topology change with continuing graceful restart disabled:

When `restart-on-topology-change` is disabled and there is a topology change during the HA OSPF graceful restart, the graceful restart will exit. The routes on the helper router (FG-601E) are lost and traffic will drop.

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:14:57*   172.16.200.31   port1
```

```
# get router info routing-table ospf
Routing table for VRF=0
O       21.21.21.21/32 [110/300] via 172.16.200.31, port1, 00:11:16
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:56:52
O       100.21.1.0/24 [110/200] via 172.16.200.31, port1, 00:13:52
```

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:14:42*   172.16.200.31   port1
```

```
# get router info routing-table ospf
Routing table for VRF=0
O       21.21.21.21/32 [110/300] via 172.16.200.31, port1, 00:11:31
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:57:07
O       100.21.1.0/24 [110/200] via 172.16.200.31, port1, 00:14:07
```

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:14:40*   172.16.200.31   port1
```

No routes are lost:

```
# get router info routing-table ospf
Routing table for VRF=0
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:57:09
```

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
31.1.1.1          1   Full/DR         00:14:38*   172.16.200.31   port1
```

No routes are lost:

```
# get router info routing-table ospf
Routing table for VRF=0
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 00:57:11
```

No routes are lost:

```
# get router info routing-table ospf
Routing table for VRF=0
O       21.21.21.21/32 [110/300] via 172.16.200.31, port1, 00:04:42
O       31.1.1.1/32 [110/200] via 172.16.200.31, port1, 01:01:59
O       100.21.1.0/24 [110/200] via 172.16.200.31, port1, 00:04:42
```

OSPFv3 graceful restart for OSPF6

OSPFv3 graceful restart can be used in OSPF6. In OSPF graceful restart mode, the `restart-on-topology-change` option can be used to keep restarting the router in graceful restart mode when a topology change is detected during a restart.

```
config router ospf6
    set restart-mode {none | graceful-restart}
    set restart-period <integer>
    set restart-on-topology-change {enable | disable}
end
```

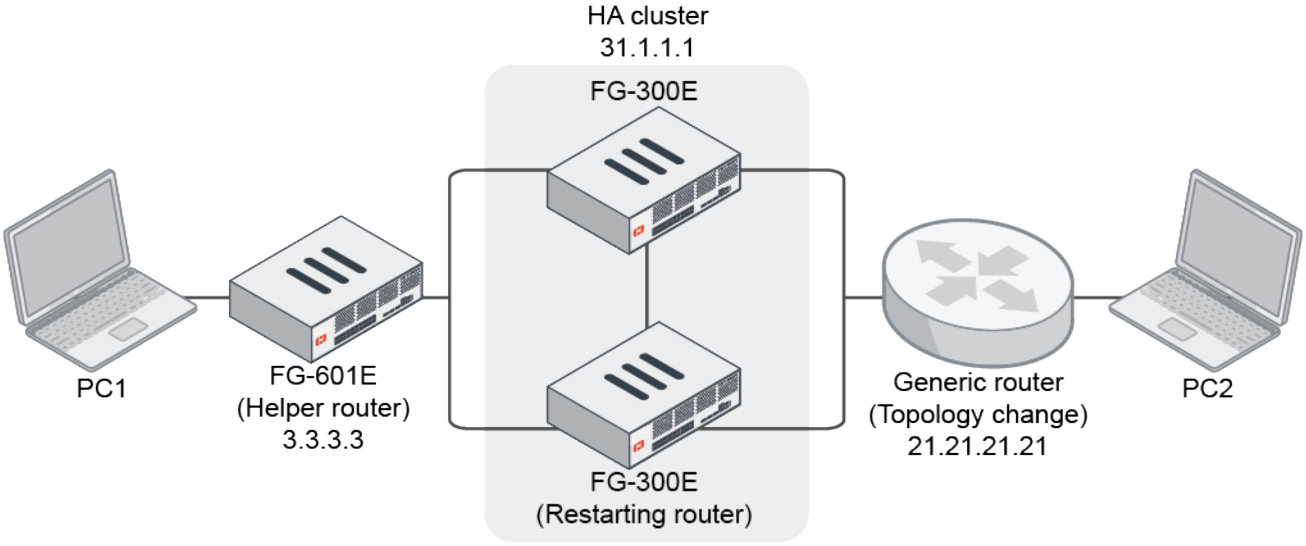
`restart-mode {none | graceful-restart}`	Set the OSPFv3 restart mode: • none: disable hitless restart • graceful-restart: enable graceful restart mode
`restart-period <integer>`	Set the graceful restart period, in seconds (1 - 3600, default = 120).
`restart-on-topology-change {enable | disable}`	Enable/disable continuing graceful restart upon a topology change.

Example

Graceful restarts allow a router's OSPF6 process to restart without interrupting its neighbors. In this example, a restarting router (one of the FG-300Es in the HA cluster) informs its neighbors using grace LSAs before restarting its OSPF process. When the helper router (the FG-601E) receives the grace LSAs, it enters helper mode to help with the graceful restart until the graceful period expires. It will act as though there are no changes on the restarting router (FG-300E). A generic router simulates a topology change during the restart event.

If `restart-on-topology-change` is enabled on the restarting router, it will not exit the graceful restart mode even when a topology change is detected.

If `restart-on-topology-change` is disabled on the restarting router, it will exit graceful restart mode when a topology change is detected.



To configure the restarting router:

```
config router ospf6
    set router-id 31.1.1.1
    set restart-mode graceful-restart
    set restart-period 600
    set restart-on-topology-change enable
    config area
        edit 0.0.0.0
        next
    end
    config ospf6-interface
        edit "port1"
            set interface "port1"
        next
        edit "looproot"
            set interface "looproot"
        next
        edit "npu"
            set interface "npu0_vlink0"
        next
    end
end
```

To configure the restarting helper router:

```
config router ospf6
    set auto-cost-ref-bandwidth 100000
    set router-id 3.3.3.3
    set restart-mode graceful-restart
    config area
        edit 0.0.0.0
        next
    end
    config ospf6-interface
        edit "port1"
            set interface "port1"
            set priority 0
        next
        edit "loopback1"
            set interface "loopback1"
        next
    end
    config redistribute "static"
        set status enable
    end
end
```

Testing the configuration

Graceful restart mode and continuing graceful restart enabled:

When graceful restart is enabled and `restart-on-topology-change` enabled, when HA encounters a failover or restarts the primary FortiGate, it will trigger a graceful restart. During this period, there is a topology change.

Before graceful restart:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:34    port1      0
```

All routes before graceful restart:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:08:01
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:26:03
O       2003:100:21:1::/64 [110/200] via fe80::209:fff:fe09:2, port1, 00:08:01
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:26:03
```

During graceful restart:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:35*   port1      0
```

All routes during graceful restart:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:09:01
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:27:03
O       2003:100:21:1::/64 [110/200] via fe80::209:fff:fe09:2, port1, 00:09:01
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:27:03
```

During graceful restart:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:33*   port1      0
```

All routes during graceful restart:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:09:07
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:27:09
O       2003:100:21:1::/64 [110/300] via fe80::209:fff:fe09:2, port1, 00:00:03
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:27:09
```

After graceful restart:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:39    port1      0
```

No routes lost after graceful restart:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:09:19
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:27:21
O       2003:100:21:1::/64 [110/300] via fe80::209:fff:fe09:2, port1, 00:00:09
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:27:21
```

Graceful restart mode enabled and continuing graceful restart disabled:

When graceful restart is enabled and `restart-on-topology-change` disabled, when HA encounters a failover or restarts the primary FortiGate, it will trigger a graceful restart. During this period, there is a topology change.

Before HA failover:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:37    port1      0
```

Before HA failover:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:00:32
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:01:31
O       2003:100:21:1::/64 [110/300] via fe80::209:fff:fe09:2, port1, 00:00:31
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:01:31
```

During graceful restart:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:33*   port1      0
```

At first, no routes are lost:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:02:17
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:03:16
O       2003:100:21:1::/64 [110/300] via fe80::209:fff:fe09:2, port1, 00:02:16
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:03:16
```

When the topology changes, routes are lost:

```
# get router info6 routing-table ospf
No route available
```

The routes are now recovered:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:02:28
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:00:01
O       2003:100:21:1::/64 [110/200] via fe80::209:fff:fe09:2, port1, 00:00:01
O       2003:172:16:200::/64 [110/110] via fe80::209:fff:fe09:2, port1, 00:00:01
```

Graceful restart mode disabled:

When graceful restart is not enabled, when HA encounters a failover or restarts the primary FortiGate, it will not trigger a graceful restart. The neighbor needs to re-establish and routes on the neighbor will be lost.

Before HA failover:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
```

```
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:37    port1      0
```

Before HA failover:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:00:50
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:01:00
O       2003:100:21:1::/64 [110/200] via fe80::209:fff:fe09:2, port1, 00:00:50
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:00:50
```

During HA failover:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Init/DROther    00:00:32    port1      0
```

During HA failover:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   ExStart/DR      00:00:38    port1      0
```

During HA failover, all are routes lost:

```
# get router info6 routing-table ospf
No route available
```

After HA failover:

```
# get router info6 ospf neighbor
OSPFv3 Process (root)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
31.1.1.1          1   Full/DR         00:00:34    port1      0
```

After HA failover, it gets a route update from the neighbor:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:00:07
O       2003:172:16:200::/64 [110/110] via ::, port1, 00:00:06
```

After HA failover, it gets a route update from more neighbors:

```
# get router info6 routing-table ospf
Routing table for VRF=0
O       2003:21:21:21::21/128 [110/200] via fe80::209:fff:fe09:2, port1, 00:00:23
O       2003:31:1:1::1/128 [110/100] via fe80::209:fff:fe09:2, port1, 00:00:33
O       2003:100:21:1::/64 [110/200] via fe80::209:fff:fe09:2, port1, 00:00:23
O       2003:172:16:200::/64 [110/100] via ::, port1, 00:00:23
```

BFD for multihop path for BGP

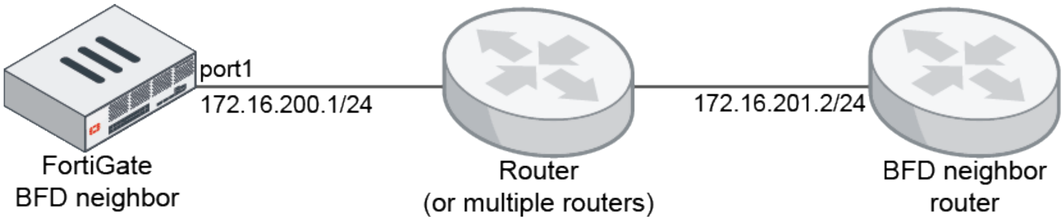
In BFD, a FortiGate can support neighbors connected over multiple hops. When BFD is down, BGP sessions are reset and will try to immediately re-establish neighbor connections. Previously, BFD was only supported when two routers or FortiGates were directly connected on the same network.

```
config router {bfd | bfd6}
    config multihop-template
        edit <ID>
            set src <class_IP/netmask>
            set dst <class_IP/netmask>
            set bfd-desired-min-tx <integer>
            set bfd-required-min-rx <integer>
            set bfd-detect-mult <integer>
            set auth-mode {none | md5}
            set md5-key <password>
        next
    end
end
```

`src <class_IP/netmask>`	Enter the source prefix.
`dst <class_IP/netmask>`	Enter the destination prefix.
`bfd-desired-min-tx <integer>`	Set the BFD desired minimal transmit interval, in milliseconds (100 - 30000, default = 250).
`bfd-required-min-rx <integer>`	Set the BFD required minimal transmit interval, in milliseconds (100 - 30000, default = 250).
`bfd-detect-mult <integer>`	Set the BFD detection multiplier (3 - 50, default = 3).
`auth-mode {none | md5}`	Set the authentication mode (none or meticulous MD5).
`md5-key <password>`	Enter the password.

Example

This example includes IPv4 and IPv6 BFD neighbor configurations. The BFD neighbor is also a BGP neighbor that is in a different AS.



To configure BFD with multihop BGP paths:

1. Enable BFD on all interfaces:

```
config system settings
    set bfd enable
end
```

2. Enable BFD on port1 and ignore the global configuration:

```
config system interface
    edit "port1"
        set bfd enable
    next
end
```

3. Configure the BGP neighbors:

```
config router bgp
    set as 65412
    set router-id 1.1.1.1
    config neighbor
        edit "172.16.201.2"
            set bfd enable
            set ebgp-enforce-multihop enable
            set soft-reconfiguration enable
            set remote-as 65050
        next
        edit "2000:172:16:201::2"
            set bfd enable
            set ebgp-enforce-multihop enable
            set soft-reconfiguration enable
            set remote-as 65050
        next
    end
end
```

4. Configure the IPv4 BFD:

```
config router bfd
    config multihop-template
        edit 1
            set src 172.16.200.0 255.255.255.0
            set dst 172.16.201.0 255.255.255.0
            set auth-mode md5
            set md5-key **********
        next
    end
end
```

5. Configure the IPv6 BFD:

```
config router bfd6
    config multihop-template
        edit 1
            set src 2000:172:16:200::/64
            set dst 2000:172:16:201::/64
        next
    end
end
```

Testing the connection

1. Verify the BFD status for IPv4 and IPv6:

```
# get router info bfd requests
BFD Peer Requests:
    client types(ct in 0x): 01=external 02=static
        04=ospf 08=bgp 10=pim-sm
src=172.16.200.1     dst=172.16.201.2     ct=08 ifi=9 type=SM
```

```
# get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
172.16.200.1    172.16.201.2    UP          port1           5/3/M
```

```
# get router info6 bfd requests
BFD Peer Requests:
    client types(ct in 0x): 01=external 02=static
        04=ospf 08=bgp 10=pim-sm
src=2000:172:16:200::1
dst=2000:172:16:201::2
ct=08 ifi=9 type=SM
```

```
# get router info6 bfd neighbor
OurAddress: 2000:172:16:200::1
NeighAddress: 2000:172:16:201::2
State: UP Interface: port1 Desc: 6/4 Multi-hop
```

2. Verify the BGP status and the BGP routing table:

```
# get router info bgp summary
VRF 0 BGP router identifier 1.1.1.1, local AS number 65412
BGP table version is 11
3 BGP AS-PATH entries
0 BGP community entries

Neighbor           V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.201.2       4      65050     185     187       10    0    0 00:54:20        4
2000:172:16:201::2 4      65050     159     160       10    0    0 00:54:24        4

Total number of neighbors 2
```

```
# get router info routing-table bgp
Routing table for VRF=0
B       172.28.1.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:54:32
B       172.28.2.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:54:32
B       172.28.5.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:54:32
B       172.28.6.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:54:32
```

```
# get router info6 bgp summary
VRF 0 BGP router identifier 1.1.1.1, local AS number 65412
BGP table version is 8
3 BGP AS-PATH entries
0 BGP community entries

Neighbor           V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.201.2       4      65050     185     187        7    0    0 00:54:24        3
2000:172:16:201::2 4      65050     159     160        7    0    0 00:54:28        3

Total number of neighbors 2
```

```
# get router info6 routing-table bgp
Routing table for VRF=0
B       2000:172:28:1::/64 [20/0] via 2000:172:16:201::2 (recursive via
2000:172:16:200::4, port1), 00:54:40
B       2000:172:28:2::/64 [20/0] via 2000:172:16:201::2 (recursive via
2000:172:16:200::4, port1), 00:54:40
B       2000:172:28:3::/64 [20/0] via 2000:172:16:201::2 (recursive via
2000:172:16:200::4, port1), 00:54:40
```

3. Simulate a disruption to the BFD connection. The BFD neighbor is lost:

```
# get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
```

```
# get router info6 bfd neighbor
```

4. The BGP neighbor is reset, and the FortiGate attempts to re-establish a connection with the neighbor. The timers are reset once the neighbor connection is re-established:

```
# get router info bgp summary
VRF 0 BGP router identifier 1.1.1.1, local AS number 65412
BGP table version is 12
4 BGP AS-PATH entries
0 BGP community entries

Neighbor           V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

172.16.201.2       4      65050     189     192       11    0    0 00:00:11        4
2000:172:16:201::2 4      65050     165     167       12    0    0 00:00:08        4

Total number of neighbors 2
```

```
# get router info6 bgp summary
VRF 0 BGP router identifier 1.1.1.1, local AS number 65412
BGP table version is 10
4 BGP AS-PATH entries
0 BGP community entries

Neighbor           V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.201.2       4      65050     189     192        8    0    0 00:00:15        3
2000:172:16:201::2 4      65050     165     167        9    0    0 00:00:12        3

Total number of neighbors 2
```

5. The BGP routes are learned again, and there are new timers in the route tables:

```
# get router info routing-table bgp
Routing table for VRF=0
B       172.28.1.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:00:15
B       172.28.2.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:00:15
B       172.28.5.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:00:15
B       172.28.6.0/24 [20/0] via 172.16.201.2 (recursive via 172.16.200.4, port1),
00:00:15
```

```
# get router info6 routing-table bgp
Routing table for VRF=0
B       2000:172:28:1::/64 [20/0] via 2000:172:16:201::2 (recursive via
2000:172:16:200::4, port1), 00:00:13
B       2000:172:28:2::/64 [20/0] via 2000:172:16:201::2 (recursive via
2000:172:16:200::4, port1), 00:00:13
```

```
B       2000:172:28:3::/64 [20/0] via 2000:172:16:201::2 (recursive via
2000:172:16:200::4, port1), 00:00:13
```

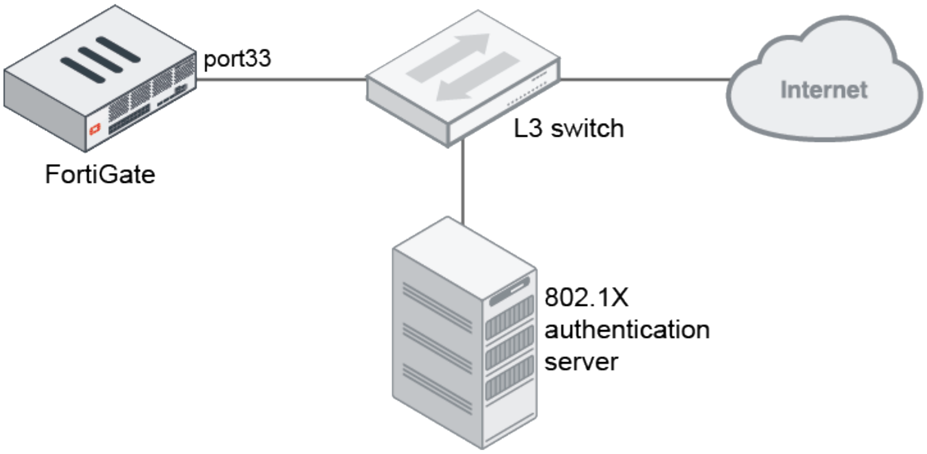
Configuring the FortiGate to act as an 802.1X supplicant

The FortiGate can be configured to act as a 802.1X supplicant. The settings can be enabled on the network interface in the CLI. The EAP authentication method can be either PEAP or TLS using a user certificate.

```
config system interface
    edit <interface>
        set eap-supplicant {enable | disable}
        set eap-method {peap | tls}
        set eap-identity <identity>
        set eap-password <password>
        set eap-ca-cert <CA_cert>
        set eap-user-cert <user_cert>
    next
end
```

Example

In this example, the FortiGate connects to an L3 switch that is not physically secured. All devices that connect to the internet must be authenticated with 802.1X by either a username and password (PEAP), or a user certificate (TLS). Configuration examples for both EAP authentication methods on port33 are shown.



To configure EAP authentication with PEAP:

1. Configure the interface:

```
config system interface
    edit "port33"
        set vdom "vdom1"
        set ip 7.7.7.2 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
fabric
        set stpforward enable
        set type physical
        set snmp-index 42
        set eap-supplicant enable
        set eap-method peap
        set eap-identity "test1"
        set eap-password **********
    next
end
```

2. Verify the interface's PEAP authentication details:

```
# diagnose test app eap_supp 2
Interface: port33
status:Authorized
method: PEAP
identity: test1
ca_cert:
client_cert:
private_key:
last_eapol_src =70:4c:a5:3b:0b:c6
```

Traffic is able to pass because the status is authorized.

To configure EAP authentication with TLS:

1. Configure the interface:

```
config system interface
    edit "port33"
        set vdom "vdom1"
        set ip 7.7.7.2 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
fabric
        set stpforward enable
        set type physical
        set snmp-index 42
        set eap-supplicant enable
        set eap-method tls
        set eap-identity "test2@fortiqa.net"
        set eap-ca-cert "root_G_CA_Cert_1.cer"
        set eap-user-cert "root_eap_client_global.cer"
    next
end
```

2. Verify the interface's TLS authentication details:

```
# diagnose test application eap_supp 2
Interface: port33
status:Authorized
method: TLS
identity: test2@fortiqa.net
ca_cert: /etc/cert/ca/root_G_CA_Cert_1.cer
client_cert: /etc/cert/local/root_eap_client_global.cer
private_key: /etc/cert/local/root_eap_client_global.key
last_eapol_src =70:4c:a5:3b:0b:c6
```

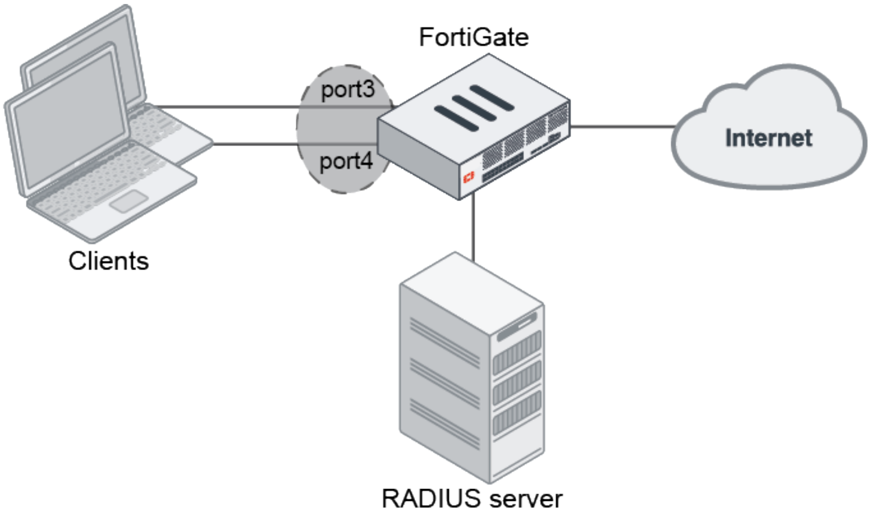
Traffic is able to pass because the status is authorized.

Support 802.1X on virtual switch for certain NP6 platforms

802.1X is supported under the hardware switch interface on the following NP6 platforms: FG-30xE, FG-40xE, and FG-110xE.

Example

In this example, port3 and port4 are part of a hardware switch interface. The hardware switch acts as a virtual switch so that devices can connect directly to these ports and perform 802.1X authentication on the port.



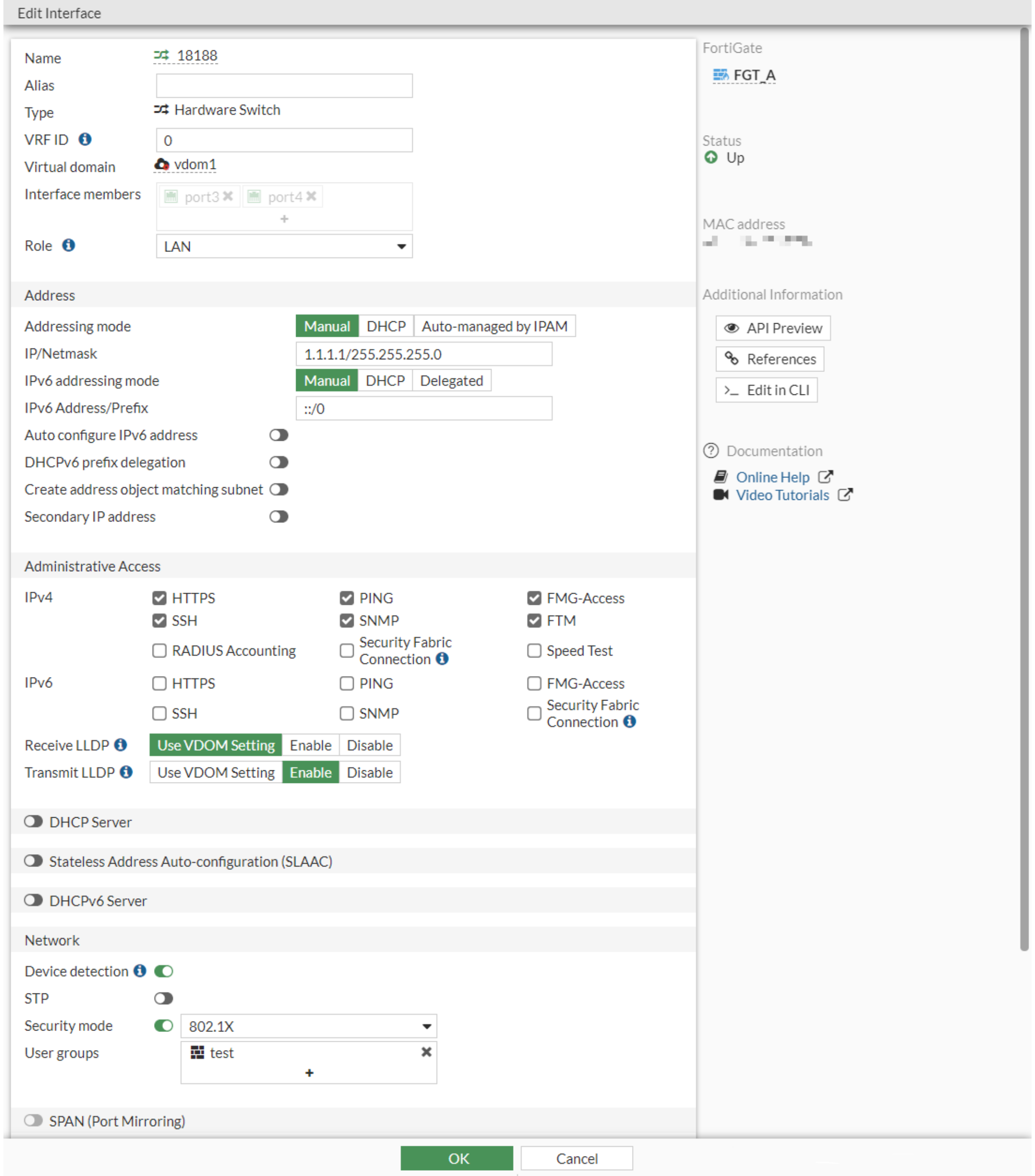
Prerequisites:

1. Configure a RADIUS server (see RADIUS servers).
2. Define a user group named test to use the remote RADIUS server and for 802.1X authentication (see User definition and groups).
3. Configure a hardware switch (named 18188) with port3 and port4 as the members (see Hardware switch).
4. Configure a firewall policy that allows traffic from the 18188 hardware switch to go to the internet.
5. Enable 802.1X authentication on the client devices.

To configure 802.1X authentication on a hardware switch in the GUI:

1. Go to *Network* > *Interfaces* and edit the hardware switch.
2. In the *Network* section, enable *Security mode* and select *802.1X*.

3. Click the + to add the *User group*.



Edit Interface

Name: 18188
Alias:
Type: Hardware Switch
VRF ID: 0
Virtual domain: vdom1
Interface members: port3, port4
Role: LAN

Address

Addressing mode: **Manual** | DHCP | Auto-managed by IPAM
IP/Netmask: 1.1.1.1/255.255.255.0
IPv6 addressing mode: **Manual** | DHCP | Delegated
IPv6 Address/Prefix: ::/0
Auto configure IPv6 address ○
DHCPv6 prefix delegation ○
Create address object matching subnet ○
Secondary IP address ○

Administrative Access

IPv4: ☑ HTTPS ☑ PING ☑ FMG-Access ☑ SSH ☑ SNMP ☑ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection ☐ Speed Test
IPv6: ☐ HTTPS ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ Security Fabric Connection
Receive LLDP: **Use VDOM Setting** | Enable | Disable
Transmit LLDP: Use VDOM Setting | **Enable** | Disable

○ DHCP Server
○ Stateless Address Auto-configuration (SLAAC)
○ DHCPv6 Server

Network

Device detection ●
STP ○
Security mode ● 802.1X
User groups: test

○ SPAN (Port Mirroring)

FortiGate: FGT_A
Status: Up
MAC address: [redacted]

Additional Information

4. Click *OK*.

To configure 802.1X authentication on a hardware switch in the CLI:

1. Configure the virtual hardware switch interfaces:

```
config system virtual-switch
    edit "18188"
        set physical-switch "sw0"
        config port
            edit "port3"
            next
            edit "port4"
            next
        end
    next
end
```

2. Configure 802.1X authentication:

```
config system interface
    edit "18188"
        set vdom "vdom1"
        set ip 1.1.1.1 255.255.255.0
        set allowaccess ping https ssh snmp fgfm ftm
        set type hard-switch
        set security-mode 802.1X
        set security-groups "test"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 52
    next
end
```

To verify the that the 802.1X authentication was successful:

1. Get a client connected to port3 to authenticate to access the internet.
2. In FortiOS, verify the 802.1X authentication port status:

```
# diagnose sys 802-1x status

Virtual switch '18188' (default mode) 802.1x member status:
  port3: Link up, 802.1X state: authorized
  port4: Link up, 802.1X state: unauthorized
```

SNMP OIDs for port block allocations IP pool statistics

The FortiGate SNMP MIB has been updated to support OIDs that provide data about any configured port block allocation (PBA) IP pools. There are four SNMP OIDs for polling critical PBAs statistics, including total PBAs, in use PBAs, expiring PBAs, and free PBAs:

Name	OID	Description
fgFwIppStatsTotalPBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.9	The total number of port block allocations.
fgFwIppStatsInusePBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.10	The number of port block allocations in use.
fgFwIppStatsExpiringPBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.11	The number of port block allocations that are expiring.
fgFwIppStatsFreePBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.12	The number of free port block allocations.

See Dynamic SNAT for more information on port block allocation IP pools.

Example 1

This example occurs when no IP pool is configured.

OID	Sample query

fgFwIppStatsTotalPBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.9`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.9 = No Such Instance currently exists at this OID`

fgFwIppStatsInusePBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.10`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.10 = No Such Instance currently exists at this OID`

fgFwIppStatsExpiringPBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.11`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.11 = No Such Instance currently exists at this OID`

fgFwIppStatsFreePBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.12`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.12 = No Such Instance currently exists at this OID`

Example 2

This example occurs when an IP pool is configured and not used in a firewall policy.

This example can also demonstrate when an IP pool is configured and used in a firewall policy but there is no traffic match.

OID	Sample query

fgFwIppStatsTotalPBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.9`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.9.13.13.13.1.13.13.13.13.2 = Gauge32: 6136`

fgFwIppStatsInusePBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.10`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.10.13.13.13.1.13.13.13.13.2 = Gauge32: 0`

fgFwIppStatsExpiringPBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.11`

OID	Sample query
	FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.11.13.13.13.1.13.13.13.13.2 = Gauge32: 0
fgFwIppStatsFreePBAs	snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.12 FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.12.13.13.13.1.13.13.13.13.2 = Gauge32: 100

Example 3

This example occurs when an IP pool is configured and used in a firewall policy with traffic matching.

OID	Sample query
fgFwIppStatsTotalPBAs	snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.9 FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.9.13.13.13.1.13.13.13.13.2 = Gauge32: 6136
fgFwIppStatsInusePBAs	snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.10 FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.10.13.13.13.1.13.13.13.13.2 = Gauge32: 1
fgFwIppStatsExpiringPBAs	snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.11 FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.11.13.13.13.1.13.13.13.13.2 = Gauge32: 0
fgFwIppStatsFreePBAs	snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.12 FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.12.13.13.13.1.13.13.13.13.2 = Gauge32: 99

Example 4

This example occurs when an IP pool is configured and used in a firewall policy but the traffic session is expired.

OID	Sample query

fgFwIppStatsTotalPBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.9`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.9.13.13.13.1.13.13.13.13.2 = Gauge32: 6136`

fgFwIppStatsInusePBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.10`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.10.13.13.13.1.13.13.13.13.2 = Gauge32: 0`

fgFwIppStatsExpiringPBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.11`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.11.13.13.13.1.13.13.13.13.2 = Gauge32: 1`

fgFwIppStatsFreePBAs	`snmpwalk -v2c -c FGT-B-SNMPv2 172.16.200.2 1.3.6.1.4.1.12356.101.5.3.2.1.1.12`
	`FORTINET-FORTIGATE-MIB::fgFwIppStatsEntry.12.13.13.13.1.13.13.13.13.2 = Gauge32: 100`

Increase the number of VRFs per VDOM

In FortiOS 7.2.0 to 7.2.3, the number of VRFs per VDOM has increased from 32 to 64 to support large SD-WAN, VPN, and BGP deployments. Up to 64 VRFs can be configured per VDOM on any device.

In FortiOS 7.2.4, the number of VRFs per VDOM has increased from 64 to 252. Up to 252 VRFs can be configured per VDOM on any device.

The VRF ID range has changed to in the following commands:

```
config system interface
    edit <name>
        set vrf <integer>
    next
end
```

```
config router {static | static6}
    edit <id>
        set vrf <integer>
    next
end
```

```
config router bgp
    config {vrf | vrf6}
        edit <integer>
        next
    end
end
```

The following diagnostic commands have been added:

```
# diagnose ip router bgp set-filter vrf <vrf_id>
```

```
# diagnose ip router bgp set-filter neighbor <neighbor_address>
```

```
# diagnose ip router bgp set-filter reset
```

```
# get router info filter show
```

```
# get router info filter vrf {vrf_id | all}
```

Example

In this example, 64 VRFs are configured on the root VDOM. The aggregate interface, agg1, is configured on the root VDOM with VRF ID 63. The diagnostic output displays the 64 configured VRFs and filtering on a specific VRF ID (63).

To configure the interface:

```
config system interface
    edit "agg1"
        set vdom "root"
        set vrf 63
        set ip 172.16.203.1 255.255.255.0
        set allowaccess ping
        set type aggregate
        set member "port11" "port12"
    next
end
```

To view the diagnostics:

1. Verify the routing table entries:

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 10.100.1.249, port4, [1/0]
O IA    2.2.2.2/32 [110/11000] via 172.16.200.2, port1, 00:09:45, [1/0]
O       3.3.3.3/32 [110/11000] via 172.16.200.4, port1, 06:59:16, [1/0]
O IA    4.4.4.4/32 [110/11100] via 172.16.200.2, port1, 00:09:51, [1/0]
O       10.100.1.0/24 [110/0] is a summary, Null, 06:59:35, [1/0]
C       10.100.1.0/30 is directly connected, port5
C       10.100.1.4/30 is directly connected, port7
C       10.100.1.248/29 is directly connected, port4
B       10.100.10.0/24 [20/300] via 10.100.1.1 (recursive is directly connected, port5),
06:59:30, [1/0]
```

```
B       10.100.11.0/24 [20/300] via 10.100.1.1 (recursive is directly connected, port5),
06:59:30, [1/0]
S       172.16.100.71/32 [10/0] via 172.16.200.254, port1, [1/0]
C       172.16.200.0/24 is directly connected, port1
C       172.16.200.200/32 is directly connected, port1
S       172.16.201.0/24 [150/0] via 172.16.200.4, port1, [1/0]
O IA    172.16.202.0/24 [110/1100] via 172.16.200.2, port1, 00:09:51, [1/0]
O IA    172.16.203.0/24 [110/1050] via 172.16.200.2, port1, 00:09:45, [1/0]
S       172.16.204.0/24 [10/0] via 172.16.200.4, port1, [1/0]
                        [10/0] via 172.16.206.2, vlan100, [101/0]
C       172.16.205.0/24 is directly connected, port2
C       172.16.206.0/24 is directly connected, vlan100
C       172.16.207.1/32 is directly connected, GRE_1
C       172.16.207.2/32 is directly connected, GRE_1
C       172.16.212.1/32 is directly connected, ipip_A_D
C       172.16.212.2/32 is directly connected, ipip_A_D
C       172.17.200.200/32 is directly connected, port1
S       172.27.1.0/24 [10/0] is a summary, Null, [1/0]
S       172.27.2.0/24 [10/0] is a summary, Null, [1/0]
S       172.27.5.0/24 [10/0] is a summary, Null, [1/0]
S       172.27.6.0/24 [10/0] is a summary, Null, [1/0]
S       172.27.7.0/24 [10/0] is a summary, Null, [1/0]
S       172.27.8.0/24 [10/0] is a summary, Null, [1/0]
S       172.29.1.0/24 [10/0] is a summary, Null, [1/0]
S       172.29.2.0/24 [10/0] is a summary, Null, [1/0]
O N2    172.31.4.0/22 [110/25] via 172.16.200.4, port1, 06:59:15, [1/0]
C       192.168.1.0/24 is directly connected, mgmt

Routing table for VRF=5
C       172.16.23.1/32 is directly connected, vlax5

Routing table for VRF=6
C       172.16.23.2/32 is directly connected, vlax6

...

Routing table for VRF=61
C       172.16.13.3/32 is directly connected, vlax61

Routing table for VRF=62
C       172.16.13.4/32 is directly connected, vlax62

Routing table for VRF=63
C       1.1.1.1/32 is directly connected, loopback1
O       2.2.2.2/32 [110/10050] via 172.16.203.2, agg1, 00:09:25, [1/0]
O IA    3.3.3.3/32 [110/11050] via 172.16.203.2, agg1, 00:09:25, [1/0]
O IA    4.4.4.4/32 [110/10150] via 172.16.203.2, agg1, 00:09:25, [1/0]
S       10.1.100.0/24 [10/0] via 172.16.203.2, agg1, [1/0]
C       172.16.14.1/32 is directly connected, vlax63
O IA    172.16.200.0/24 [110/1050] via 172.16.203.2, agg1, 00:09:25, [1/0]
S       172.16.202.0/24 [10/0] via 172.16.203.2, agg1, [1/0]
C       172.16.203.0/24 is directly connected, agg1
S       172.16.204.0/24 [10/0] via 172.16.203.2, agg1, [1/0]
O IA    172.16.212.2/32 [110/150] via 172.16.203.2, agg1, 00:09:25, [1/0]
B       172.25.1.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
00:01:54, [1/0]
```

```
B       172.26.1.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
00:01:54, [1/0]
B       172.26.2.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
00:01:54, [1/0]
B       172.28.0.0/16 [200/0] is a summary, Null, 00:03:25, [1/0]
B       172.28.1.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1), 00:03:25,
[1/0]
B       172.28.2.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1), 00:03:25,
[1/0]
B       172.28.5.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1), 00:03:25,
[1/0]
B       172.28.6.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1), 00:03:25,
[1/0]
O E2    172.31.4.0/22 [110/25] via 172.16.203.2, agg1, 00:09:24, [1/0]
```

2. Verify the routing table entries filtered on VRF ID 63:

   ```
   # get router info filter vrf 63
   ```

   a. BGP routing table:

      ```
      # get router info routing-table bgp
      Routing table for VRF=63
      B       172.25.1.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
      00:02:44, [1/0]
      B       172.26.1.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
      00:02:44, [1/0]
      B       172.26.2.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
      00:02:44, [1/0]
      B       172.28.0.0/16 [200/0] is a summary, Null, 00:04:15, [1/0]
      B       172.28.1.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
      00:04:15, [1/0]
      B       172.28.2.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
      00:04:15, [1/0]
      B       172.28.5.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
      00:04:15, [1/0]
      B       172.28.6.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
      00:04:15, [1/0]
      ```

   b. All routing table entries:

      ```
      # get router info routing-table all
      Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
             O - OSPF, IA - OSPF inter area
             N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
             E1 - OSPF external type 1, E2 - OSPF external type 2
             i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
             V - BGP VPNv4
             * - candidate default

      Routing table for VRF=63
      C       1.1.1.1/32 is directly connected, loopback1
      O       2.2.2.2/32 [110/10050] via 172.16.203.2, agg1, 00:10:18, [1/0]
      O IA    3.3.3.3/32 [110/11050] via 172.16.203.2, agg1, 00:10:18, [1/0]
      O IA    4.4.4.4/32 [110/10150] via 172.16.203.2, agg1, 00:10:18, [1/0]
      S       10.1.100.0/24 [10/0] via 172.16.203.2, agg1, [1/0]
      C       172.16.14.1/32 is directly connected, vlax63
      O IA    172.16.200.0/24 [110/1050] via 172.16.203.2, agg1, 00:10:18, [1/0]
      ```

```
S       172.16.202.0/24 [10/0] via 172.16.203.2, agg1, [1/0]
C       172.16.203.0/24 is directly connected, agg1
S       172.16.204.0/24 [10/0] via 172.16.203.2, agg1, [1/0]
O IA    172.16.212.2/32 [110/150] via 172.16.203.2, agg1, 00:10:18, [1/0]
B       172.25.1.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
00:02:47, [1/0]
B       172.26.1.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
00:02:47, [1/0]
B       172.26.2.0/24 [200/0] via 2.2.2.2 [2] (recursive via 172.16.203.2, agg1),
00:02:47, [1/0]
B       172.28.0.0/16 [200/0] is a summary, Null, 00:04:18, [1/0]
B       172.28.1.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
00:04:18, [1/0]
B       172.28.2.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
00:04:18, [1/0]
B       172.28.5.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
00:04:18, [1/0]
B       172.28.6.0/24 [200/0] via 3.3.3.3 (recursive via 172.16.203.2, agg1),
00:04:18, [1/0]
O E2    172.31.4.0/22 [110/25] via 172.16.203.2, agg1, 00:10:17, [1/0]
```

3. Run debugs on the VRF:

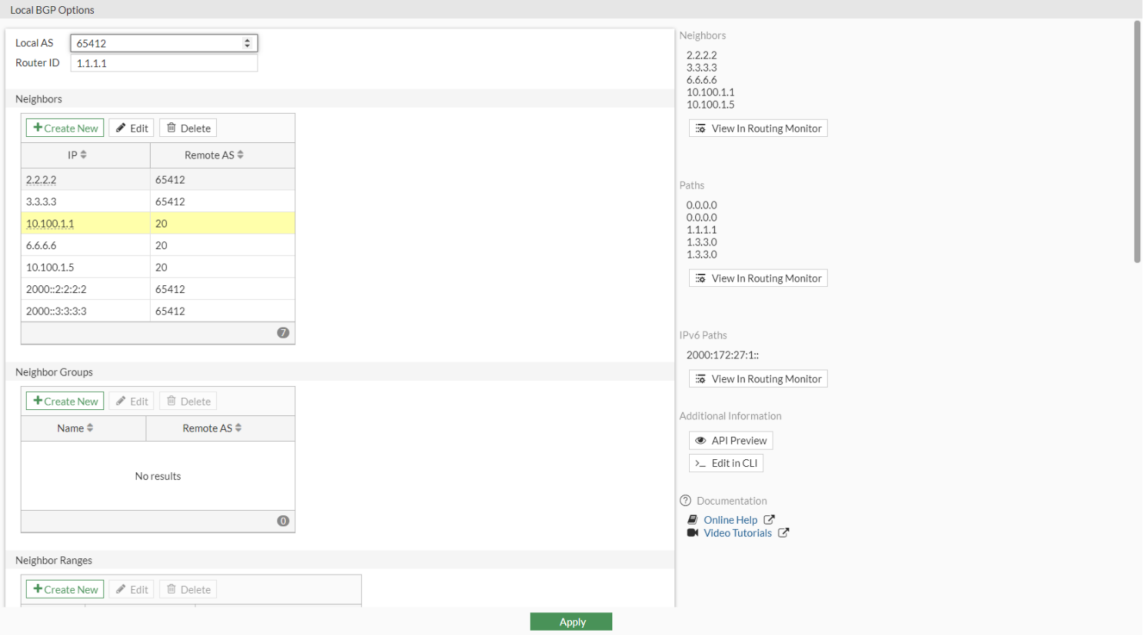
```
# diagnose ip router bgp set-filter vrf 63
# diagnose ip router bgp level info
# diagnose ip router bgp all enable

BGP: 2003::3:3:3:3-Outgoing [DECODE] Msg-Hdr: type 4, length 19
BGP: 2003::3:3:3:3-Outgoing [DECODE] KAlive: Received!
BGP: 2003::3:3:3:3-Outgoing [FSM] State: Established Event: 26
BGP: 2003::2:2:2:2-Outgoing [FSM] State: Established Event: 34
BGP: 2003::2:2:2:2-Outgoing [DECODE] Msg-Hdr: type 4, length 19
BGP: 2003::2:2:2:2-Outgoing [DECODE] KAlive: Received!
BGP: 2003::2:2:2:2-Outgoing [FSM] State: Established Event: 26
BGP: 2.2.2.2-Outgoing [FSM] State: Established Event: 34
BGP: 2003::3:3:3:3-Outgoing [FSM] State: Established Event: 34
BGP: 2.2.2.2-Outgoing [ENCODE] Msg-Hdr: Type 4
BGP: 2.2.2.2-Outgoing [ENCODE] Keepalive: 963 KAlive msg(s) sent
BGP: 2003::3:3:3:3-Outgoing [ENCODE] Msg-Hdr: Type 4
BGP: 2003::3:3:3:3-Outgoing [ENCODE] Keepalive: 965 KAlive msg(s) sent
BGP: 2003::3:3:3:3-Outgoing [FSM] State: Established Event: 34
BGP: 2003::2:2:2:2-Outgoing [FSM] State: Established Event: 34
BGP: 2.2.2.2-Outgoing [FSM] State: Established Event: 34
BGP: 3.3.3.3-Outgoing [DECODE] Msg-Hdr: type 4, length 19
BGP: 3.3.3.3-Outgoing [DECODE] KAlive: Received!
BGP: 3.3.3.3-Outgoing [FSM] State: Established Event: 26

BGP: [RIB] Scanning BGP Network Routes for VRF 63...
BGP: 2003::2:2:2:2-Outgoing [FSM] State: Established Event: 34
BGP: 2003::3:3:3:3-Outgoing [FSM] State: Established Event: 34
```

GUI support for advanced BGP options - 7.2.1

Advanced BGP options can be configured in the GUI on the *Network* > *BGP* page, including: the BGP neighbor local AS, hold time timer, keepalive timer, and enforcing eBGP multihop. The *View in Routing Monitor* buttons in the right-side of the screen can display the BGP neighbors list, the BGP IPv4 routing table, or the BGP IPv6 routing table in a slide-out window instead of redirecting to the monitor page. The *Routing* monitor includes an option to soft reset a neighbor from the BGP neighbors list.

BGP page enhancements

The *View in Routing Monitor* button is available to view neighbors, paths, and IPv6 paths.



Local BGP Options

Local AS: 65412
Router ID: 1.1.1.1

Neighbors

+Create New | Edit | Delete

IP	Remote AS
2.2.2.2	65412
3.3.3.3	65412
10.100.1.1	20
6.6.6.6	20
10.100.1.5	20
2000::2:2:2:2	65412
2000::3:3:3:3	65412

Neighbor Groups

+Create New | Edit | Delete

Name	Remote AS
No results	

Neighbor Ranges

+Create New | Edit | Delete

Neighbors
2.2.2.2
3.3.3.3
6.6.6.6
10.100.1.1
10.100.1.5

View In Routing Monitor

Paths
0.0.0.0
0.0.0.0
1.1.1.1
1.3.3.0
1.3.3.0

View In Routing Monitor

IPv6 Paths
2000:172:27:1::

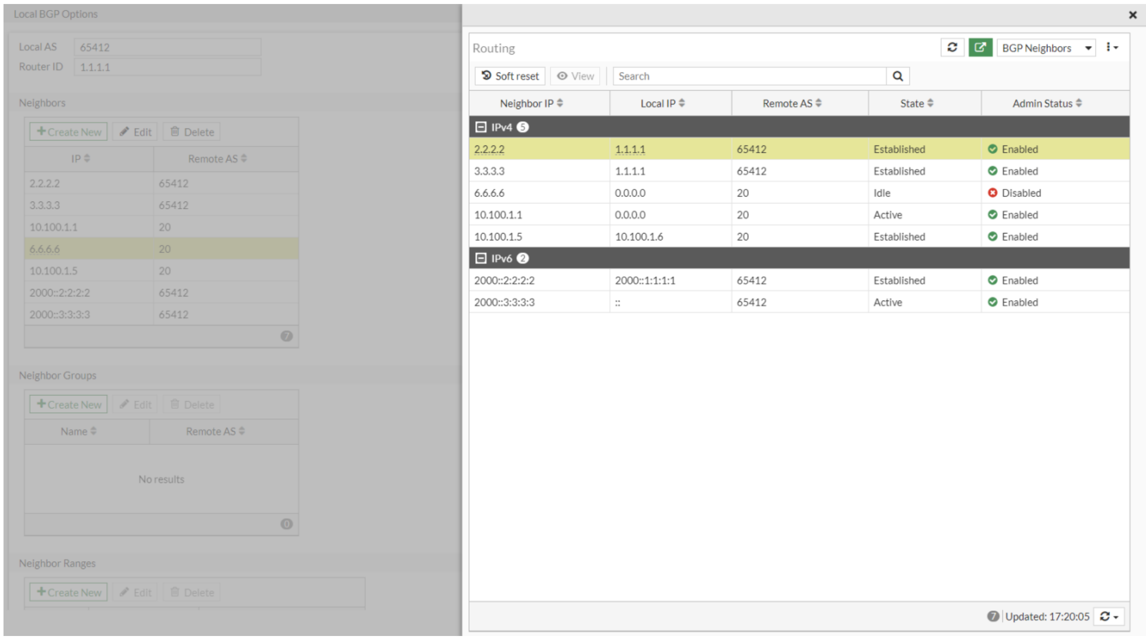
View In Routing Monitor

Additional Information
API Preview
Edit in CLI

Documentation
Online Help
Video Tutorials

Apply

- *Routing* monitor dropdown selected to display *BGP Neighbors*:



Local BGP Options

Local AS: 65412
Router ID: 1.1.1.1

Neighbors

+Create New | Edit | Delete

IP	Remote AS
2.2.2.2	65412
3.3.3.3	65412
10.100.1.1	20
6.6.6.6	20
10.100.1.5	20
2000::2:2:2:2	65412
2000::3:3:3:3	65412

Neighbor Groups

+Create New | Edit | Delete

Name	Remote AS
No results	

Neighbor Ranges

+Create New | Edit | Delete

Routing — BGP Neighbors

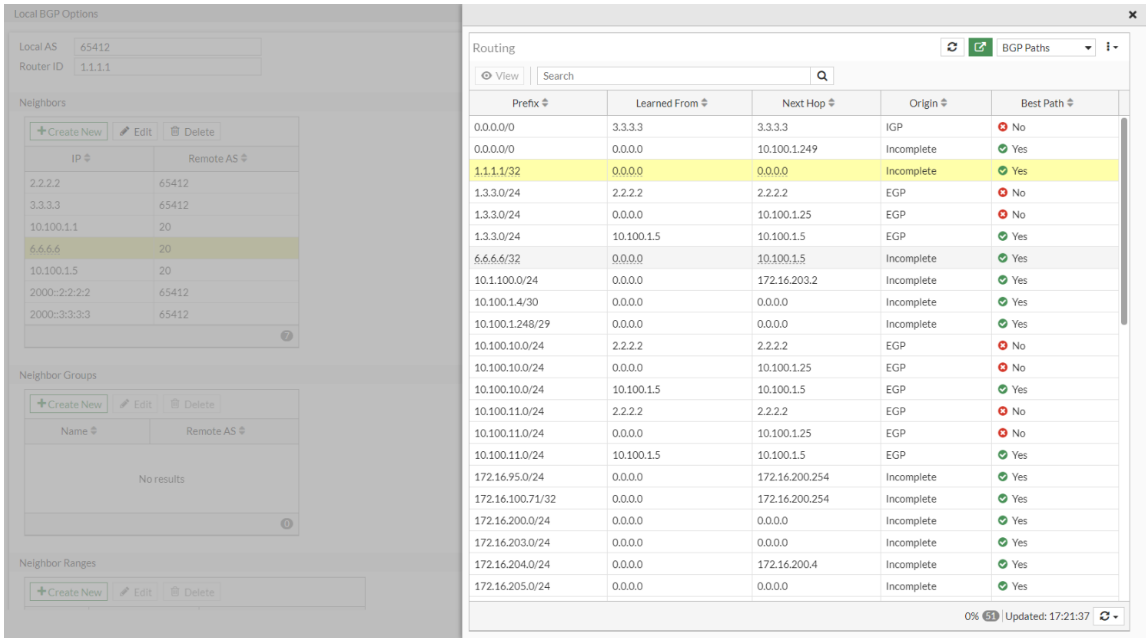
Soft reset | View | Search

Neighbor IP	Local IP	Remote AS	State	Admin Status
IPv4 5				
2.2.2.2	1.1.1.1	65412	Established	✓ Enabled
3.3.3.3	1.1.1.1	65412	Established	✓ Enabled
6.6.6.6	0.0.0.0	20	Idle	✗ Disabled
10.100.1.1	0.0.0.0	20	Active	✓ Enabled
10.100.1.5	10.100.1.6	20	Established	✓ Enabled
IPv6 2				
2000::2:2:2:2	2000::1:1:1:1	65412	Established	✓ Enabled
2000::3:3:3:3	::	65412	Active	✓ Enabled

Updated: 17:20:05

When a neighbor is selected, the *Soft reset* option is available.

- *Routing* monitor dropdown selected to display *BGP Paths*:



Local BGP Options

Local AS 65412
Router ID 1.1.1.1

Neighbors

+Create New | Edit | Delete

IP	Remote AS
2.2.2.2	65412
3.3.3.3	65412
10.100.1.1	20
6.6.6.6	20
10.100.1.5	20
2000::2:2:2:2	65412
2000::3:3:3:3	65412

Neighbor Groups

+Create New | Edit | Delete

Name	Remote AS

No results

Neighbor Ranges

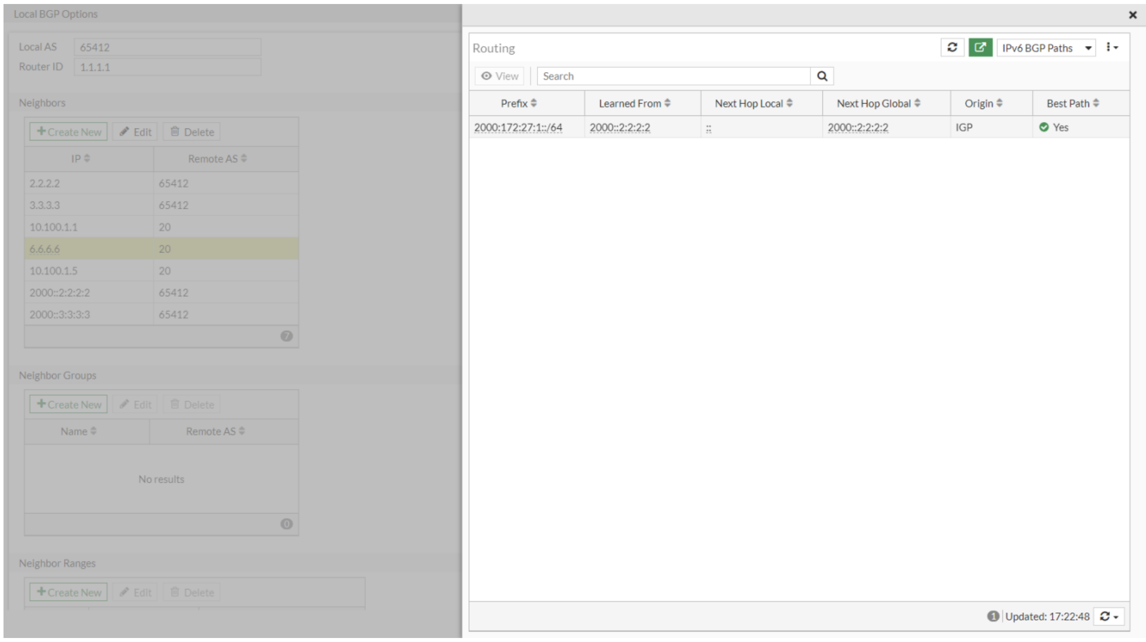
+Create New | Edit | Delete

Routing — BGP Paths

Prefix	Learned From	Next Hop	Origin	Best Path
0.0.0.0/0	3.3.3.3	3.3.3.3	IGP	✗ No
0.0.0.0/0	0.0.0.0	10.100.1.249	Incomplete	✓ Yes
1.1.1.1/32	0.0.0.0	0.0.0.0	Incomplete	✓ Yes
1.3.3.0/24	2.2.2.2	2.2.2.2	EGP	✗ No
1.3.3.0/24	0.0.0.0	10.100.1.25	EGP	✗ No
1.3.3.0/24	10.100.1.5	10.100.1.5	EGP	✓ Yes
6.6.6.6/32	0.0.0.0	10.100.1.5	Incomplete	✓ Yes
10.1.100.0/24	0.0.0.0	172.16.203.2	Incomplete	✓ Yes
10.100.1.4/30	0.0.0.0	0.0.0.0	Incomplete	✓ Yes
10.100.1.248/29	0.0.0.0	0.0.0.0	Incomplete	✓ Yes
10.100.10.0/24	2.2.2.2	2.2.2.2	EGP	✗ No
10.100.10.0/24	0.0.0.0	10.100.1.25	EGP	✗ No
10.100.10.0/24	10.100.1.5	10.100.1.5	EGP	✓ Yes
10.100.11.0/24	2.2.2.2	2.2.2.2	EGP	✗ No
10.100.11.0/24	0.0.0.0	10.100.1.25	EGP	✗ No
10.100.11.0/24	10.100.1.5	10.100.1.5	EGP	✓ Yes
172.16.95.0/24	0.0.0.0	172.16.200.254	Incomplete	✓ Yes
172.16.100.71/32	0.0.0.0	172.16.200.254	Incomplete	✓ Yes
172.16.200.0/24	0.0.0.0	0.0.0.0	Incomplete	✓ Yes
172.16.203.0/24	0.0.0.0	0.0.0.0	Incomplete	✓ Yes
172.16.204.0/24	0.0.0.0	172.16.200.4	Incomplete	✓ Yes
172.16.205.0/24	0.0.0.0	0.0.0.0	Incomplete	✓ Yes

0% 51 Updated: 17:21:37

- *Routing* monitor dropdown selected to display *IPv6 BGP Paths*:



Local BGP Options

Local AS 65412
Router ID 1.1.1.1

Neighbors

+Create New | Edit | Delete

IP	Remote AS
2.2.2.2	65412
3.3.3.3	65412
10.100.1.1	20
6.6.6.6	20
10.100.1.5	20
2000::2:2:2:2	65412
2000::3:3:3:3	65412

Neighbor Groups

+Create New | Edit | Delete

Name	Remote AS

No results

Neighbor Ranges

+Create New | Edit | Delete

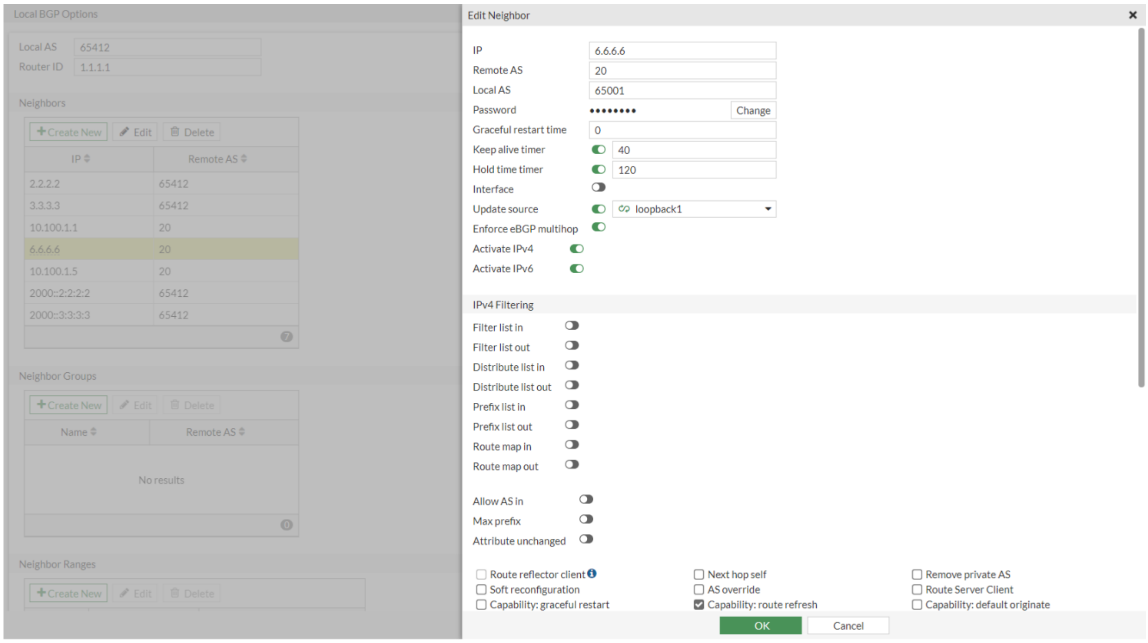
Routing — IPv6 BGP Paths

Prefix	Learned From	Next Hop Local	Next Hop Global	Origin	Best Path
2000:172:27:1::/64	2000::2:2:2:2	::	2000::2:2:2:2	IGP	✓ Yes

1 Updated: 17:22:48

Neighbor configuration page enhancements

There are fields to enter the *Local AS*, *Keep alive timer*, *Hold time timer*, and *Enforce eBGP multihop*.



Local BGP Options

Local AS 65412

Router ID 1.1.1.1

Neighbors

IP	Remote AS
2.2.2.2	65412
3.3.3.3	65412
10.100.1.1	20
6.6.6.6	20
10.100.1.5	20
2000::2:2:2:2	65412
2000::3:3:3:3	65412

7

Neighbor Groups

Name	Remote AS
No results	

0

Neighbor Ranges

Edit Neighbor

IP	6.6.6.6
Remote AS	20
Local AS	65001
Password	•••••••• Change
Graceful restart time	0
Keep alive timer	● 40
Hold time timer	● 120
Interface	○
Update source	● loopback1
Enforce eBGP multihop	●
Activate IPv4	●
Activate IPv6	●

IPv4 Filtering

Filter list in	○
Filter list out	○
Distribute list in	○
Distribute list out	○
Prefix list in	○
Prefix list out	○
Route map in	○
Route map out	○
Allow AS in	○
Max prefix	○
Attribute unchanged	○

□ Route reflector client	□ Next hop self	□ Remove private AS
□ Soft reconfiguration	□ AS override	□ Route Server Client
□ Capability: graceful restart	☑ Capability: route refresh	□ Capability: default originate

Support BGP AS number input in asdot and asdot+ format - 7.2.1

BGP Autonomous System (AS) numbers can be inputted in asdot and asdot+ format in compliance with RFC 5396 when configuring the following in the CLI.

- BGP AS, neighbor local and remote AS, and neighbor group local and remote AS:

```
config router bgp
       set as <string>
       config neighbor
        edit <ip>
            set remote-as <string>
            set local-as <string>
        next
    end
    config neighbor-group
        edit <name>
            set remote-as <string>
            set local-as <string>
        next
    end
end
```

`as <string>`	Enter the router AS number in asplain (1 - 4294967295), asdot, or asdot+ format. Enter 0 to disable BGP.
`remote-as <string>`	Enter a value in asplain (1 - 4294967295), asdot, or asdot+ format.
`local-as <string>`	Enter a value in asplain (1 - 4294967295), asdot, or asdot+ format.

- Route map AS path:

```
config router route-map
    edit <name>
        config rule
            edit <id>
                set set-aspath <string>
            next
        end
    next
end
```

`set-aspath <string>`	Enter a value in asplain (1 - 4294967295), asdot, or asdot+ format.

`get router info bgp summary` and other BGP router commands still display the AS numbers in asplain format.

Example

In this example, neighbor 1.1.1.1's remote AS is configured in asdot format. Neighbor 172.16.201.2's remote AS is configured in asdot format, and the local AS in asplain format.

To configure the AS in asdot and asplain formats:

```
config router bgp
    set as 65535.65535
    set router-id 3.3.3.3
    config neighbor
        edit "1.1.1.1"
            set remote-as 65535.65535
        next
        edit "172.16.201.2"
            set remote-as 65050
            set local-as 65516.65516
        next
    end
end
```

To verify the BGP neighbors and routing table:

```
# get router info bgp summary
VRF 0 BGP router identifier 3.3.3.3, local AS number 4294967295
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
1.1.1.1 4 4294967295 21 18 3 0 0 00:04:09 13
172.16.201.2 4 65050 24 28 4 0 0 00:05:42 4

Total number of neighbors 2
```

The BGP AS number `65535.65535` in asdot format corresponds to AS number `4294967295` in asplain format in this output.

SNMP OIDs with details about authenticated users - 7.2.1

The fgFwAuthUserTables SNMP table gathers information about authenticated users. These are users that have been authenticated by methods supported on the FortiGate (local, FSSO, RSSO, and so on). This table supports SNMP VDOM access control and OIDs for IPv4 and IPv6 authenticated users.

Category	Name	OID
Number of firewall authenticated users in each VDOM	fgFwAuthUserTables.fgFwAuthUserInfoTable.fgFwAuthUserInfoEntry.fgFwAuthUserInfoVdom	1.3.6.1.4.1.12356.101.5.2.3.1.1.1
	fgFwAuthUserTables.fgFwAuthUserInfoTable.fgFwAuthUserInfoEntry.fgFwAuthIpv4UserNumber	1.3.6.1.4.1.12356.101.5.2.3.1.1.2
	fgFwAuthUserTables.fgFwAuthUserInfoTable.fgFwAuthUserInfoEntry.fgFwAuthIpv6UserNumber	1.3.6.1.4.1.12356.101.5.2.3.1.1.3
List of authenticated users in each VDOM (IPv4)	fgFwAuthUserTables.fgFwAuthIpv4UserTable.fgFwAuthIpv4UserEntry.fgFwAuthIpv4UserIndex	1.3.6.1.4.1.12356.101.5.2.3.2.1.1
	fgFwAuthUserTables.fgFwAuthIpv4UserTable.fgFwAuthIpv4UserEntry.fgFwAuthIpv4UserVdom	1.3.6.1.4.1.12356.101.5.2.3.2.1.2
	fgFwAuthUserTables.fgFwAuthIpv4UserTable.fgFwAuthIpv4UserEntry.fgFwAuthIpv4UserName	1.3.6.1.4.1.12356.101.5.2.3.2.1.3
	fgFwAuthUserTables.fgFwAuthIpv4UserTable.fgFwAuthIpv4UserEntry.fgFwAuthIpv4UserType	1.3.6.1.4.1.12356.101.5.2.3.2.1.4
	fgFwAuthUserTables.fgFwAuthIpv4UserTable.fgFwAuthIpv4UserEntry.fgFwAuthIpv4UserAddr	1.3.6.1.4.1.12356.101.5.2.3.2.1.5
List of authenticated users in each VDOM (IPv6)	fgFwAuthUserTables.fgFwAuthIpv6UserTable.fgFwAuthIpv6UserEntry.fgFwAuthIpv6UserIndex	1.3.6.1.4.1.12356.101.5.2.3.3.1.1
	fgFwAuthUserTables.fgFwAuthIpv6UserTable.fgFwAuthIpv6UserEntry.fgFwAuthIpv6UserVdom	1.3.6.1.4.1.12356.101.5.2.3.3.1.2
	fgFwAuthUserTables.fgFwAuthIpv6UserTable.fgFwAuthIpv6UserEntry.fgFwAuthIpv6UserName	1.3.6.1.4.1.12356.101.5.2.3.3.1.3
	fgFwAuthUserTables.fgFwAuthIpv6UserTable.fgFwAuthIpv6UserEntry.fgFwAuthIpv6UserType	1.3.6.1.4.1.12356.101.5.2.3.3.1.4
	fgFwAuthUserTables.fgFwAuthIpv6UserTable.fgFwAuthIpv6UserEntry.fgFwAuthIpv6UserAddr	1.3.6.1.4.1.12356.101.5.2.3.3.1.5

Example 1: when there is an IPv4 and IPv6 authenticated user

SNMP query:

```
snmpwalk -v1 -c REGR-SYS 172.16.200.1 1.3.6.1.4.1.12356.101.5.2.3-----------------------------
---------------------------------------------------> fgFwAuthUserTable
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.1 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.2 = INTEGER: 2-------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.3 = INTEGER: 3-------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.1 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.2 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.3 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.1 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.2 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.3 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.1.1 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserIndex
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.2.1 = INTEGER: 2-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserVdom
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.3.1 = STRING: "IPvUser"------------------------------
---------------------------------------------->fgFwAuthIpv4UserName
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.4.1 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserType
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.5.1 = IpAddress: 172.16.200.55-----------------------
-------------------------------------------->fgFwAuthIpv4UserAddr
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.1.1 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserIndex
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.2.1 = INTEGER: 2-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserVdom
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.3.1 = STRING: "IPv6prefUser"-------------------------
-------------------------------------------->fgFwAuthIpv6UserName
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.4.1 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserType
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.5.1 = Hex-STRING: 20 00 01 72 00 16 02 00 00 00 00
00 00 00 00 00---------------->fgFwAuthIpv6UserAddr
```

To verify the authenticated user list in FortiOS:

```
# diagnose firewall auth list
172.16.200.55, IPvUser
        type: rsso, id: 0, duration: 5, idled: 5
        flag(12): deny radius
        server: vdom1
        packets: in 0 out 0, bytes: in 0 out 0

----- 1 listed, 0 filtered ------
```

```
# diagnose firewall auth ipv6 list
2000:172:16:200::/64, IPv6prefUser
        type: rsso, id: 0, duration: 183, idled: 183
        flag(12): deny radius
        server: vdom1
        packets: in 0 out 0, bytes: in 0 out 0

----- 1 listed, 0 filtered ------
```

Example 2: when there is an IPv4 authenticated user and no IPv6 authenticated user

SNMP query:

```
snmpwalk -v1 -c REGR-SYS 172.16.200.1 1.3.6.1.4.1.12356.101.5.2.3----------------------------
--------------------------------------------------> fgFwAuthUserTable
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.1 = INTEGER: 1-------------------------------------
----------------------------------------------->fgFwAuthUserInfoVdom (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.2 = INTEGER: 2-------------------------------------
----------------------------------------------->fgFwAuthUserInfoVdom (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.3 = INTEGER: 3-------------------------------------
----------------------------------------------->fgFwAuthUserInfoVdom (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.1 = INTEGER: 0-------------------------------------
----------------------------------------------->fgFwAuthIpv4UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.2 = INTEGER: 1-------------------------------------
----------------------------------------------->fgFwAuthIpv4UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.3 = INTEGER: 0-------------------------------------
----------------------------------------------->fgFwAuthIpv4UserNumber (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.1 = INTEGER: 0-------------------------------------
----------------------------------------------->fgFwAuthIpv6UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.2 = INTEGER: 1-------------------------------------
----------------------------------------------->fgFwAuthIpv6UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.3 = INTEGER: 0-------------------------------------
----------------------------------------------->fgFwAuthIpv6UserNumber (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.1.1 = INTEGER: 1-------------------------------------
----------------------------------------------->fgFwAuthIpv4UserIndex
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.2.1 = INTEGER: 2-------------------------------------
----------------------------------------------->fgFwAuthIpv4UserVdom
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.3.1 = STRING: "IPvUser"------------------------------
--------------------------------------------->fgFwAuthIpv4UserName
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.4.1 = INTEGER: 1-------------------------------------
----------------------------------------------->fgFwAuthIpv4UserType
FORTINET-FORTIGATE-MIB::fgFwUsers.3.2.1.5.1 = IpAddress: 172.16.200.55-----------------------
------------------------------------------->fgFwAuthIpv4UserAddr
```

To verify the authenticated user list in FortiOS:

```
# diagnose firewall auth list
172.16.200.55, IPvUser
        type: rsso, id: 0, duration: 127, idled: 127
        flag(12): deny radius
        server: vdom1
        packets: in 0 out 0, bytes: in 0 out 0

----- 1 listed, 0 filtered ------
```

```
# diagnose firewall auth ipv6 list

----- 0 listed, 0 filtered ------
```

Example 3: when there is an IPv6 authenticated user and no IPv4 authenticated user

SNMP query:

```
snmpwalk -v1 -c REGR-SYS 172.16.200.1 1.3.6.1.4.1.12356.101.5.2.3---------------------------
--------------------------------------------------> fgFwAuthUserTable
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.1 = INTEGER: 1------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.2 = INTEGER: 2------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.3 = INTEGER: 3------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.1 = INTEGER: 0------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.2 = INTEGER: 1------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.3 = INTEGER: 0------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.1 = INTEGER: 0------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.2 = INTEGER: 1------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.3 = INTEGER: 0------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.1.1 = INTEGER: 1------------------------------------
------------------------------------------------>fgFwAuthIpv6UserIndex
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.2.1 = INTEGER: 2------------------------------------
------------------------------------------------>fgFwAuthIpv6UserVdom
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.3.1 = STRING: "IPv6prefUser"------------------------
-------------------------------------------->fgFwAuthIpv6UserName
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.4.1 = INTEGER: 1------------------------------------
------------------------------------------------>fgFwAuthIpv6UserType
FORTINET-FORTIGATE-MIB::fgFwUsers.3.3.1.5.1 = Hex-STRING: 20 00 01 72 00 16 02 00 00 00 00
00 00 00 00 00---------------->fgFwAuthIpv6UserAddr
```

To verify the authenticated user list in FortiOS:

```
# diagnose firewall auth list

----- 0 listed, 0 filtered ------

# diagnose firewall auth ipv6 list
2000:172:16:200::/64, IPv6prefUser
        type: rsso, id: 0, duration: 69, idled: 69
        flag(12): deny radius
        server: vdom1
        packets: in 0 out 0, bytes: in 0 out 0

----- 1 listed, 0 filtered ------
```

Example 4: when there are no authenticated users

SNMP query:

```
snmpwalk -v1 -c REGR-SYS 172.16.200.1 1.3.6.1.4.1.12356.101.5.2.3---------------------------
--------------------------------------------------> fgFwAuthUserTable
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.1 = INTEGER: 1-------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.2 = INTEGER: 2-------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.1.3 = INTEGER: 3-------------------------------------
------------------------------------------------>fgFwAuthUserInfoVdom (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.1 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.2 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.2.3 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv4UserNumber (vdom2)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.1 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (root)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.2 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (vdom1)
FORTINET-FORTIGATE-MIB::fgFwUsers.3.1.1.3.3 = INTEGER: 0-------------------------------------
------------------------------------------------>fgFwAuthIpv6UserNumber (vdom2)
```

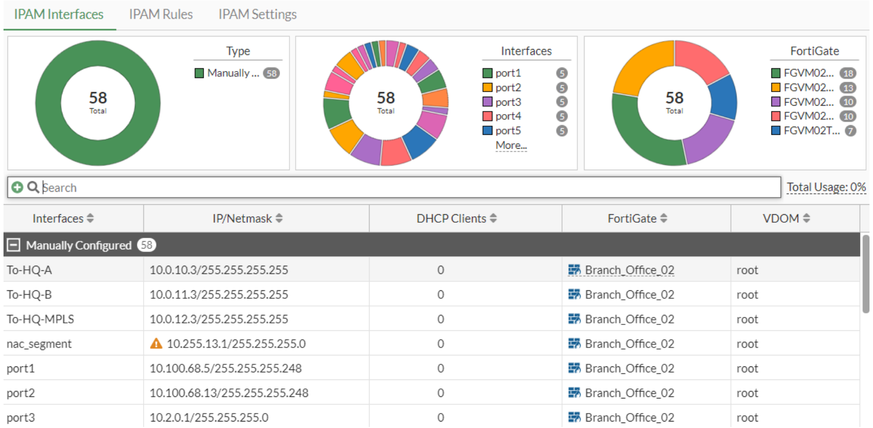
To verify the authenticated user list in FortiOS:

```
# diagnose firewall auth  list

----- 0 listed, 0 filtered ------

# diagnose firewall auth ipv6  list

----- 0 listed, 0 filtered -----
```

Add new IPAM GUI page - 7.2.1

IP address management (IPAM) details have been migrated to a centralized *Network > IPAM* page. The *IPAM* page replaces the *Security Fabric > Fabric Connectors > IPAM* widget and uses three tabs to display information:

- *IPAM Interfaces*
- *IPAM Rules*
- *IPAM Settings*



Interfaces	IP/Netmask	DHCP Clients	FortiGate	VDOM
Manually Configured 58				
To-HQ-A	10.0.10.3/255.255.255.255	0	Branch_Office_02	root
To-HQ-B	10.0.11.3/255.255.255.255	0	Branch_Office_02	root
To-HQ-MPLS	10.0.12.3/255.255.255.255	0	Branch_Office_02	root
nac_segment	⚠ 10.255.13.1/255.255.255.0	0	Branch_Office_02	root
port1	10.100.68.5/255.255.255.248	0	Branch_Office_02	root
port2	10.100.68.13/255.255.255.248	0	Branch_Office_02	root
port3	10.2.0.1/255.255.255.0	0	Branch_Office_02	root

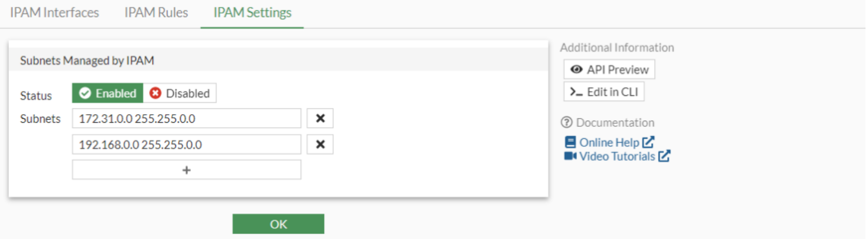
The *IPAM* page is only viewable on a FortiGate that is not in a Security Fabric or on the root FortiGate in a Security Fabric. Downstream FortiGates in a Security Fabric will display a notification to view the root FortiGate.

To enable IPAM status in the GUI:

1. Go to *Network > IPAM > IPAM Settings*.
2. Select *Enabled*. The *Subnets* field is displayed.

IPAM status is disabled by default. After performing a factory reset, enabled IPAM status will auto-generate two subnets. These subnets can be modified and deleted.

3. Enter the IP address and netmask in the *Subnets* field. Additional subnets can be added using the +.



Subnets Managed by IPAM

Status: ● Enabled ○ Disabled

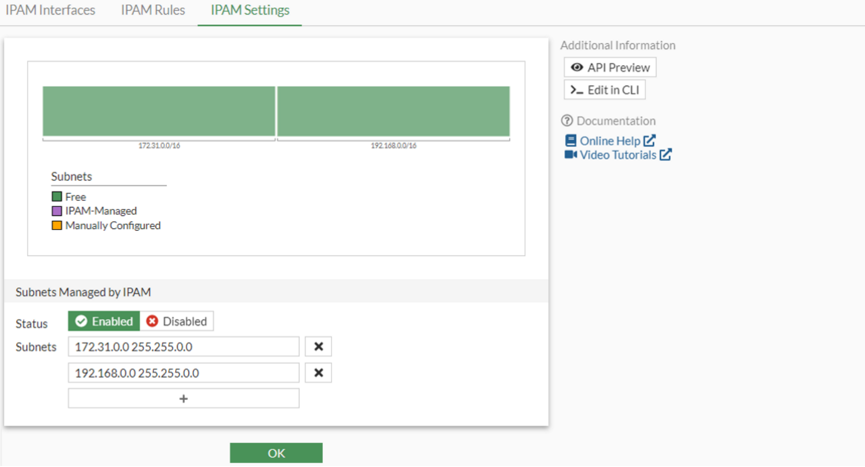
Subnets: 172.31.0.0 255.255.0.0 ✕

192.168.0.0 255.255.0.0 ✕

+

4. Click *OK*. A chart is displayed showing available space and IP address overlap between *IPAM-Managed* and

Manually Configured IP addresses.



Subnets Managed by IPAM

Status: Enabled | Disabled

Subnets: 172.31.0.0 255.255.0.0

192.168.0.0 255.255.0.0

To enable IPAM status in the CLI:

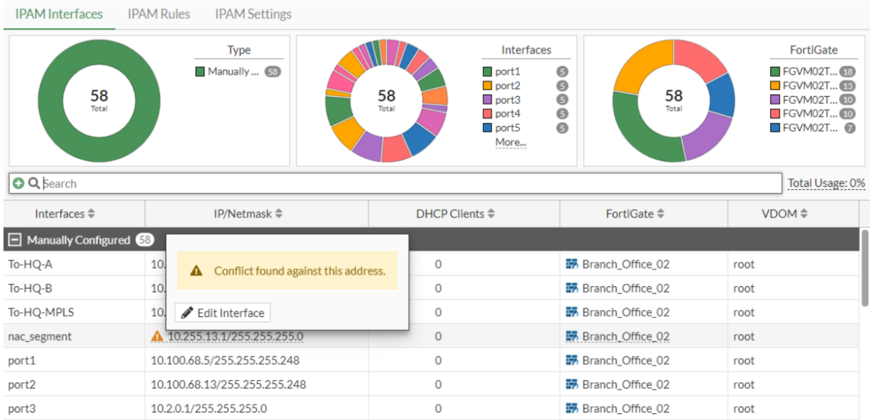
```
config system ipam
    set status enable
    config pools
        edit "default-pool"
            set subnet 172.31.0.0 255.255.0.0
        next
        edit "lan-pool"
            set subnet 192.168.0.0 255.255.0.0
        next
    end
end
```

IPAM conflict markers

The *IPAM Interfaces* tab displays conflict markers when there are IP pool IP address conflicts with manually configured IP addresses. Administrators can use the *Edit Interface* dialog to manually resolve the conflict.

To resolve conflicts in the GUI:

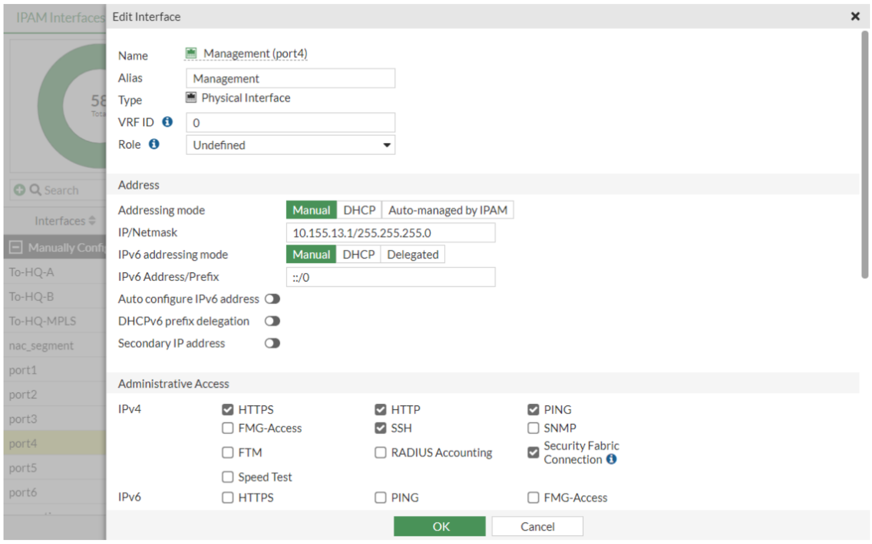
1. Go to *Network* > *IPAM* > *IPAM Interfaces*.
2. Hover your mouse over the conflict marker. The conflict marker information is displayed.



Conflict found against this address.

Interfaces	IP/Netmask	DHCP Clients	FortiGate	VDOM
Manually Configured 58				
To-HQ-A	10.	0	Branch_Office_02	root
To-HQ-B	10.	0	Branch_Office_02	root
To-HQ-MPLS	10.	0	Branch_Office_02	root
nac_segment	⚠ 10.255.13.1/255.255.255.0	0	Branch_Office_02	root
port1	10.100.68.5/255.255.255.248	0	Branch_Office_02	root
port2	10.100.68.13/255.255.255.248	0	Branch_Office_02	root
port3	10.2.0.1/255.255.255.0	0	Branch_Office_02	root

3. Click *Edit Interface*. The *Edit Interface* pane opens.



Edit Interface

Name: Management (port4)
Alias: Management
Type: Physical Interface
VRF ID: 0
Role: Undefined

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask: 10.155.13.1/255.255.255.0
IPv6 addressing mode: [✓ Manual] DHCP Delegated
IPv6 Address/Prefix: ::/0
Auto configure IPv6 address ○
DHCPv6 prefix delegation ○
Secondary IP address ○

Administrative Access

IPv4: ☑ HTTPS ☑ HTTP ☑ PING □ FMG-Access ☑ SSH □ SNMP □ FTM □ RADIUS Accounting ☑ Security Fabric Connection □ Speed Test
IPv6: □ HTTPS □ PING □ FMG-Access

4. Enter a new IP address and netmask in the *IP/Netmask* field.
5. Click *OK*. A confirmation message is displayed.
6. Click *OK*.

Assign multiple IP pools and subnets using IPAM Rules - 7.2.1

Multiple IP pools can be assigned to different interfaces based on name and role using the *IPAM Rules* tab on the *Network* > *IPAM* page. This allows more flexibility when enabling network segmentation.

IPAM pools and rules can be defined on a FortiGate not in a Security Fabric or in the root FortiGate of a Security Fabric.

IPAM pools can be defined using the `config pools` command:

```
config system ipam
    config pools
        edit <pool_name>
```

```
            set subnet <IP address/netmask>
        next
    end
end
```

IPAM rules can be defined using the `config rules` command:

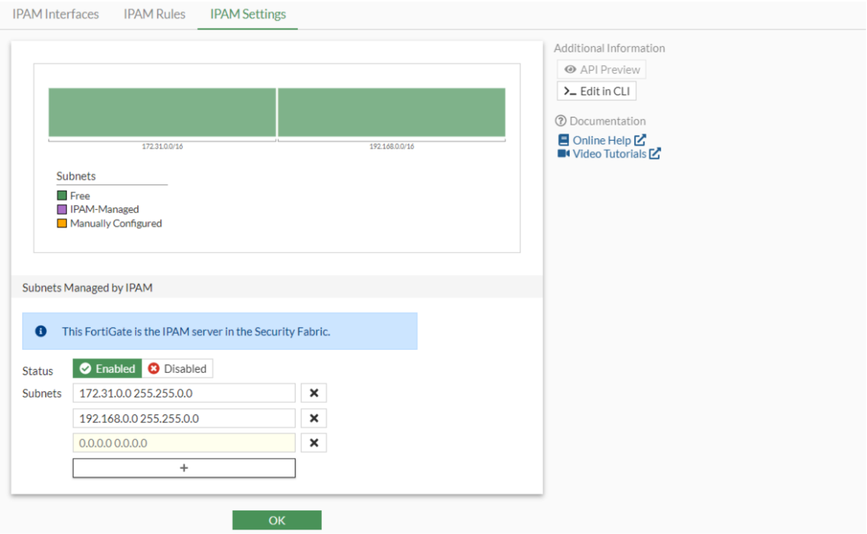
```
config system ipam
    config rules
        edit <rule_name>
            set device {<FortiGate_serial_number> | *}
            set interface {<name> | *}
            set pool <pool_name>
        next
    end
end
```

A DHCP server can also be configured for IPAM-enabled interfaces using the following command.

```
# execute ipam create-dhcp-server <interface>
```

To configure IPAM rules in the GUI:

1. Enable IPAM status. See Add new IPAM GUI page 7.2.1 on page 197 for more information.
2. Configure the subnet:
   a. Go to *Network* > *IPAM* > *IPAM Settings*.
   b. Select the + in the *Subnets Managed by IPAM* section. A new *Subnets* field is displayed.



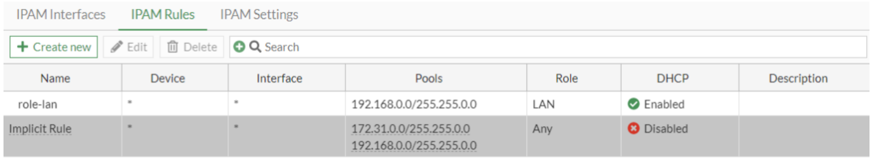
Subnets Managed by IPAM

This FortiGate is the IPAM server in the Security Fabric.

Status: ✓ Enabled [selected] ✗ Disabled

Subnets: 172.31.0.0 255.255.0.0 ✕
192.168.0.0 255.255.0.0 ✕
0.0.0.0 0.0.0.0 ✕

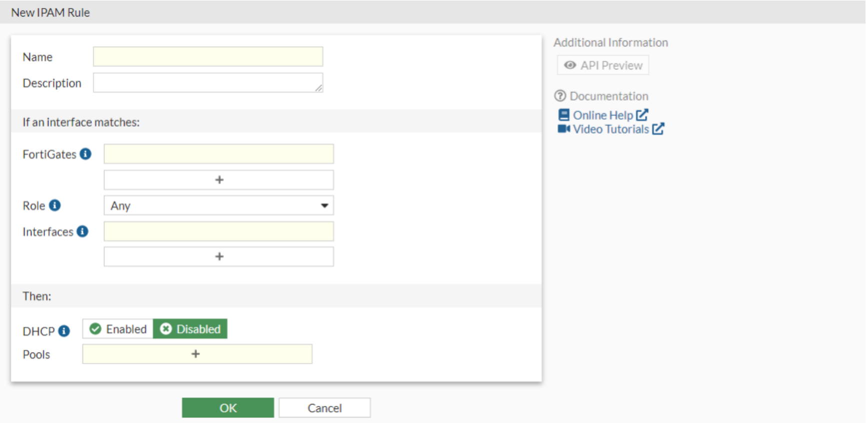
   c. Enter the IP address and netmask.
   d. Click *OK*.
3. Go to *Network* > *IPAM* > *IPAM Rules*. The *role-lan* and *Implicit Rule* rules have been configured by default.



Name	Device	Interface	Pools	Role	DHCP	Description
role-lan	*	*	192.168.0.0/255.255.0.0	LAN	✓ Enabled	
Implicit Rule	*	*	172.31.0.0/255.255.0.0 192.168.0.0/255.255.0.0	Any	✗ Disabled	

Implicit Rule cannot be modified or deleted. *role-lan* appears only after factory reset of the FortiGate and can be modified and deleted.

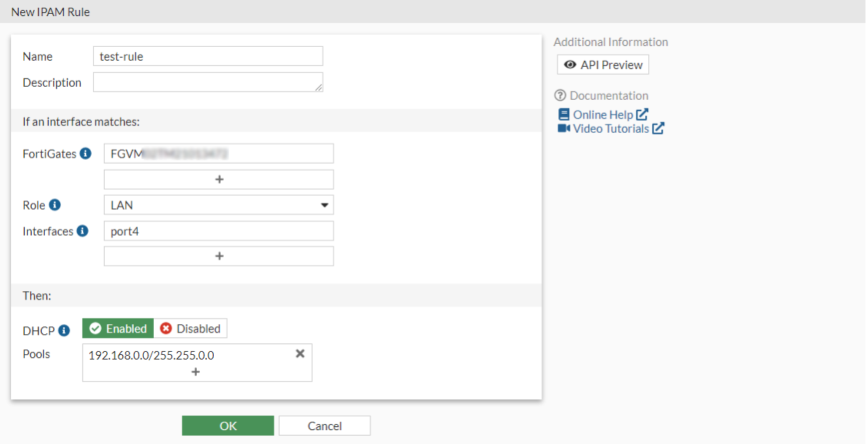
4. Click *Create new*. The *New IPAM Rule* page is displayed.



Role: Any

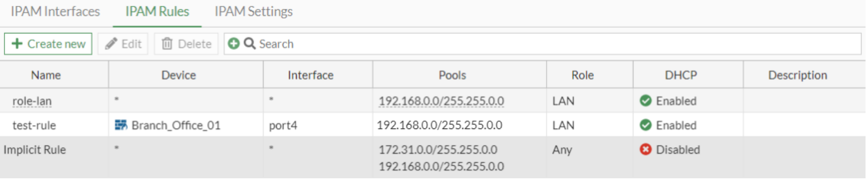
DHCP: ○ Enabled ● Disabled

5. Enter the rule details, as necessary.



Name	test-rule
Description	
FortiGates	FGVM[redacted]
Role	LAN
Interfaces	port4
DHCP	● Enabled ○ Disabled
Pools	192.168.0.0/255.255.0.0

6. Click *OK*. The rule will be configured and appear in the *IPAM Rules* tab.



Name	Device	Interface	Pools	Role	DHCP	Description
role-lan	*	*	192.168.0.0/255.255.0.0	LAN	✓ Enabled	
test-rule	Branch_Office_01	port4	192.168.0.0/255.255.0.0	LAN	✓ Enabled	
Implicit Rule	*	*	172.31.0.0/255.255.0.0 192.168.0.0/255.255.0.0	Any	✗ Disabled	

To configure IPAM rules in the CLI:

```
config system ipam
    set status enable
    config pools
        edit "default-pool"
            set subnet 172.31.0.0 255.255.0.0
        next
        edit "lan-pool"
```

```
            set subnet 192.168.0.0 255.255.0.0
        next
    end
    config rules
        edit "test-rule"
            set device "*"
            set interface "port4"
            set role lan
            set pool "lan-pool"
            set dhcp enable
        next
    end
end
```

Add VCI pattern matching as a condition for IP or DHCP option assignment - 7.2.1

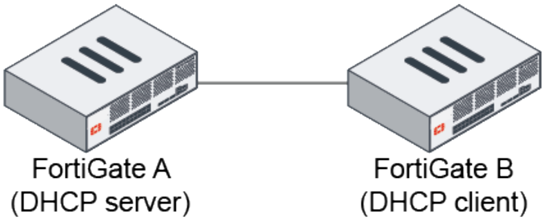
VCIs (vendor class identifiers) are supported in DHCP to allow VCI pattern matching as a condition for IP or DHCP option assignment. A single IP address, IP ranges of a pool, and dedicated DHCP options can be mapped to a specific VCI string.

```
config system dhcp server
    edit <id>
        config ip-range
            edit <id>
                set vci-match {enable | disable}
                set vci-string <string>
            next
        end
        config options
            edit <id>
                set vci-match {enable | disable}
                set vci-string <string>
            next
        end
    next
end
```

`vci-match {enable	disable}`	Enable/disable VCI matching. When enabled, only DHCP requests with a matching VCI are served with this range.
`vci-string <string>`	Set the VCI string. Enter one or more VCI strings in quotation marks separated by spaces.

Example

In this example, any DHCP client that matches the FortiGate-201F VCI will get their IP from the pool of 10.2.2.133-10.2.2.133, and options 42 (NTP servers) and 150 (TFTP server address). Any DHCP client that matches the FortiGate-101F VCI will get their IP from the default pool (10.2.2.132-10.2.2.132/10.2.2.134-10.2.2.254) and only get the 150 option.



To configure VCI pattern matching on FortiGate A:

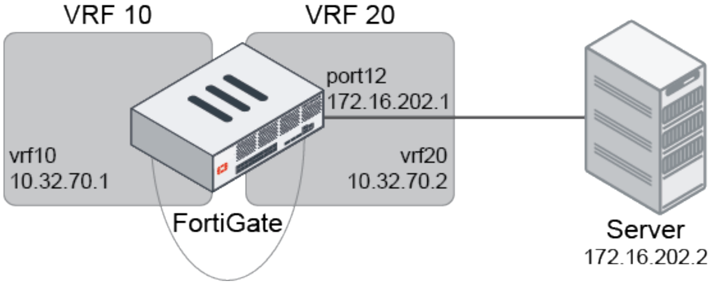
```
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.2.2.131
        set netmask 255.255.255.0
        set interface "port3"
        config ip-range
            edit 1
                set start-ip 10.2.2.132
                set end-ip 10.2.2.132
            next
            edit 2
                set start-ip 10.2.2.133
                set end-ip 10.2.2.133
                set vci-match enable
                set vci-string "FortiGate-201F"
            next
            edit 3
                set start-ip 10.2.2.134
                set end-ip 10.2.2.254
            next
        end
        config options
            edit 1
                set code 42
                set type ip
                set vci-match enable
                set vci-string "FortiGate-201F"
                set ip "8.8.8.8"
            next
            edit 2
                set code 150
                set type ip
                set ip "172.16.200.55"
            next
        end
        set vci-match enable
        set vci-string "FortiGate-201F" "FortiGate-101F"
    next
end
```

Support cross-VRF local-in and local-out traffic for local services - 7.2.1

When local-out traffic such as SD-WAN health checks, SNMP, syslog, and so on are initiated from an interface on one VRF and then pass through interfaces on another VRF, the reply traffic will be successfully forwarded back to the original VRF.

Example

In this example, there is an NPU VDOM link that is configured on the root VDOM. Two VLANs, vrf10 and vrf20, are created on either ends of the NPU VDOM link, each belonging to a different VRF.



When pinging from the vrf10 interface in VRF 10 to the destination server 172.16.202.2, since there is a single static route for VRF 10 with a gateway of vrf20/10.32.70.2, traffic is sent to the next hop and subsequently routed through port12 to the server.

As seen in the sniffer trace, the ICMP replies are received on port12 in VRF 20, then pass through vrf20, and are ultimately forwarded back to vrf10 in VRF 10. The traffic flow demonstrates that local-out traffic sourced from one VRF passing through another VRF can return back to the original VRF.

To configure cross-VRF local-out traffic for local services:

1. Configure the interfaces:

```
config system interface
    edit "vrf10"
        set vdom "root"
        set vrf 10
        set ip 10.32.70.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 35
        set interface "npu0_vlink0"
        set vlanid 22
    next
    edit "vrf20"
        set vdom "root"
        set vrf 20
        set ip 10.32.70.2 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 36
        set interface "npu0_vlink1"
        set vlanid 22
    next
    edit "port12"
        set vdom "root"
        set vrf 20
        set ip 172.16.202.1 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
fabric ftm speed-test
        set type physical
        set alias "TO_FGT_D_port22"
        set snmp-index 14
        config ipv6
            set ip6-address 2003:172:16:202::1/64
            set ip6-allowaccess ping
        end
    next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "vrf20"
        set dstintf "port12"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
    next
end
```

3. Configure the static route:

```
config router static
    edit 2
        set gateway 10.32.70.2
        set distance 3
        set device "vrf10"
    next
end
```

To test the configuration:

1. Execute a ping from the vrf10 interface in VRF 10 to the destination server (172.16.202.2):

```
# execute ping-options interface vrf10
# execute ping 172.16.202.2
PING 172.16.202.2 (172.16.202.2): 56 data bytes
64 bytes from 172.16.202.2: icmp_seq=0 ttl=254 time=0.1 ms
64 bytes from 172.16.202.2: icmp_seq=1 ttl=254 time=0.0 ms

--- 172.16.202.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
```

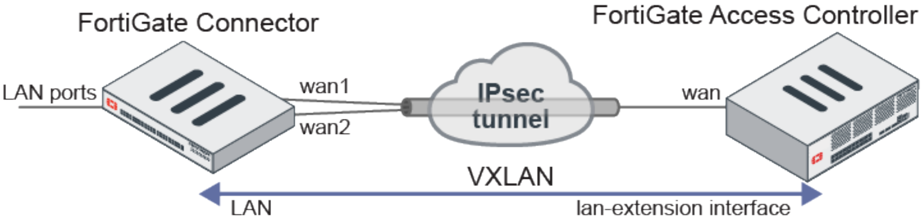
2. Run a sniffer trace on 172.16.202.2 for ICMP:

```
# diagnose sniffer packet any "host 172.16.202.2 and icmp" 4
interfaces=[any]
filters=[host 172.16.202.2 and icmp]
3.393920 vrf10 out 10.32.70.1 -> 172.16.202.2: icmp: echo request
3.393922 npu0_vlink0 out 10.32.70.1 -> 172.16.202.2: icmp: echo request
3.393927 vrf20 in 10.32.70.1 -> 172.16.202.2: icmp: echo request
3.393943 port12 out 10.32.70.1 -> 172.16.202.2: icmp: echo request
3.393977 port12 in 172.16.202.2 -> 10.32.70.1: icmp: echo reply
3.393987 vrf20 out 172.16.202.2 -> 10.32.70.1: icmp: echo reply
3.393988 npu0_vlink1 out 172.16.202.2 -> 10.32.70.1: icmp: echo reply
3.393993 vrf10 in 172.16.202.2 -> 10.32.70.1: icmp: echo reply
4.393941 vrf10 out 10.32.70.1 -> 172.16.202.2: icmp: echo request
4.393942 npu0_vlink0 out 10.32.70.1 -> 172.16.202.2: icmp: echo request
4.393948 vrf20 in 10.32.70.1 -> 172.16.202.2: icmp: echo request
4.393957 port12 out 10.32.70.1 -> 172.16.202.2: icmp: echo request
4.393980 port12 in 172.16.202.2 -> 10.32.70.1: icmp: echo reply
4.393987 vrf20 out 172.16.202.2 -> 10.32.70.1: icmp: echo reply
4.393987 npu0_vlink1 out 172.16.202.2 -> 10.32.70.1: icmp: echo reply
4.393994 vrf10 in 172.16.202.2 -> 10.32.70.1: icmp: echo reply
```

FortiGate as FortiGate LAN extension - 7.2.1

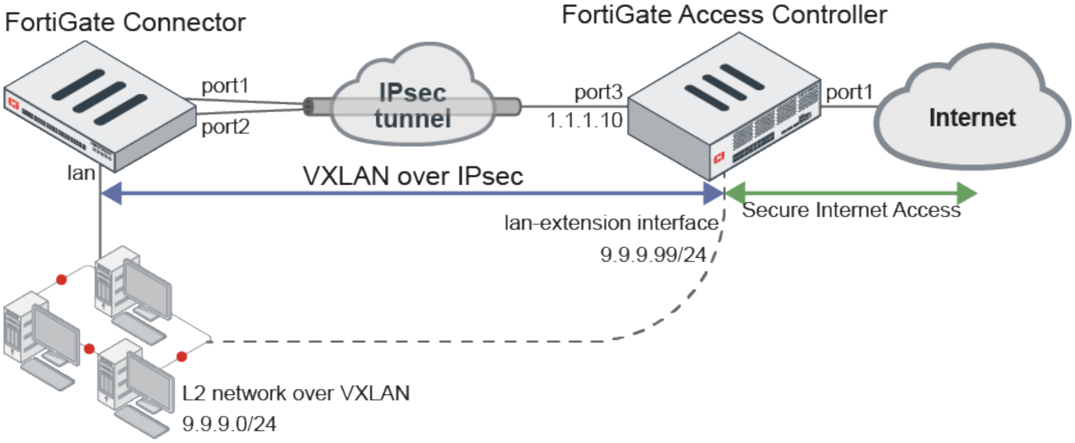
LAN extension mode allows a remote FortiGate to provide remote connectivity to a local FortiGate over a backhaul connection.

The remote FortiGate, called the FortiGate Connector, discovers the local FortiGate, called the FortiGate Controller, and forms one or more IPsec tunnels back to the FortiGate Controller. A VXLAN is established over the IPsec tunnels creating an L2 network between the FortiGate Controller and the network behind the FortiGate Connector.



In this example, the Controller provides secure internet access to the remote network behind the Connector. The Controller has two WAN connections: an inbound backhaul connection and an outbound internet connection. The Connector has two wired WAN/uplink ports that are connected to the internet.

After the Connector discovers the Controller and is authorized by the Controller, the Controller pushes a FortiGate LAN extension profile to the Connector. The Connector uses the profile configurations to form two IPsec tunnels back to the Controller. Additional VXLAN aggregate interfaces are automatically configured to create an L2 network between the Connector LAN port and a virtual LAN extension interface on the Controller. Clients behind the Connector can then connect to the internet through the Controller that is securing the internet connection.



To discover and authorize the FortiGate Controller:

1. On the FortiGate Controller:
   a. Enable security fabric connections on port3 to allow the Connector to connect over CAPWAP:

```
config system interface
    edit "port3"
        set vdom "root"
        set ip 1.1.1.10 255.255.255.0
        set allowaccess fabric ping
    next
end
```

2. On the FortiGate Connector:
   a. Set the VDOM type to LAN extension, making the VDOM act as a FortiExtender in LAN extension mode, and add the Controller IP address:

```
config vdom
    edit lan-ext
        config system settings
            set vdom-type lan-extension
            set lan-extension-controller-addr "1.1.1.10"
            set ike-port 4500
        end
    next
end
```

   b. Configure port1 and port2 to access the Controller:

```
config system interface
    edit "port1"
        set vdom "lan-ext"
        set ip 5.5.5.1 255.255.255.0
        set allowaccess ping fabric
        set type physical
        set lldp-reception enable
        set role wan
    next
    edit "port2"
        set vdom "lan-ext"
```

```
            set ip 6.6.6.1 255.255.255.0
            set allowaccess ping fabric
            set type physical
            set lldp-reception enable
            set role wan
        next
    end
```

3. On the FortiGate Controller:
   a. Extension controller configurations are automatically initialized:

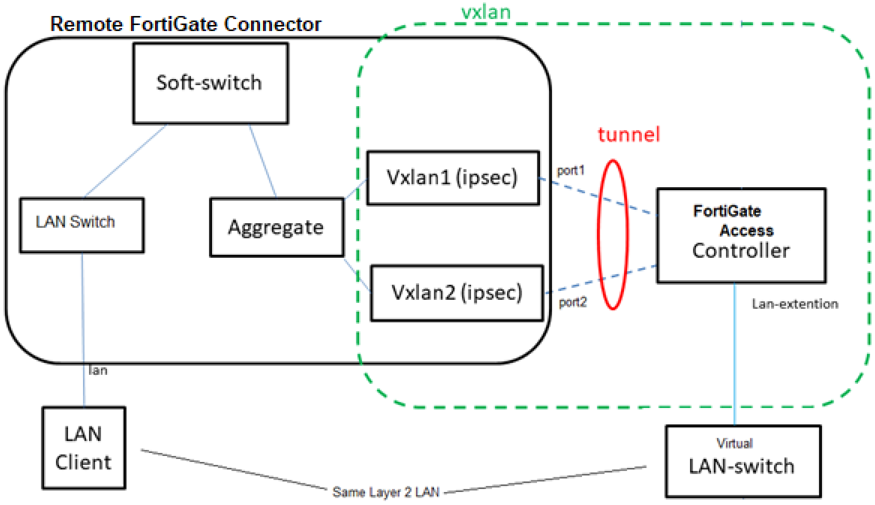
```
config extension-controller fortigate-profile
    edit "FGCONN-lanext-default"
        set id 0
        config lan-extension
            set ipsec-tunnel "fg-ipsec-XdSpij"
            set backhaul-interface "port3"
        end
    next
end
```

```
config extension-controller fortigate
    edit "FGT60E0000000001"
        set id "FG5H1E0000000001"
        set device-id 0
        set profile "FGCONN-lanext-default"
    next
end
```

   b. Enable FortiGate administration to authorize the Connector:

```
config extension-controller fortigate
    edit "FGT60E0000000001"
        set authorized enable
    next
end
```

4. After the FortiGate Connector has been authorized, the Controller pushes the IPsec tunnel configuration to the Connector, forcing it to establish the tunnel and form the VXLAN mechanism.



The VXLANs are built on the IPsec tunnels between the Connector and Controller. The VXLAN interfaces are aggregated for load balancing and redundancy. A softswitch combines the aggregate interface with the local LAN ports, allowing the LAN ports to be part of the VXLAN. This combines the local LAN ports with the virtual LAN extension interface on the FortiGate Controller.

a. The Connector receives the IPsec configurations from the Controller, and creates tunnels for each uplink:

```
config vpn ipsec phase1-interface
    edit "ul-port1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set localid "peerid-T4YLv2rp62SU6JhoCPIv02MzjLtS7P5HlxRER1Qpi6O9ZsAsbPSpvoiE"
        set dpd on-idle
        set comments "[FGCONN] Do NOT edit. Automatically generated by extension 
controller."
        set remote-gw 1.1.1.10
        set psksecret ******
    next
    edit "ul-port2"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set localid "peerid-T4YLv2rp62SU6JhoCPIv02MzjLtS7P5HlxRER1Qpi6O9ZsAsbPSpvoiE"
        set dpd on-idle
        set comments "[FGCONN] Do NOT edit. Automatically generated by extension 
controller."
        set remote-gw 1.1.1.10
        set psksecret ******
    next
end
```

b. VXLAN interfaces are formed over each tunnel:

```
config system vxlan
    edit "vx-port1"
        set interface "ul-port1"
        set vni 1
        set dstport 9999
        set remote-ip "10.252.0.1"
    next
    edit "vx-port2"
        set interface "ul-port2"
        set vni 1
        set dstport 9999
        set remote-ip "10.252.0.1"
    next
end
```

c. An aggregate interface is configured to load balance between the two VXLAN interfaces, using the source MAC and providing link redundancy:

```
config system interface
    edit "le-agg-link"
```

```
            set vdom "lan-ext"
            set type aggregate
            set member "vx-port1" "vx-port2"
            set snmp-index 35
            set lacp-mode static
            set algorithm Source-MAC
        next
    end
```

d. The softswitch bridges the aggregate interface and the local LAN to connect the LAN to the VXLAN bridged L2 network that goes to the FortiGate LAN extension interface:

```
config system switch-interface
    edit "le-switch"
        set vdom "lan-ext"
        set member "le-agg-link" "lan"
    next
end
```

e. After the IPsec tunnel is setup and the VXLAN is created over the tunnel, the LAN extension interface is automatically created on the Controller:

```
config system interface
    edit "FGT60E0000000001"
        set vdom "root"
        set ip 192.168.0.254 255.255.255.0
        set allowaccess ping ssh
        set type lan-extension
        set role lan
        set snmp-index 27
        set ip-managed-by-fortiipam enable
        set interface "fg-ipsec-XdSpij"
    next
end
```

To configure the LAN extension interface and firewall policy on the FortiGate Controller:

1. Set the IP address and netmask of the LAN extension interface:

```
config system interface
    edit "FGT60E0000000001"
        set ip 9.9.9.99 255.255.255.0
        set ip-managed-by-fortiipam enable
    next
end
```

Devices on the remote LAN network will use this as their gateway.

2. Optionally, enable DHCP on the interface to assign IP addresses to the remote devices:

```
config system dhcp server
    edit 3
        set dns-service default
        set default-gateway 9.9.9.99
        set netmask 255.255.255.0
        set interface "FGT60E0000000001"
        config ip-range
            edit 1
                set start-ip 9.9.9.100
                set end-ip 9.9.9.254
            next
        end
        set dhcp-settings-from-fortiipam enable
        config exclude-range
            edit 1
                set start-ip 9.9.9.254
                set end-ip 9.9.9.254
            next
        end
    next
end
```

3. Configure the firewall policy to allow traffic from the LAN extension interface to the WAN interface (port1):

```
config firewall policy
    edit "lan-ext"
        set name "qsaf"
        set srcintf "FGT60E0000000001"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

Optionally, security profiles and other settings can be configured.

The policy allows remote LAN clients to access the internet through the backhaul channel. Clients in the remote LAN behind the Connector receive an IP address over DHCP and access the internet securely through the Controller.

Allow VLAN sub-interfaces to be used in virtual wire pairs - 7.2.4

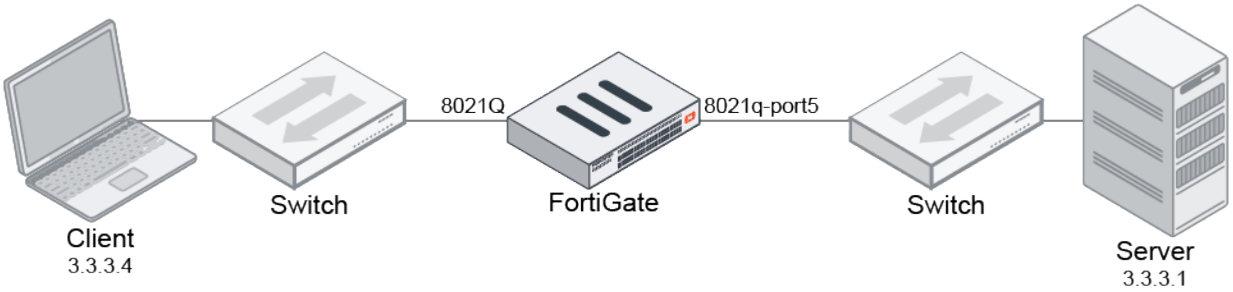
This information is also available in the FortiOS 7.2 Administration Guide:

- Using VLAN sub-interfaces in virtual wire pairs

VLAN sub-interfaces, such as regular 802.1Q and 802.1ad (QinQ), are allowed to be members of a virtual wire pair.

Example

In this example, the FortiGate has two VLAN interfaces. The first interface is a QinQ (802.1ad) interface over the physical interface port3. The second interface is a basic 802.1Q VLAN interface over physical interface port5. These two interfaces are grouped in a virtual wire pair so that bi-directional traffic is allowed. This example demonstrates ICMP from the client (3.3.3.4) sent to the server (3.3.3.1).



To configure VLAN sub-interfaces in a virtual wire pair:

1. Configure the QinQ interfaces:

```
config system interface
    edit "8021ad-port3"
        set vdom "vdom1"
        set vlan-protocol 8021ad
        set device-identification enable
        set role lan
        set snmp-index 31
        set interface "port3"
        set vlanid 3
    next
    edit "8021Q"
        set vdom "vdom1"
        set device-identification enable
        set role lan
        set snmp-index 32
        set interface "8021ad-port3"
        set vlanid 33
    next
end
```

2. Configure the 802.1Q interface:

```
config system interface
    edit "8021q-port5"
        set vdom "vdom1"
        set device-identification enable
        set role lan
        set snmp-index 33
        set interface "port5"
        set vlanid 5
    next
end
```

3. Configure the virtual wire pair:

```
config system virtual-wire-pair
    edit "VWP1"
        set member "8021Q" "8021q-port5"
    next
end
```

4. Configure the firewall policy:

```
config firewall policy
    edit 1
        set name "1"
        set srcintf "8021Q" "8021q-port5"
        set dstintf "8021Q" "8021q-port5"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

To verify that bi-directional traffic passes through the FortiGate:

```
# diagnose sys session filter policy  1
# diagnose sys session list

session info: proto=1 proto_state=00 duration=18 expire=42 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=may_dirty br npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=56->55/55->56 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 3.3.3.4:3072->3.3.3.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 3.3.3.1:3072->3.3.3.4:0(0.0.0.0:0)
src_mac=08:5b:0e:71:bf:c6  dst_mac=d4:76:a0:5d:b2:de
misc=0 policy_id=1 pol_uuid_idx=534 auth_info=0 chk_client_info=0 vd=3
serial=00005f6c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=187/156, ipid=156/187,
vlan=0x0005/0x0021
vlifid=156/187, vtag_in=0x0005/0x0021 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/5
total session 1
```

Add static route tag and BGP neighbor password - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- BGP neighbor password

The following routing extensions are added:

- Static route tags:

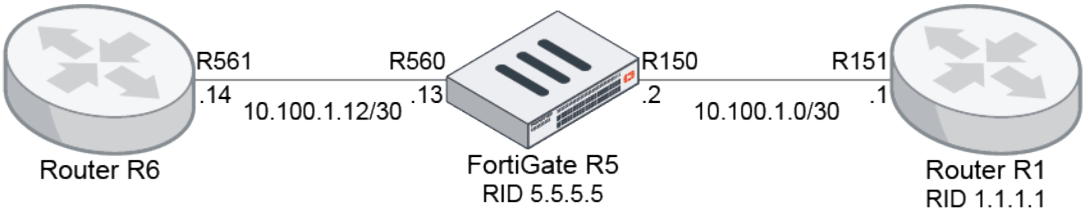
```
config router static
    edit <seq-num>
        set tag <id>
    next
end
```

- BGP neighbor passwords (used for the neighbor range):

```
config router bgp
    config neighbor-group
        edit <name>
            set password <password>
        next
    end
end
```

Example 1

In this example, a static route is configured with a route tag. The route tag is then matched in the route map, and used to set the route's metric and advertise to the BGP neighbor.



To configure the FortiGate:

1. Configure the static route:

```
config router static
    edit 1
        set dst 77.7.7.7 255.255.255.255
        set distance 2
        set device "R560"
        set tag 565
    next
end
```

2. Configure the route map:

```
config router route-map
    edit "map1"
        config rule
            edit 2
                set match-tag 565
                set set-metric 2301
            next
        end
    next
end
```

3. Configure the BGP neighbor:

```
config router bgp
    config neighbor
        edit "10.100.1.2"
```

```
            set route-map-out "map1"
        next
    end
end
```

On its neighbor side, router R1 receives the advertised route from the FortiGate router R5.

4. Verify the BGP routing table:

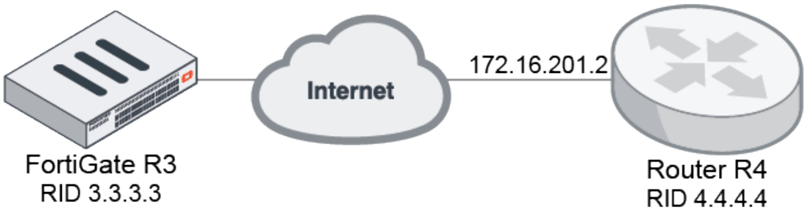
```
# get router info routing-table bgp
Routing table for VRF=0
B       77.7.7.7/32 [20/2301] via 10.100.1.1 (recursive is directly connected, R150),
03:18:53, [1/0]
```

5. Verify the network community:

```
# get router info bgp network 77.7.7.7/32
VRF 0 BGP routing table entry for 77.7.7.7/32
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   2.2.2.2 3.3.3.3 10.100.1.5 2000::2:2:2:2
  Original VRF 0
  20
    10.100.1.1 from 10.100.1.1 (5.5.5.5)
      Origin incomplete metric 2301, localpref 200, valid, external, best
      Last update: Wed Oct  5 16:48:28 2022
```

Example 2

In this example, a BGP group is configured, and it uses a password to establish the neighborhood.



To configure the BGP group:

1. Configure the R3 FortiGate settings:

```
config router bgp
    config neighbor-group
        edit "FGT"
            set soft-reconfiguration enable
            set remote-as 65050
            set local-as 65518
            set local-as-no-prepend enable
            set local-as-replace-as enable
            set route-map-in "del-comm"
            set keep-alive-timer 30
            set holdtime-timer 90
            set update-source "npu0_vlink0"
            set weight 1000
            set password ENC ********
        next
    end
    config neighbor-range
        edit 1
            set prefix 172.16.201.0 255.255.255.0
            set max-neighbor-num 10
            set neighbor-group "FGT"
        next
    end
end
```

2. Configure the R4 router settings:

```
config router bgp
    config neighbor
        edit "172.16.201.1"
            set soft-reconfiguration enable
            set remote-as 65518
            set password ********
        next
    end
end
```

DHCP enhancements - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Option 77
- Configuring the lease time for IP ranges

The following enhancements have been added for DHCP:

- Increase the number of supported IP ranges from 3 to 10
- Support DHCP option 77 for User Class information
- Support customizing the lease time

```
config system dhcp server
    edit <id>
        config ip-range
            edit <id>
                set uci-match {enable | disable}
                set uci-string <string>
                set lease-time <integer>
            next
        end
        config options
            edit <id>
                set uci-match {enable | disable}
                set uci-string <string>
            next
        end
    next
end
```

`uci-match {enable | disable}`	Enable/disable User Class information (UCI) matching for option 77. When enabled, only DHCP requests with a matching UCI are served with this range.
`uci-string <string>`	Enter one or more UCI strings in quotation marks separated by spaces.
`lease-time <integer>`	Set the lease time for a specific IP range, in seconds (300 - 864000, default = 0). If the default (0) is used for an IP range, it applies the global DHCP server lease time setting, which is set to 604800 by default.

Example 1: configuring IP ranges

In this example, ten IP ranges are configured on the DHCP server.

To configure ten IP ranges on a DHCP server:

```
config system dhcp server
    edit 1
        set netmask 255.255.255.0
        set interface "port1"
        config ip-range
            edit 1
                set start-ip 17.17.17.1
                set end-ip 17.17.17.1
            next
            edit 2
                set start-ip 17.17.17.2
                set end-ip 17.17.17.2
            next
            edit 3
                set start-ip 17.17.17.3
                set end-ip 17.17.17.3
            next
            edit 4
                set start-ip 17.17.17.4
                set end-ip 17.17.17.4
            next
            edit 5
                set start-ip 17.17.17.5
                set end-ip 17.17.17.5
            next
            edit 6
                set start-ip 17.17.17.6
                set end-ip 17.17.17.6
            next
            edit 7
                set start-ip 17.17.17.7
                set end-ip 17.17.17.7
            next
            edit 8
                set start-ip 17.17.17.8
                set end-ip 17.17.17.8
            next
            edit 9
                set start-ip 17.17.17.9
                set end-ip 17.17.17.9
            next
            edit 10
                set start-ip 17.17.17.10
                set end-ip 17.17.17.10
            next
        end
    next
end
```

Example 2: configuring User Class matching and lease time

In this example, when the User Class ID is matched, the FortiGate assigns the second IP range (17.17.17.2), and the lease time is set to 1111 seconds.

To configure the DHCP server:

```
config system dhcp server
    edit 1
        set netmask 255.255.255.0
        set interface "port1"
        config ip-range
            edit 1
                set start-ip 17.17.17.1
                set end-ip 17.17.17.1
                set vci-match enable
                set vci-string "Cisco AP c3800"
            next
            edit 2
                set start-ip 17.17.17.2
                set end-ip 17.17.17.2
                set uci-match enable
                set uci-string "FGT-3112"
                set lease-time 1111
            next
            edit 3
                set start-ip 17.17.17.3
                set end-ip 17.17.17.3
            next
        end
        set vci-match enable
        set vci-string "FGT"
    next
end
```

When a client request consists of a `FGT-3112` User Class ID, 17.17.17.2 is allocated to it.

To verify the configuration:

1. Run debugging for the DHCP server:

   ```
   # diagnose debug application dhcps -1
       [debug]locate_network prhtype(1) pihtype(1)
       [debug]find_lease(): leaving function WITHOUT a lease
       [note]DHCPDISCOVER from e8:1c:ba:de:aa:16 via port1(ethernet)
   ```

```
[debug]found a new lease of ip 17.17.17.2
[debug]added ip 17.17.17.2 mac e8:1c:ba:de:aa:16 in vd root
[debug]packet length 548
[debug]op = 1  htype = 1  hlen = 6  hops = 0
[debug]xid = 1b7c2c82  secs = 14336  flags = 80
[debug]ciaddr = 0.0.0.0
[debug]yiaddr = 0.0.0.0
[debug]siaddr = 0.0.0.0
[debug]giaddr = 0.0.0.0
[debug]chaddr = e8:1c:ba:de:aa:16
[debug]filename =
[debug]server_name =
[debug]  host-name = "500E-B-3112"
[debug]  dhcp-message-type = 1
[debug]  dhcp-parameter-request-list = 1,2,3,121,6,12,15,28,40,42,240,241
[debug]  dhcp-max-message-size = 1458
[debug]  dhcp-class-identifier = "FortiGate-500E"
[debug]  dhcp-client-identifier = 1:e8:1c:ba:de:aa:16
[debug]  user-class = "FGT-3112"
```

2. Verify the DHCP leases:

```
# execute dhcp lease-list
    port1
      IP             MAC-Address          Hostname        VCI               SSID
AP           SERVER-ID           Expiry
      17.17.17.2    e8:1c:ba:de:aa:16    500E-B-3112     FortiGate-500E
           1                  Fri Oct  7 10:11:33 2022
```

Example 3: configuring User Class matching for custom option assignments

In this example, when the User Class ID is matched, the FortiGate assigns option 66, the TFTP server name, and the value testdatatestdata.

To configure the DHCP server:

```
config system dhcp server
    edit 1
        set netmask 255.255.255.0
        set interface "port1"
        config ip-range
            edit 1
                set start-ip 17.17.17.1
                set end-ip 17.17.17.1
            next
        end
        config options
            edit 1
                set code 66
                set type string
                set uci-match enable
                set uci-string "FGT-3112"
                set value "testdatatestdata"
            next
        end
        set vci-match enable
        set vci-string "FGT"
    next
end
```

When a client request consists of a `FGT-3112` User Class ID, option 66 is included in the DHCP offer.

To verify the DHCP discover and offer through packet captures:

```
Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf6f26d22
    Seconds elapsed: 0
    Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Fortinet_de:aa:16 (e8:1c:ba:de:aa:16)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    ...
    Option: (77) User Class Information
        Length: 8
        User Class Data (Text): FGT-3112
    Option: (255) End
        Option End: 255
    Padding: 000000000000000000000000000000000000000000000000000000000000000000000…

Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf6f26d22
    Seconds elapsed: 0
    Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 17.17.17.1
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Fortinet_de:aa:16 (e8:1c:ba:de:aa:16)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Offer)
        Length: 1
        DHCP: Offer (2)
    Option: (54) DHCP Server Identifier (17.17.17.94)
        Length: 4
        DHCP Server Identifier: 17.17.17.94
    Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (604800s) 7 days
    Option: (1) Subnet Mask (255.255.255.0)
        Length: 4
        Subnet Mask: 255.255.255.0
    Option: (58) Renewal Time Value
        Length: 4
        Renewal Time Value: (302400s) 3 days, 12 hours
    Option: (59) Rebinding Time Value
        Length: 4
        Rebinding Time Value: (529200s) 6 days, 3 hours
    Option: (66) TFTP Server Name
        Length: 16
        TFTP Server Name: testdatatestdata
    Option: (224) Private
        Length: 17
        Value: 4647354830453538313939303330313000
    Option: (255) End
```

Improve DVLAN QinQ performance for NP7 platforms - 7.2.5

This information is also available in the FortiOS 7.2 Administration Guide:

- DVLAN QinQ on NP7 platforms

DVLAN 802.1ad and 802.1Q modes are supported on NP7 platforms, which provides better performance and packet processing.

For more information about this feature, see Improve DVLAN QinQ performance for NP7 platforms.

IPv6

This section includes information about IPv6 related new features:

- Configuring IPv4 over IPv6 DS-Lite service on page 222
- NAT46 and NAT64 for SIP ALG on page 227
- Send Netflow traffic to collector in IPv6 7.2.1 on page 234
- IPv6 feature parity with IPv4 static and policy routes 7.2.1 on page 235

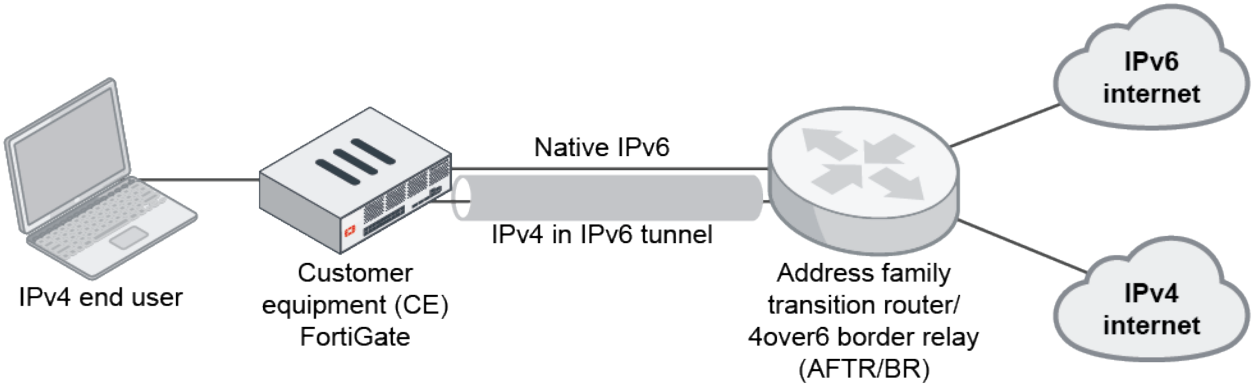
Configuring IPv4 over IPv6 DS-Lite service

IPv4 over IPv6 DS-Lite service can be configured on a virtual network enabler (VNE) tunnel. In addition, VNE tunnel fixed IP mode supports username and password authentication.

```
config system vne-tunnel
    set status enable
    set mode {map-e | fixed-ip | ds-lite}
    set ipv4-address <IPv4_address>
    set br <IPv6_address or FQDN>
    set http-username <string>
    set http-password <password>
end
```

`mode {map-e | fixed-ip | ds-lite}`	Set the VNE tunnel mode: • map-e: MAP-E • fixed-ip: fixed IP • ds-lite: DS-Lite
`ipv4-address <IPv4_address>`	Enter the tunnel IPv4 address and netmask. This setting is optional.
`br <IPv6_address or FQDN>`	Enter the IPv6 or FQDN of the border relay.
`http-username <string>`	Enter the HTTP authentication user name.
`http-password <password>`	Enter the HTTP authentication password.

DS-Lite allows applications using IPv4 to access the internet with IPv6. DS-Lite is supported by internet providers that do not have enough public IPv4 addresses for their customers, so DS-Lite is used for IPv6 internet connections. When a DS-Lite internet connections is used, the FortiGate encapsulates all data from IPv4 applications into IPv6 packets. The packets are then transmitted to the internet service provider using the IPv6 connection. Next, a dedicated server unpacks the IPv6 packets and forwards the IPv4 data to the actual destination on the internet.


IPv6 internet
Native IPv6
IPv4 in IPv6 tunnel
IPv4 end user
Customer equipment (CE) FortiGate
Address family transition router/ 4over6 border relay (AFTR/BR)
IPv4 internet

DS-Lite example

In this example, DS-Lite VNE tunnel mode is used between the FortiGate and the BR.

To configure a DS-Lite tunnel between the FortiGate and the BR:

1. Configure the IPv6 interface:

```
config system interface
    edit "wan1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping fgfm
        set type physical
        set role wan
        set snmp-index 1
        config ipv6
            set ip6-allowaccess ping
            set dhcp6-information-request enable
            set autoconf enable
            set unique-autoconf-addr enable
        end
    next
end
```

2. Configure the VNE tunnel:

```
config system vne-tunnel
    set status enable
    set interface "wan1"
    set ssl-certificate "Fortinet_Factory"
    set auto-asic-offload enable
    set ipv4-address 192.168.1.99 255.255.255.255
    set br "dgw.xxxxx.jp"
    set mode ds-lite
end
```

3. View the wan1 IPv6 configuration details:

```
config system interface
    edit "wan1"
        config ipv6
            get
                ip6-mode            : static
                nd-mode             : basic
                ip6-address         : 2001:f70:2880:xxxx:xxxx:xxxx:fe39:ccd2/64
                ip6-allowaccess     : ping
                icmp6-send-redirect : enable
                ra-send-mtu         : enable
                ip6-reachable-time  : 0
                ip6-retrans-time    : 0
                ip6-hop-limit       : 0
                dhcp6-information-request: enable
                cli-conn6-status    : 1
                vrrp-virtual-mac6   : disable
                vrip6_link_local    : ::
                ip6-dns-server-override: enable
                Acquired DNS1       : 2001:f70:2880:xxxx:xxxx:xxxx:fe40:9082
                Acquired DNS2       : ::
                ip6-extra-addr:
                ip6-send-adv        : disable
                autoconf            : enable
                prefix      : 2001:f70:2880:xxxx::/64
                preferred-life-time         : 942735360
                valid-life-time     : 1077411840
                unique-autoconf-addr: enable
                interface-identifier: ::
```

```
                dhcp6-relay-service : disable
            end
        next
    end
```

4. Verify the IPv6 address list:

```
# diagnose ipv6 address list
dev=5 devname=wan1 flag= scope=0 prefix=64 addr=2001:f70:2880:xxxx:xxxx:xxxx:fe39:ccd2
preferred=11525 valid=13325 cstamp=6520 tstamp=6892
dev=5 devname=wan1 flag=P scope=253 prefix=64 addr=fe80::xxxx:xxxx:fe39:ccd2
preferred=4294967295 valid=4294967295 cstamp=6373 tstamp=6373
dev=18 devname=root flag=P scope=254 prefix=128 addr=::1 preferred=4294967295
valid=4294967295 cstamp=3531 tstamp=3531
dev=25 devname=vsys_ha flag=P scope=254 prefix=128 addr=::1 preferred=4294967295
valid=4294967295 cstamp=5604 tstamp=5604
dev=27 devname=vsys_fgfm flag=P scope=254 prefix=128 addr=::1 preferred=4294967295
valid=4294967295 cstamp=6377 tstamp=6377
```

5. Test the tunnel connection by pinging the Google public DNS IPv6 address:

```
# execute ping6 2001:4860:4860::8888
PING 2001:4860:4860::8888(2001:4860:4860::8888) 56 data bytes
64 bytes from 2001:4860:4860::8888: icmp_seq=1 ttl=114 time=6.89 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=2 ttl=114 time=3.39 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=3 ttl=114 time=3.46 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=4 ttl=114 time=3.34 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=5 ttl=114 time=3.39 ms
--- 2001:4860:4860::8888 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss, time 4079ms
rtt min/avg/max/mdev = 3.340/4.097/6.895/1.400 ms
```

Fixed IP mode example

In this example, fixed IP VNE tunnel mode with HTTP authentication is used between the FortiGate and the BR.

To configure a fixed IP mode with HTTP authentication between the FortiGate and the BR:

1. Configure the IPv6 interface:

```
config system interface
    edit "wan1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping fgfm
        set type physical
        set role wan
        set snmp-index 1
        config ipv6
            set ip6-allowaccess ping
            set dhcp6-information-request enable
            set autoconf enable
        end
    next
end
```

2. Configure the VNE tunnel:

```
config system vne-tunnel
    set status enable
    set interface "wan1"
    set ipv4-address 120.51.xxx.xxx1 255.255.255.255
    set br "2001:f60:xxxx:xxxx::1"
    set update-url "https://ddnsweb1.ddns.xxxxxx.jp/cgi-bin/ddns_
api.cgi?d=xxxxxx.v4v6.xxxxx.jp&p=**********&a=[IP6]&u=xxxxxx.v4v6.xxxxx.jp"
    set mode fixed-ip
    set http-username "laptop-1"
    set http-password **********
end
```

3. Verify the wan1 IPv6 configuration details:

```
config system interface
    edit "wan1"
        config ipv6
            get
                ....
```

4. Verify the VNE daemon:

```
# diagnose test application vned 1
-----------------------------------------------------------------------------
vdom: root/0, is master, devname=wan1 link=0 tun=vne.root mode=fixed-ip ssl_
cert=Fortinet_Factory
end user ipv6 perfix: 2001:f70:2880:xxxx::/64
interface ipv6 addr: 2001:f70:2880:xxxx:xxxx:xxxx:fe39:ccd2
config ipv4 perfix: 120.51.xxx.xxx/255.255.255.255
config br: 2001:f60:xxxx:xxxx::1
HTTP username: laptop-1
update url: https://ddnsweb1.ddns.xxxxxx.jp/cgi-bin/ddns_
api.cgi?d=xxxxxx.v4v6.xxxxx.jp&p=**********&a=[IP6]&u=xxxxxx.v4v6.xxxxx.jp
host: ddnsweb1.ddns.xxxxxx.jp path: /cgi-bin/ddns_
api.cgi?d=xxxxxx.v4v6.xxxxx.jp&p=**********&a=[IP6]&u=xxxxxx.v4v6.xxxxx.jp port:443 ssl:
1
tunnel br: 2001:f60:xxxx:xxxx::1
tunnel ipv6 addr: 2001:f70:2880:xxxx:xxxx:xxxx:fe39:ccd2
tunnel ipv4 addr: 120.51.xxx.xxx1/255.255.255.255
update result: <H1>DDNS API</H1><HR><H2>* Query parameter check :
OK</H2>FQDN=xxxxxx.v4v6.xxxxx.jp<BR>Password=**********<BR>IPv6=2001:f70:2880:xxxx:xxxx:
xxxx:fe39:ccd2<BR>UID=xxxxxx.v4v6.xxxxx.jp<BR>Address=2001:f70:2880:xxxx:xxxx:xxxx:fe39:
ccd2<BR><H2>* routerinfo check : OK</H2><H2>* records check : OK</H2><H2>* routerinfo
update : OK</H2><H2>* records update : OK</H2><H2>* DDNS API update : Success [2022-01-
18 18:37:58 1642498678]</H2>
Fixed IP rule client: state=succeed retries=0 interval=0 expiry=0 reply_code=0
fqdn=2001:f60:xxxx:xxxx::1 num=1 cur=0 ttl=4294967295 expiry=0
2001:f60:xxxx:xxxx::1
Fixed IP DDNS client: state=succeed retries=0 interval=10 expiry=0 reply_code=200
```

```
fqdn=ddnsweb1.ddns.xxxxxx.jp num=1 cur=0 ttl=6 expiry=0
2001:f61:0:2a::18
```

5. Test the tunnel connection by pinging the Google public DNS IPv4 and IPv6 addresses:

```
# execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=119 time=3.7 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=3.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=3.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=3.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=3.5 ms
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.5/3.6/3.7 ms
```

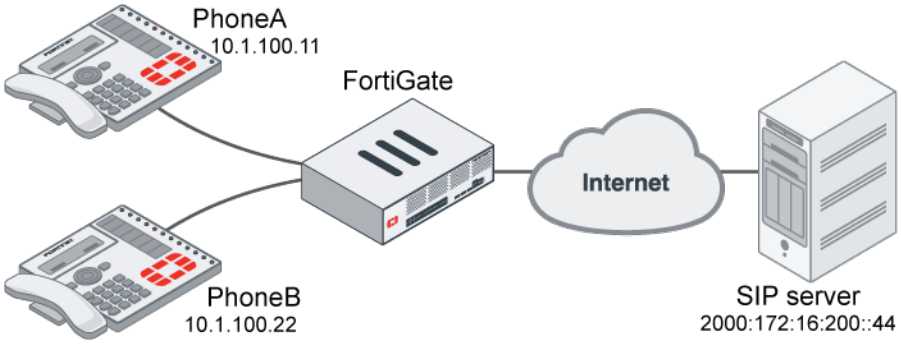
```
# execute ping6 2001:4860:4860::8888
PING 2001:4860:4860::8888(2001:4860:4860::8888) 56 data bytes
64 bytes from 2001:4860:4860::8888: icmp_seq=1 ttl=114 time=6.99 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=2 ttl=114 time=3.61 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=3 ttl=114 time=3.34 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=4 ttl=114 time=3.27 ms
64 bytes from 2001:4860:4860::8888: icmp_seq=5 ttl=114 time=3.75 ms
--- 2001:4860:4860::8888 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss, time 4039ms
rtt min/avg/max/mdev = 3.276/4.195/6.992/1.409 ms
```

NAT46 and NAT64 for SIP ALG

NAT46 and NAT64 are supported for SIP ALG. A mix of IPv4 and IPv6 networks can use SIP ALG, allowing for proper call handling.

NAT46 example

In this example, SIP phones on the internal network use IPv4, and the SIP server on an external network uses IPv6. NAT46 is used with SIP ALG to allow for seamless communication. A VoIP profile, `sip`, has already been created.



To configure the FortiGate:

1. Configure a firewall VIP with NAT46 enabled:

```
config firewall vip
    edit "vip46_server_asterisk"
        set extip 10.1.100.100
        set nat44 disable
        set nat46 enable
        set extintf "port1"
        set ipv6-mappedip 2000:172:16:200::44
    next
end
```

2. Configure an IPv6 pool:

```
config firewall ippool6
    edit "client_server_nat46"
        set startip 2000:172:16:200::200
        set endip 2000:172:16:200::207
        set nat46 enable
    next
end
```

3. Configure a firewall policy:

```
config firewall policy
    edit 1
        set name "policy46-1"
        set srcintf "port1"
        set dstintf "port9"
        set action accept
        set nat46 enable
        set srcaddr "all"
        set dstaddr "vip46_server_asterisk"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set voip-profile "sip"
        set logtraffic all
        set auto-asic-offload disable
        set ippool enable
        set poolname6 "client_server_nat46"
    next
end
```

To check the SIP calls and session lists when the phones are registering to the SIP server:

1. View the SIP proxy SIP calls:

```
# diagnose sys sip-proxy calls
sip calls
  vdom 3 (vdom1) vrf 0 call 7f64bf044b00
    call-id: 1513782757
    txn 7f64bf048f00 (REGISTER)
```

```
      cseq 2 dir 0 state 5 status 200 expiry 868 HA 0
      i_session: 7f64bf045e00  r_session: 7f64bf045e00
      register: present
      from: sip:2002@10.1.100.100
      to: sip:2002@10.1.100.100
      src: 10.1.100.22:5060
      dst: [2000:172:16:200::44]:5060

  vdom 3 (vdom1) vrf 0 call 7f64bf076700
    call-id: 1490871789
    txn 7f64bf047a00 (REGISTER)
      cseq 2 dir 0 state 5 status 200 expiry 861 HA 0
      i_session: 7f64bf045000  r_session: 7f64bf045000
      register: present
      from: sip:2001@10.1.100.100
      to: sip:2001@10.1.100.100
      src: 10.1.100.11:5060
      dst: [2000:172:16:200::44]:5060
```

2. View the IPv4 session list:

```
# diagnose sys session list

orgin->sink: org pre->post, reply pre->post dev=9->52/52->9 gwy=10.1.100.100/10.1.100.11
hook=pre dir=org act=noop 10.1.100.11:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.11:5060(0.0.0.0:0)
peer=2000:172:16:200::203:65476->2000:172:16:200::44:5060 naf=1
hook=pre dir=org act=noop 2000:172:16:200::203:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::203:65476(:::0)

orgin->sink: org pre->post, reply pre->post dev=9->52/52->9 gwy=10.1.100.100/10.1.100.22
hook=pre dir=org act=noop 10.1.100.22:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.22:5060(0.0.0.0:0)
peer=2000:172:16:200::200:65476->2000:172:16:200::44:5060 naf=1
hook=pre dir=org act=noop 2000:172:16:200::200:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::200:65476(:::0)
```

3. View the IPv4 expectation session list:

```
# diagnose sys session list expectation

orgin->sink: org pre->post, reply pre->post dev=9->0/52->0 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.100:0->10.1.100.11:5060(0.0.0.0:0)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
peer=:::0->:::0 naf=2

orgin->sink: org pre->post, reply pre->post dev=9->0/52->0 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.100:0->10.1.100.22:5060(0.0.0.0:0)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
peer=:::0->:::0 naf=2
```

4. View the IPv6 session list:

```
# diagnose sys session6 list

hook=pre dir=org act=noop 2000:172:16:200::203:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::203:65476(:::0)
peer=10.1.100.100:5060->10.1.100.11:5060 naf=2
```

```
hook=pre dir=org act=noop 10.1.100.11:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.11:5060(0.0.0.0:0)

hook=pre dir=org act=noop 2000:172:16:200::200:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::200:65476(:::0)
peer=10.1.100.100:5060->10.1.100.22:5060 naf=2
hook=pre dir=org act=noop 10.1.100.22:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.22:5060(0.0.0.0:0)
```

5. View the IPv6 expectation session list:

```
# diagnose sys session6 list expectation

orgin->sink: org pre->post, reply pre->post dev=17->0/52->0
hook=post dir=org act=noop 2000:172:16:200::44:0->2000:172:16:200::200:65476(:::0)
hook=pre dir=org act=noop :::0->:::0(:::0)
peer=10.1.100.100:0->10.1.100.22:5060 naf=1

orgin->sink: org pre->post, reply pre->post dev=17->0/52->0
hook=post dir=org act=noop 2000:172:16:200::44:0->2000:172:16:200::203:65476(:::0)
hook=pre dir=org act=noop :::0->:::0(:::0)
peer=10.1.100.100:0->10.1.100.11:5060 naf=1
```

To check the SIP calls and session lists when one phone is calling another phone:

1. View the SIP proxy SIP calls:

```
# diagnose sys sip-proxy calls

sip calls
  vdom 3 (vdom1) vrf 0 call 7f64bf057a00
    call-id: 217ac4733f80ac766c7e0f3a69d317a1@[2000:172:16:200::44]:5060
    txn 7f64bf038800 (INVITE)
      cseq 103 dir 1 state 11 status 200 expiry 252 HA 0
      i_session: 7f64bf036500  r_session: 7f64bf036500
      register: not-present
      contact[0]:  factory 7f64bf057900/4 expectation 7f64bf02cf00/2 session
7f64bf036500
      contact[1]:  factory 7f64bf057700/3 expectation 7f64bf02ca00/3 session
7f64bf036500
      from: sip:2001@[2000:172:16:200::44]
      to: sip:2002@[2000:172:16:200::200]:65476;o=10.1.100.22;line=28c59e086cac7c9
      src: [2000:172:16:200::44]:5060
      dst: 10.1.100.22:5060

  vdom 3 (vdom1) vrf 0 call 7f64bf057a00
    call-id: 217ac4733f80ac766c7e0f3a69d317a1@[2000:172:16:200::44]:5060
    txn 7f64bf038100 (INVITE)
      cseq 102 dir 1 state 11 status 200 expiry 252 HA 0
      i_session: 7f64bf036500  r_session: 7f64bf036500
      register: not-present
      contact[0]:  factory 7f64bf057900/4 expectation 7f64bf02cf00/2 session
7f64bf036500
      contact[1]:  factory 7f64bf057700/3 expectation 7f64bf02ca00/3 session
7f64bf036500
      from: sip:2001@[2000:172:16:200::44]
      to: sip:2002@[2000:172:16:200::200]:65476;o=10.1.100.22;line=28c59e086cac7c9
      src: [2000:172:16:200::44]:5060
      dst: 10.1.100.22:5060

  vdom 3 (vdom1) vrf 0 call 7f64bf057600
    call-id: 1876706695
    txn 7f64bf037300 (REGISTER)
      cseq 2 dir 0 state 5 status 200 expiry 856 HA 0
      i_session: 7f64bf036500  r_session: 7f64bf036500
      register: present
      from: sip:2002@10.1.100.100
      to: sip:2002@10.1.100.100
      src: 10.1.100.22:5060
      dst: [2000:172:16:200::44]:5060

  vdom 3 (vdom1) vrf 0 call 7f64bf057400
    call-id: 1372246794
    txn 7f64bf035e00 (REGISTER)
      cseq 2 dir 0 state 5 status 200 expiry 853 HA 0
      i_session: 7f64bf035000  r_session: 7f64bf035000
      register: present
      from: sip:2001@10.1.100.100
      to: sip:2001@10.1.100.100
      src: 10.1.100.11:5060
      dst: [2000:172:16:200::44]:5060

  vdom 3 (vdom1) vrf 0 call 7f64bf057800
    call-id: 16530657
    txn 7f64bf038f00 (INVITE)
      cseq 102 dir 1 state 11 status 200 expiry 252 HA 0
      i_session: 7f64bf035000  r_session: 7f64bf035000
      register: not-present
      contact[0]:  factory 7f64bf057900/4 expectation 7f64bf02cc80/2 session
7f64bf035000
      contact[1]:  factory 7f64bf057500/3 expectation 7f64bf02c780/3 session
7f64bf035000
      from: sip:2002@[2000:172:16:200::44]
      to: sip:2001@[2000:172:16:200::44]
      src: [2000:172:16:200::44]:5060
      dst: 10.1.100.11:5060

  vdom 3 (vdom1) vrf 0 call 7f64bf057800
    call-id: 16530657
    txn 7f64bf037a00 (INVITE)
      cseq 21 dir 0 state 11 status 200 expiry 252 HA 0
      i_session: 7f64bf035000  r_session: 7f64bf035000
      register: not-present
      contact[0]:  factory 7f64bf057500/3 expectation 7f64bf02c780/3 session
7f64bf035000
      contact[1]:  factory 7f64bf057900/4 expectation 7f64bf02cc80/2 session
7f64bf035000
      from: sip:2001@10.1.100.100
      to: sip:2002@10.1.100.100
      src: 10.1.100.11:5060
      dst: [2000:172:16:200::44]:5060
```

2. View the IPv6 session list:

```
# diagnose sys session6 list

hook=pre dir=org act=noop 2000:172:16:200::203:17078->2000:172:16:200::44:17090(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:17090->2000:172:16:200::203:17078(:::0)
peer=10.1.100.100:17090->10.1.100.11:17078 naf=2

hook=pre dir=org act=noop 2000:172:16:200::200:17078->2000:172:16:200::44:17082(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:17082->2000:172:16:200::200:17078(:::0)
peer=10.1.100.100:17082->10.1.100.22:17078 naf=2
hook=pre dir=org act=noop 10.1.100.22:17078->10.1.100.100:17082(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:17082->10.1.100.22:17078(0.0.0.0:0)

hook=pre dir=org act=noop 2000:172:16:200::203:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::203:65476(:::0)
peer=10.1.100.100:5060->10.1.100.11:5060 naf=2
hook=pre dir=org act=noop 10.1.100.11:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.11:5060(0.0.0.0:0)

hook=pre dir=org act=noop 2000:172:16:200::200:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::200:65476(:::0)
peer=10.1.100.100:5060->10.1.100.22:5060 naf=2
hook=pre dir=org act=noop 10.1.100.22:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.22:5060(0.0.0.0:0)
```

3. View the IPv6 expectation session list:

```
# diagnose sys session6 list expectation

hook=post dir=org act=noop 2000:172:16:200::44:0->2000:172:16:200::203:65476(:::0)
hook=pre dir=org act=noop :::0->:::0(:::0)
peer=10.1.100.100:0->10.1.100.11:5060 naf=1
```

4. View the IPv4 session list:

```
# diagnose sys session list

orgin->sink: org pre->post, reply pre->post dev=9->52/52->9 gwy=10.1.100.100/10.1.100.22
hook=pre dir=org act=noop 10.1.100.22:17078->10.1.100.100:17082(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:17082->10.1.100.22:17078(0.0.0.0:0)
peer=2000:172:16:200::200:17078->2000:172:16:200::44:17082 naf=1
hook=pre dir=org act=noop 2000:172:16:200::200:17078->2000:172:16:200::44:17082(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:17082->2000:172:16:200::200:17078(:::0)

orgin->sink: org pre->post, reply pre->post dev=9->52/52->9 gwy=10.1.100.100/10.1.100.22
hook=pre dir=org act=noop 10.1.100.22:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.22:5060(0.0.0.0:0)
peer=2000:172:16:200::200:65476->2000:172:16:200::44:5060 naf=1
hook=pre dir=org act=noop 2000:172:16:200::200:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::200:65476(:::0)

orgin->sink: org pre->post, reply pre->post dev=9->52/52->9 gwy=10.1.100.100/10.1.100.11
hook=pre dir=org act=noop 10.1.100.11:5060->10.1.100.100:5060(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.100:5060->10.1.100.11:5060(0.0.0.0:0)
peer=2000:172:16:200::203:65476->2000:172:16:200::44:5060 naf=1
hook=pre dir=org act=noop 2000:172:16:200::203:65476->2000:172:16:200::44:5060(:::0)
hook=post dir=reply act=noop 2000:172:16:200::44:5060->2000:172:16:200::203:65476(:::0)
```

5. View the IPv4 expectation session list:

```
# diagnose sys session list expectation

orgin->sink: org pre->post, reply pre->post dev=9->0/52->0 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.100:0->10.1.100.11:5060(0.0.0.0:0)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
peer=:::0->:::0 naf=2

orgin->sink: org pre->post, reply pre->post dev=9->0/52->0 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.100:0->10.1.100.22:17078(0.0.0.0:0)
peer=:::0->:::0 naf=2

orgin->sink: org pre->post, reply pre->post dev=9->0/52->0 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.100:0->10.1.100.22:17079(0.0.0.0:0)
peer=:::0->:::0 naf=2

orgin->sink: org pre->post, reply pre->post dev=9->0/52->0 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=noop 10.1.100.22:0->10.1.100.100:17083(0.0.0.0:0)
peer=2000:172:16:200::200:17085->2000:172:16:200::44:17903 naf=1
```

Log messages

When the phones are registering to the SIP server:

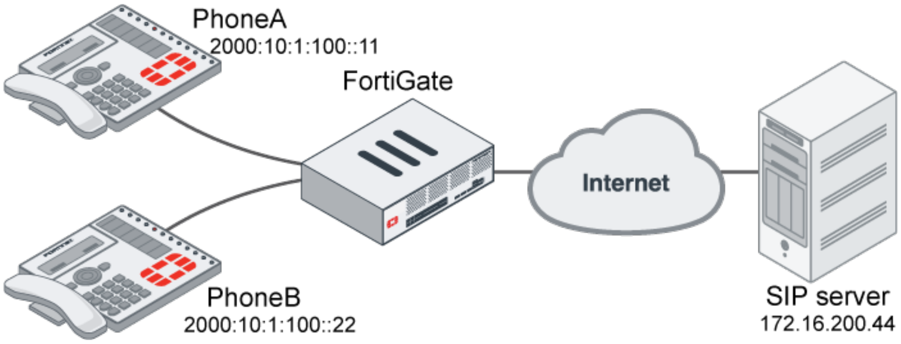
```
date=2022-02-17 time=16:44:47 eventtime=1645145087805236720 tz="-0800" logid="0814044032"
type="utm" subtype="voip" eventtype="voip" level="information" vd="vdom1" session_id=924
epoch=0 event_id=9 srcip=10.1.100.11 src_port=5060 dstip=2000:172:16:200::44 dst_port=5060
proto=17 src_int="port1" dst_int="port9" policy_id=1 profile="sip" voip_proto="sip"
kind="register" action="permit" status="authentication-required" duration=0 dir="session_
origin" call_id="1868762230" from="sip:2001@10.1.100.100" to="sip:2001@10.1.100.100"
```

When one phone is calling another phone:

```
date=2022-02-17 time=16:44:53 eventtime=1645145093351288241 tz="-0800" logid="0814044032"
type="utm" subtype="voip" eventtype="voip" level="information" vd="vdom1" session_id=924
epoch=0 event_id=11 srcip=10.1.100.11 src_port=5060 dstip=2000:172:16:200::44 dst_port=5060
proto=17 src_int="port1" dst_int="port9" policy_id=1 profile="sip" voip_proto="sip"
kind="call" action="permit" status="start" duration=0 dir="session_origin" call_
id="133636365" from="sip:2001@10.1.100.100" to="sip:2002@10.1.100.100"
```

NAT64 example

In this example, SIP phones on the internal network use IPv6, and the SIP server on an external network uses IPv4. NAT64 is used with SIP ALG to allow for seamless communication. A VoIP profile, `sip`, has already been created.



To configure the FortiGate:

1. Configure a firewall VIP with NAT64 enabled:

```
config firewall vip
    edit "vip64-1-asterisk"
        set extip 2000:10:1:100::100
        set nat66 disable
        set nat64 enable
        set ipv4-mappedip 172.16.200.44
    next
end
```

2. Configure an IP pool:

```
config firewall ippool
    edit "client_server_nat46"
        set startip 172.16.200.2
        set endip 172.16.200.3
        set nat64 enable
    next
end
```

3. Configure a firewall policy:

```
config firewall policy
    edit 1
        set name "policy64-1"
        set srcintf "port1"
        set dstintf "port9"
        set action accept
        set nat64 enable
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "vip64-1-asterisk"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set voip-profile "sip"
        set logtraffic all
        set auto-asic-offload disable
        set ippool enable
        set poolname "client_server_nat64"
    next
end
```

Send Netflow traffic to collector in IPv6 - 7.2.1

Netflow traffic can be sent from the FortiGate to a collector using IPv6. Both the source and collector IP addresses can be IPv6 addresses.

When VDOMs are enabled, the source and collector IPv6 addresses can be configured globally or in individual VDOMs.

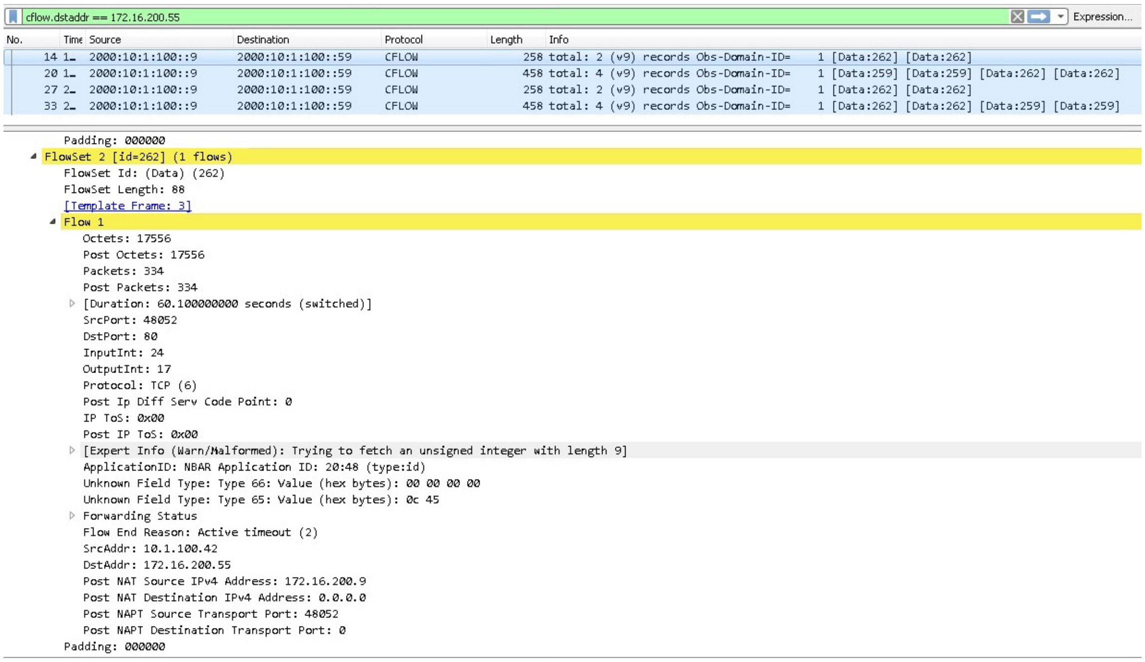
To set the Netflow collector and source IP addresses to IPv6 addresses:

```
config system netflow
    set collector-ip "2000:10:1:100::59"
    set source-ip "2000:10:1:100::9"
    set active-flow-timeout 60
    set template-tx-timeout 60
end
```

To confirm that the collector IP address is set to an IPv6 address on the FortiGate:

```
# diagnose test application sflowd 3
===== Netflow Vdom Configuration =====
Global collector:2000:10:1:100::59:[2055] source ip: 2000:10:1:100::9 active-timeout
(seconds):60 inactive-timeout(seconds):15
____ vdom: root, index=0, is master, collector: disabled (use global config) (mgmt vdom)
   |_ coll_ip:[2000:10:1:100::59]:2055,src_ip:2000:10:1:100::9
   |_ seq_num:229 pkts/time to next template: 16/27
   |_ exported: Bytes:2477154, Packets:5618, Sessions:58 Flows:66
   |_ active_intf: 1
   |____ interface:port17 sample_direction:both device_index:17 snmp_index:17
```

To confirm that the collector IP address is an IPv6 address on the collector:



```
No.    Time Source             Destination         Protocol   Length Info
    14 1…   2000:10:1:100::9   2000:10:1:100::59   CFLOW         258 total: 2 (v9) records Obs-Domain-ID=    1 [Data:262] [Data:262]
    20 1…   2000:10:1:100::9   2000:10:1:100::59   CFLOW         458 total: 4 (v9) records Obs-Domain-ID=    1 [Data:259] [Data:259] [Data:262] [Data:262]
    27 2…   2000:10:1:100::9   2000:10:1:100::59   CFLOW         258 total: 2 (v9) records Obs-Domain-ID=    1 [Data:262] [Data:262]
    33 2…   2000:10:1:100::9   2000:10:1:100::59   CFLOW         458 total: 4 (v9) records Obs-Domain-ID=    1 [Data:262] [Data:262] [Data:259] [Data:259]

    Padding: 000000
  ◢ FlowSet 2 [id=262] (1 flows)
      FlowSet Id: (Data) (262)
      FlowSet Length: 88
      [Template Frame: 3]
    ◢ Flow 1
        Octets: 17556
        Post Octets: 17556
        Packets: 334
        Post Packets: 334
      ▷ [Duration: 60.100000000 seconds (switched)]
        SrcPort: 48052
        DstPort: 80
        InputInt: 24
        OutputInt: 17
        Protocol: TCP (6)
        Post Ip Diff Serv Code Point: 0
        IP ToS: 0x00
        Post IP ToS: 0x00
      ▷ [Expert Info (Warn/Malformed): Trying to fetch an unsigned integer with length 9]
        ApplicationID: NBAR Application ID: 20:48 (type:id)
        Unknown Field Type: Type 66: Value (hex bytes): 00 00 00 00
        Unknown Field Type: Type 65: Value (hex bytes): 0c 45
      ▷ Forwarding Status
        Flow End Reason: Active timeout (2)
        SrcAddr: 10.1.100.42
        DstAddr: 172.16.200.55
        Post NAT Source IPv4 Address: 172.16.200.9
        Post NAT Destination IPv4 Address: 0.0.0.0
        Post NAPT Source Transport Port: 48052
        Post NAPT Destination Transport Port: 0
    Padding: 000000
```

IPv6 feature parity with IPv4 static and policy routes - 7.2.1

This enhancement introduces options in IPv6 static and policy routes for parity with IPv4 static and policy routes.

```
config router static6
    edit <seq-num>
        set dstaddr <string>
        set weight <integer>
    next
end
```

`dstaddr <string>`	Enter the name of the firewall address or address group.
`weight <integer>`	Set the administrative weight (0 - 255, default = 0).

```
config router policy6
    edit <seq-num>
        set srcaddr <string>
        set dstaddr <string>
        set action {deny | permit}
        set input-device-negate {enable | disable}
        set src-negate {enable | disable}
        set dst-negate {enable | disable}
    next
end
```

`srcaddr <string>`	Enter the source address name.
`dstaddr <string>`	Enter the destination address name.
`action {deny | permit}`	Set the action of the policy route: • `deny`: do not search the policy route table. • `permit`: use this policy route for forwarding.
`input-device-negate {enable | disable}`	Enable/disable negating input device match.
`src-negate {enable | disable}`	Enable/disable negating source address match.
`dst-negate {enable | disable}`	Enable/disable negating destination address match.

To configure an IPv6 static route:

```
config router static6
    edit 10
        set gateway 2000:172:16:200::2
        set device "port1"
        set weight 50
        set dstaddr "2021"
    next
end
```

To verify the IPv6 static routing table:

```
# get router info6 routing-table static
Routing table for VRF=0
S       2000:2:2:2::/64 [10/0] via 2000:172:16:200::2, port1, 00:00:03, [1024/50]
S       2001:2:2:2::/64 [10/0] via 2000:172:16:200::2, port1, 00:00:03, [1024/50]
```

To configure an IPv6 policy route:

```
config router policy6
    edit 1
        set input-device "port2"
        set input-device-negate enable
        set srcaddr "222" "2000" "20fqdn" "2021"
        set src-negate enable
        set dst "3333::33/128"
        set gateway 2000:172:16:203::2
        set output-device "agg1"
    next
end
```

To verify the IPv6 policy routing table:

```
# diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xfc 0xfc flags=0x4 deny tos=0x00 tos_mask=0x00 protocol=6 sport=2-22 iif=72
(ipip_A_D) 30(l2t.root) dport=3-33 path(0)
source(1): 10.1.1.1-10.1.1.11
destination(2): 10.100.22.0-10.100.22.255 10.100.2.22-10.100.2.22
source wildcard(2): 22.2.2.2/255.255.255.255 22.2.2.22/255.255.255.255
destination wildcard(2): 33.3.3.3/255.255.255.255 33.3.3.33/255.255.255.255
internet service(3): Act-on-DNS(5242883,0,0,0,0) Act-on-FTP(5242887,0,0,0,0) Act-on-ICMP
(5242882,0,0,0,0)
hit_count=3 last_used=2022-06-28 11:05:25
```

Web proxy

This section includes information about web proxy related new features:

- HTTPS download of PAC files for explicit proxy 7.2.1 on page 237
- Support CORS protocol in explicit web proxy when using session-based, cookie-enabled, and captive portal-enabled SAML authentication 7.2.1 on page 239

HTTPS download of PAC files for explicit proxy - 7.2.1

Proxy auto-config (PAC) files can be downloaded for an explicit proxy through the FortiGate's captive portal using HTTPS to ensure a secure download.

Example

In this example, a Windows PC has an HTTPS URL configured in its proxy settings to download a PAC file from a FortiGate by using a download link, https://cp.myqalab.local:7831/proxy.pac, through a captive portal. Once the PAC file is securely downloaded using HTTPS, browsers installed on the PC can use the proxy in the PAC file to visit a website.

The global web proxy settings must be configured to use a customized SSL certificate because the default Fortinet_Factory certificate will not be accepted by Windows due to security restrictions. The customized SSL certificate is used as the HTTPS server's certificate on the FortiGate. All CA certificates in the server certificate must be installed and trusted on the Windows PC.

To download a PAC file using HTTPS:

1. Configure the explicit web proxy to get a PAC file through HTTPS:

```
config web-proxy explicit
    set pac-file-server-status enable
    unset pac-file-server-port
    set pac-file-name "proxy.pac"
    set pac-file-data "function FindProxyForURL(url, host) {
   // testtest
   return \"PROXY 10.1.100.1:8080\";
}
"
    set pac-file-through-https enable
end
```

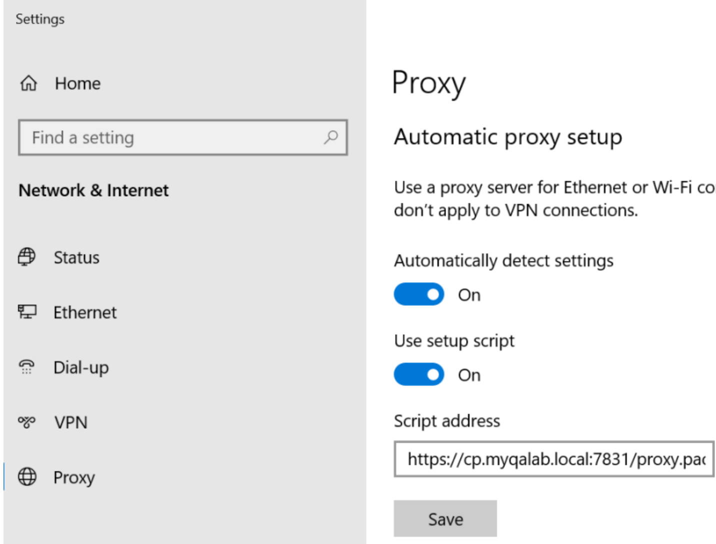
2. Configure the captive portal to be used as an HTTPS server to provide the service to download the PAC file:

```
config authentication setting
    set captive-portal-type ip
    set captive-portal-ip 10.1.100.1
    set captive-portal-ssl-port 7831
end
```

3. Configure the global web proxy settings to use a customized SSL certificate:

```
config web-proxy global
    set ssl-cert "server_cert"
end
```

4. On the Windows PC, go to *Settings* > *Network & Internet* > *Proxy*.



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings

On

Use setup script

On

Script address

https://cp.myqalab.local:7831/proxy.pac

5. In the *Automatic proxy setup* section, click *Save* to trigger the PAC file download from the HTTPS URL.

Support CORS protocol in explicit web proxy when using session-based, cookie-enabled, and captive portal-enabled SAML authentication - 7.2.1

The FortiGate explicit web proxy supports the Cross-Origin Resource Sharing (CORS) protocol, which allows the FortiGate to process a CORS preflight request and an actual CORS request properly, in addition to a simple CORS request when using session-based, cookie-enabled, and captive portal-enabled SAML authentication. This allows a FortiGate explicit web proxy user with this specific configuration to properly view a web page requiring CORS with domains embedded in it other than its own domain.

For more information about this feature, see Support CORS protocol in explicit web proxy when using session-based, cookie-enabled, and captive portal-enabled SAML authentication.

System

This section includes information about system related new features:

- General on page 240
- High availability on page 269
- FortiGuard on page 307
- Security on page 317

General

This section includes information about general system related new features:

- Improve admin-restrict-local handling of multiple authentication servers on page 240
- Access control for SNMP based on the MIB-view and VDOM on page 242
- Backing up and restoring configuration files in YAML format on page 244
- Remove split-task VDOMs and add a new administrative VDOM type on page 245
- Introduce maturity firmware levels on page 247
- Restrict SSH and telnet jump host capabilities 7.2.1 on page 250
- Enable automatic firmware updates 7.2.1 on page 250
- Deregistration from the GUI 7.2.1 on page 252
- Add government end user option for FortiCare registration 7.2.1 on page 254
- Support backing up configurations with password masking 7.2.1 on page 255
- New default certificate for HTTPS administrative access 7.2.1 on page 257
- Remove maintainer account 7.2.4 on page 261
- Allow the FortiGate to override FortiCloud SSO administrator user permissions 7.2.4 on page 262
- Display warnings for supported Fabric devices passing their hardware EOS date 7.2.5 on page 268
- Support checking for firmware updates daily when auto firmware upgrade is enabled 7.2.6 on page 268
- Enable automatic firmware upgrades by default on entry-level FortiGates 7.2.6 on page 268
- Command to compute file hashes 7.2.6 on page 269

Improve admin-restrict-local handling of multiple authentication servers

Under `config system global`, when the `admin-restrict-local` setting is enabled, local administrators cannot be used until all remote authentication servers are down. The FortiGate now only checks if all remote authentication servers applied in `system admin` are down, instead of all remote servers configured on the FortiGate, before allowing local administrators to log in.

To configure remote authentication groups and apply remote authentication to system administrative users:

1. Configure multiple remote authentication servers (this example uses one RADIUS and one LDAP server):

```
config user radius
    edit "1006290-radius"
        set server "10.1.100.55"
        set secret **********
    next
end
```

```
config user ldap
    edit "1006290-ldap"
        set server "172.16.200.55"
        set cnid "cn"
        set dn "dc=qa,dc=fortinet,dc=com"
        set type regular
        set username "cn=admin,dc=qa,dc=fortinet,dc=com"
        set password **********
    next
end
```

2. Configure the user groups:

```
config user group
    edit "radius-group"
        set member "1006290-radius"
    next
    edit "ldap-group"
        set member "1006290-ldap"
    next
end
```

3. Configure an administrative user with the RADIUS server:

```
config system admin
    edit "1006290-radius-admin"
        set remote-auth enable
        set accprofile "prof_admin"
        set vdom "vdom1"
        set wildcard enable
        set remote-group "radius-group"
    next
end
```

To restrict local administrator access until the remote authentication server is down:

1. Enable `admin-restrict-local`:

```
config system global
    set admin-restrict-local enable
end
```

2. Get the remote and local administrators to log in to the FortiGate with SSH. The remote administrator is able to log in, but the local administrator is unable to log in:

- Remote:

  ```
  root@PC1:~# ssh mschap@10.1.100.1
  mschap@10.1.100.1's password:
  FortiGate-101F $ get system status
  Version: FortiGate-101F v7.2.0, ...
  ```

- Local:

  ```
  root@PC1:~# ssh admin@10.1.100.1
  admin@10.1.100.1's password:
  Permission denied, please try again.
  ```

3. Shut down the RADIUS server and keep the LDAP server running. The local administrator is now able to log in to the FortiGate:

   ```
   root@PC1:~# ssh admin@10.1.100.1
   admin@10.1.100.1's password:
   FortiGate-101F # get system status
   Version: FortiGate-101F v7.2.0, ...
   ```

Access control for SNMP based on the MIB-view and VDOM

Administrators can provide access control to SNMP users and communities based on restricting a MIB-view to specific OID subtrees. They can also define access based on the VDOM. This allows multi-tenant FortiGate deployments to provide restricted access per VDOM.

- MIB-view access control allows the SNMP clients to query specific OIDs that are filtered by the MIB-view settings.
- VDOM access control allows the SNMP clients to query data from specific VDOMs that are filtered by the VDOM settings.

When access control is enabled, the users can only access the information that is allowed by the access control, and all other information is inaccessible. Administrators have granular control, and can easily restrict specific information based on access control.

To configure MIB-views:

```
config system snmp mib-view
    edit <MIB view name>
        set include <OIDs>
        set exclude <OIDs>
    next
end
```

set include <OIDs>>	The OID subtrees to be included in the view. A maximum of 16 subtrees can be added.
set exclude <OIDs>	The OID subtrees to be excluded in the view. A maximum of 64 subtrees can be added.

To configure access control based on MIB-views and VDOMs for SNMP users and communities:

```
config system snmp user
    edit <user>
        set mib-view <view>
```

```
        set vdoms <vdoms>
    next
end
```

```
config system snmp community
    edit <community>
        set mib-view <view>
        set vdoms <vdoms>
    next
end
```

set mib-view <view>	The SNMP access control MIB view.
set vdoms <vdoms>	SNMP access control VDOMs.

Example

In this example, two MIB-views are created and, with VDOMs, used to control access for SNMP users and communities.

To configure access control for SNMP users and communities:

1. Configure two MIB-views:

   ```
   config system snmp mib-view
       edit "view1"
           set include "1.3.6.1.2"
       next
       edit "view2"
           set include "1.3.6.1.2.1"
           set exclude "1.3.6.1.2.1.2.1" "1.3.6.1.2.1.4.31" "1.3.6.1.2.1.1.9.1"
       next
   end
   ```

2. Add MIB-view and VDOM restrictions to SNMP users:

   ```
   config system snmp user
       edit "v3user"
           set mib-view "view1"
       next
       edit "v3user1"
           set vdom "vdom1"
       next
       edit "v3user2"
           set mib-view "view1"
           set vdoms "root" "vdom1"
       next
   end
   ```

3. Add MIB-view and VDOM restrictions to SNMP communities:

   ```
   config system snmp community
       edit 1
           set name "REGR-SYS"
           set vdoms "vdom1"
       next
       edit 2
   ```

```
            set name "REGR-SYS1"
            set mib-view "view2"
        next
        edit 3
           set name "REGR-SYS2"
           set mib-view "view1"
           set vdoms "root" "vdom1"
        next
    end
```

Backing up and restoring configuration files in YAML format

Configuration files can be backed up or restored on an FTP or TFTP server in YAML format (in addition to FortiOS format). Files formatted in YAML are easy to read and have a consistent model that supports generic tools.

To back up configuration files in YAML format:

```
# execute backup yaml-config {ftp | tftp} <filename> <server> [username] [password]
```

To restore configuration files in YAML format:

```
# execute restore yaml-config {ftp | tftp} <filename> <server> [username] [password]
```

In FortiOS 7.2.4 and later, and 7.4.0 and later, use:

```
# execute restore config {ftp | tftp} <filename> <server> [username]
[password]
```

Examples

To back up configuration files in YAML format to the TFTP server:

```
# execute backup yaml-config  tftp  301E.yaml 172.16.200.55
    Please wait...
    Connect to tftp server 172.16.200.55 ...
    #
    Send config file to tftp server OK.
```

To restore configuration files in YAML format to the FTP server:

```
# execute restore  yaml-config  ftp  301E-1.yaml 172.16.200.55 root sys@qa123456
    This operation will overwrite the current setting and could possibly reboot the system!
    Do you want to continue? (y/n) y
    Please wait...
    Connect to ftp server 172.16.200.55 ...
    Get config file from ftp server OK.
    File check OK.
    #
    The system is going down NOW !!
```

YAML configuration file example

The following is an example of output from a YAML configuration file:

```
vdom:
    - root:
global:
    system_global:
        alias: "FortiGate-301E"
        hostname: "FortiGate-301E"
        switch-controller: enable
        timezone: 04
        vdom-mode: multi-vdom
    system_accprofile:
        - prof_admin:
            secfabgrp: read-write
            ftviewgrp: read-write
            authgrp: read-write
            sysgrp: read-write
            netgrp: read-write
            loggrp: read-write
            fwgrp: read-write
            vpngrp: read-write
            utmgrp: read-write
            wanoptgrp: read-write
            wifi: read-write
```

Remove split-task VDOMs and add a new administrative VDOM type

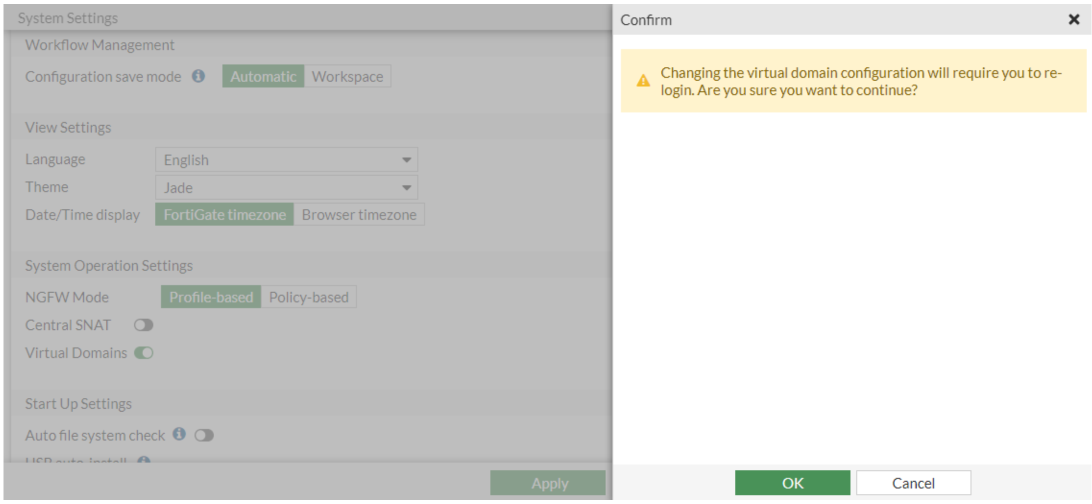
When a virtual domain (VDOM) is set to multi VDOM mode, individual VDOMs can be configured as an administrative or traffic type. When the VDOM type is set to *Admin*, the VDOM is used for management purposes only. Administrative users can log in to the FortiGate using SSH, HTTPS, and so on but traffic cannot pass through. When VDOM type is set to *Traffic*, the VDOM can pass traffic like regular VDOMs.

Only one administrative VDOM can exist at a time and cannot be set on a FortiWifi. A VDOM cannot be an administrative type and in transparent mode at the same time.

The multi VDOM is more flexible than split-task VDOM mode. Upon upgrade, if a FortiGate is in split-task VDOM mode, it will be converted to multi VDOM mode. The FG-traffic VDOM will become a traffic VDOM. The root VDOM will become an administrative VDOM.

To configure an administrative VDOM in the GUI:

1. Enable virtual domains:
   1. Go to *System > Settings* and enable *Virtual Domains* in the *System Operation Settings* section.



System Settings

Workflow Management

Configuration save mode: Automatic | Workspace

View Settings

Language: English

Theme: Jade

Date/Time display: FortiGate timezone | Browser timezone

System Operation Settings

NGFW Mode: Profile-based | Policy-based

Central SNAT

Virtual Domains

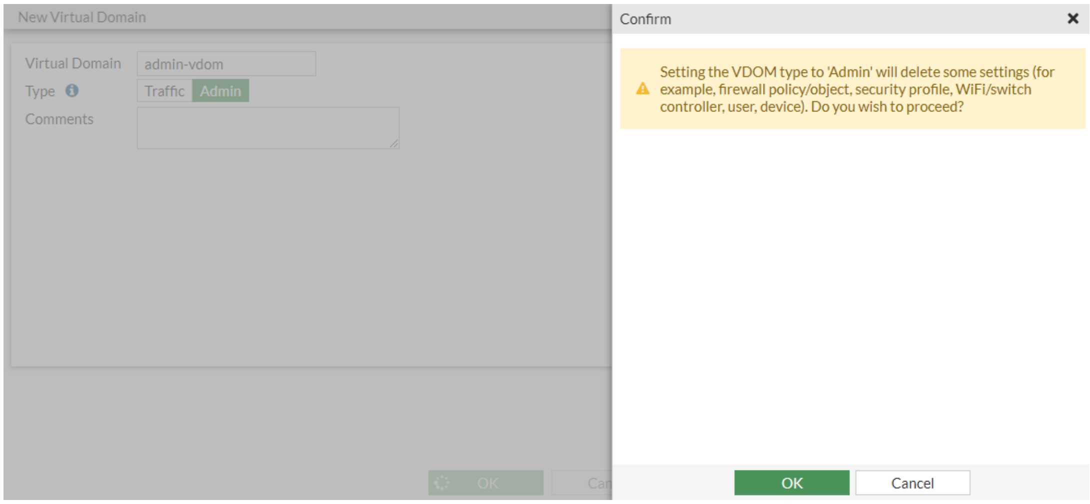
Start Up Settings

Auto file system check

Confirm

Changing the virtual domain configuration will require you to re-login. Are you sure you want to continue?

   2. Click *OK* in the confirmation pane.
   3. Enter your *Username* and *Password* to log in. Virtual domains are enabled.
2. Create an administrative VDOM:
   1. Go to *System > VDOM* and click *Create New*.
   2. Enter a *Virtual Domain* name and set the *Type* to *Admin*.
   3. Click *OK*.



New Virtual Domain

Virtual Domain: admin-vdom

Type: Traffic | Admin

Comments

Confirm

Setting the VDOM type to 'Admin' will delete some settings (for example, firewall policy/object, security profile, WiFi/switch controller, user, device). Do you wish to proceed?

   4. Click *OK* in the confirmation pane.

      The administrative VDOM is created.

To configure the VDOM type in the CLI:

```
config system settings
    set vdom-type {traffic | admin}
end
```

Introduce maturity firmware levels

Starting with FortiOS 7.2.0, released FortiOS firmware images use tags to indicate the following maturity levels:

- The *Feature* tag indicates that the firmware release includes new features.
- The *Mature* tag indicates that the firmware release includes no new, major features. Mature firmware will contain bug fixes and vulnerability patches where applicable.

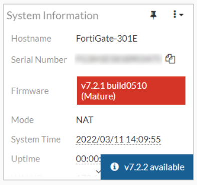
Administrators can use the tags to identify the maturity level of the current firmware in the GUI or CLI.

Administrators can view the maturity level of each firmware image that is available for upgrade on the *Fabric Management* page. When upgrading from mature firmware to feature firmware, a warning message is displayed.

To demonstrate the functionality of this feature, this example uses FortiGates that are running and upgrading to fictitious build numbers.

To view maturity levels for firmware in the GUI:

1. Go to *Dashboard > Status*. The *Firmware* field in the *System Information* widget displays the version with build and either *(Mature)* or *(Feature)*.
   The following is an example of firmware with the *(Mature)* tag:



System Information

Hostname FortiGate-301E

Serial Number [redacted]

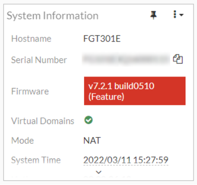
Firmware v7.2.1 build0510 (Mature)

Mode NAT

System Time 2022/03/11 14:09:55

Uptime 00:00:

The following is an example of firmware with the *(Feature)* tag:



System Information

Hostname FGT301E

Serial Number [redacted]

Firmware v7.2.1 build0510 (Feature)

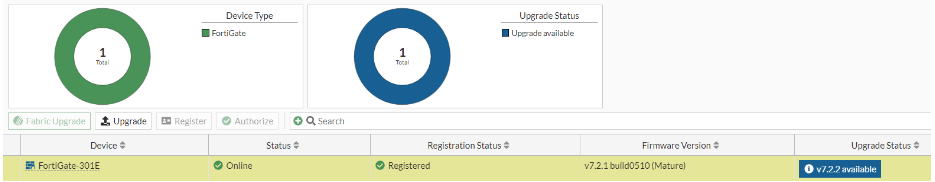
Virtual Domains ✓

Mode NAT

System Time 2022/03/11 15:27:59

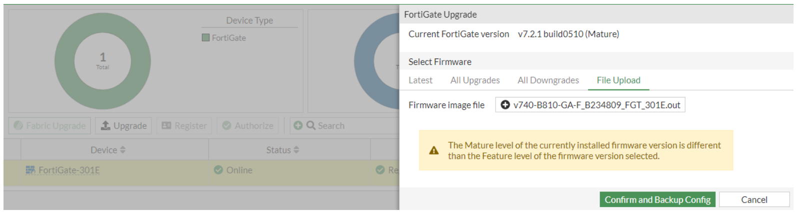
To upgrade mature firmware to feature firmware with a file upload in the GUI:

1. Go to *System > Fabric Management* . The *Firmware Version* column displays the version and *(Mature)*.



Device	Status	Registration Status	Firmware Version	Upgrade Status
FortiGate-301E	✓ Online	✓ Registered	v7.2.1 build0510 (Mature)	v7.2.2 available

2. Select the FortiGate, and click *Upgrade*. The *FortiGate Upgrade* pane opens.
3. Click the *File Upload* tab and upload the image file.
   When upgrading to feature firmware, a warning message appears about the maturity level of the selected firmware for the upgrade. In this example, the upgrade would go from a mature firmware version to a feature firmware version.



FortiGate Upgrade

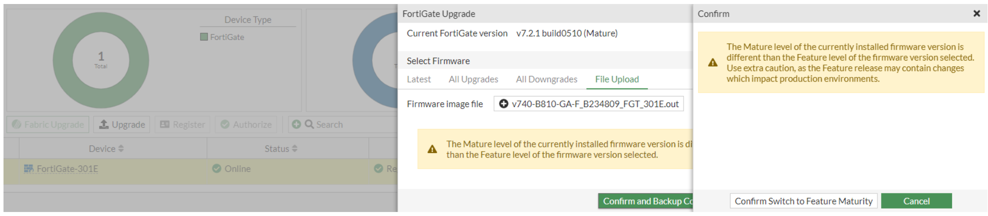
Current FortiGate version v7.2.1 build0510 (Mature)

Select Firmware

Firmware image file: v740-B810-GA-F_B234809_FGT_301E.out

The Mature level of the currently installed firmware version is different than the Feature level of the firmware version selected.

4. Click *Confirm and Backup Config*.
   The *Confirm* pane opens with a warning message:



FortiGate Upgrade

Current FortiGate version v7.2.1 build0510 (Mature)

Select Firmware

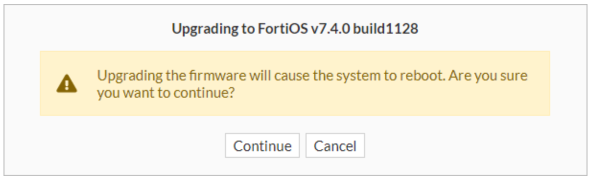
Firmware image file: v740-B810-GA-F_B234809_FGT_301E.out

The Mature level of the currently installed firmware version is di than the Feature level of the firmware version selected.

Confirm

The Mature level of the currently installed firmware version is different than the Feature level of the firmware version selected. Use extra caution, as the Feature release may contain changes which impact production environments.

5. Review the warning, and click *Confirm Switch to Feature Maturity*.
   The new firmware image is uploaded to the FortiGate, and a confirmation dialog box is displayed.



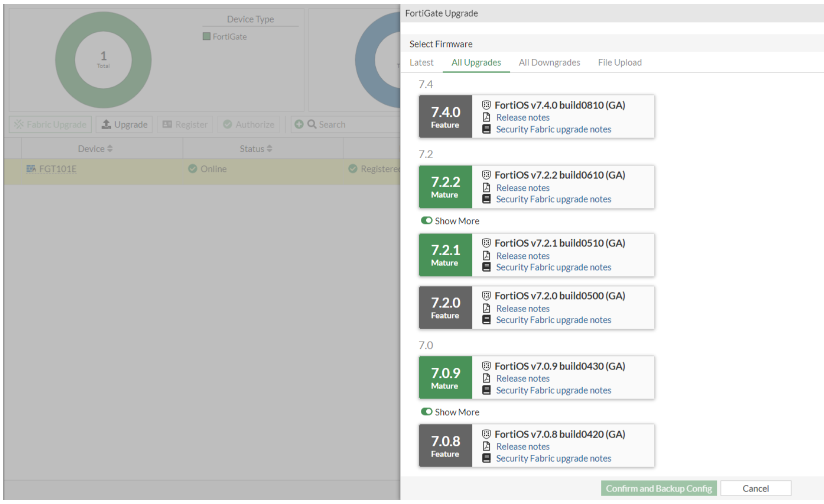
Upgrading to FortiOS v7.4.0 build1128

Upgrading the firmware will cause the system to reboot. Are you sure you want to continue?

6. Click *Continue* to complete the upgrade.

To upgrade mature firmware to feature firmware using the upgrade path in the GUI:

1. Go to *System > Fabric Management* .
2. Select a FortiGate, and click *Upgrade*. The *FortiGate Upgrade* pane opens.
3. Click the *All Upgrades* tab to view all available firmware images with their maturity levels.
   A gray box around the version number and the label *Feature* identifies feature firmware version. A green box around the version with the label *Mature* identifies a mature firmware version.



FortiGate Upgrade

Select Firmware

7.4

- 7.4.0 Feature — FortiOS v7.4.0 build0810 (GA)

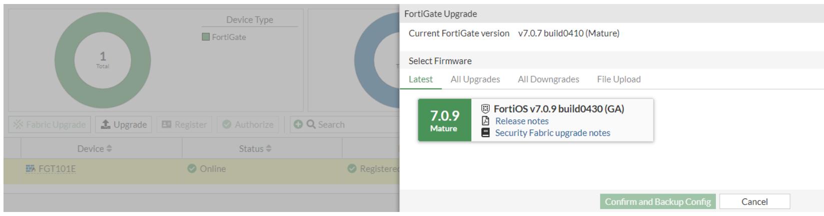
7.2

- 7.2.2 Mature — FortiOS v7.2.2 build0610 (GA)
- 7.2.1 Mature — FortiOS v7.2.1 build0510 (GA)
- 7.2.0 Feature — FortiOS v7.2.0 build0500 (GA)

7.0

- 7.0.9 Mature — FortiOS v7.0.9 build0430 (GA)
- 7.0.8 Feature — FortiOS v7.0.8 build0420 (GA)

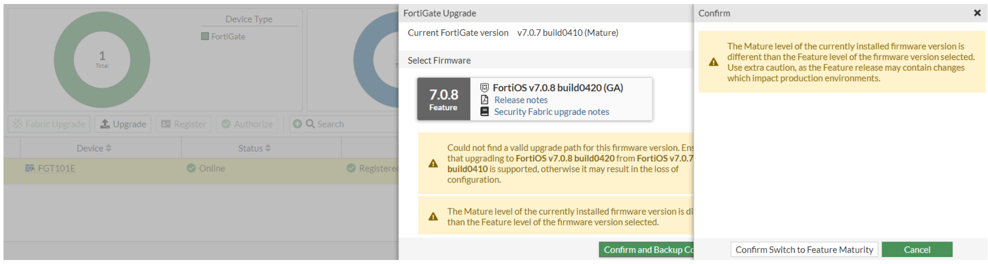
4. Click the *Latest* tab to view the latest available firmware version with its maturity level.
   In the following example, the latest firmware version is mature:



Current FortiGate version v7.0.7 build0410 (Mature)

FortiOS v7.0.9 build0430 (GA)

5. Select a version and click *Confirm and Backup Config*.
   When the latest firmware version is a feature release, a warning is displayed.



Current FortiGate version v7.0.7 build0410 (Mature)

FortiOS v7.0.8 build0420 (GA)

Could not find a valid upgrade path for this firmware version. Ens that upgrading to **FortiOS v7.0.8 build0420** from **FortiOS v7.0.7 build0410** is supported, otherwise it may result in the loss of configuration.

The Mature level of the currently installed firmware version is di than the Feature level of the firmware version selected.

The Mature level of the currently installed firmware version is different than the Feature level of the firmware version selected. Use extra caution, as the Feature release may contain changes which impact production environments.

6. Click *Confirm Switch to Feature Maturity* to complete the upgrade.

To view maturity levels for firmware in the CLI:

```
# get system status
Version: FortiGate-301E v7.4.0,build0810,220307 (GA.F)
...
```

In this example, the `Version` field includes `.F` to indicate that the maturity level is feature.

```
# get system status
Version: FortiGate-301E v7.2.2,build0610,220304 (GA.M)
...
```

In this example, the `Version` field includes `.M` to indicate that the maturity level is mature.

To upgrade mature firmware to feature firmware in the CLI:

```
# execute restore image tftp v744-B1010-GA-F_B234847_FGT_301E.out 172.16.200.55
This operation will replace the current firmware version!
Do you want to continue? (y/n)y
Please wait...
Connect to tftp server 172.16.200.55 ...
##############################################################################
Get image from tftp server OK.
Verifying the signature of the firmware image.

Warning: Upgrading to an image with Feature maturity notation.
Image file uploaded is marked as a Feature image, are you sure you want to upgrade?
Do you want to continue? (y/n)y
Please confirm again. Are you sure you want to upgrade using uploaded file?
Do you want to continue? (y/n)y
Checking new firmware integrity ... pass
Please wait for system to restart.
Firmware upgrade in progress ...
Done.
The system is going down NOW !!
```

In this example, the firmware is upgraded from mature status to feature status, and includes warnings.

Restrict SSH and telnet jump host capabilities - 7.2.1

Jump hosts are used to access devices in separate security zones, such as the internet and an internal network. Administrator access profiles can be configured to prevent administrators from using the FortiGate as a jump host for SSH and telnet connections.

To configure permission to execute SSH or telnet commands in an access profile:

```
config system accprofile
    edit <name>
        set system-execute-ssh {enable | disable}
        set system-execute-telnet {enable | disable}
    next
end
```

To block SSH and telnet connections for an administrator:

1. Disable permission to execute SSH or telnet commands in an administrator access profile:

```
config system accprofile
    edit "test_accprofile"
        set system-execute-ssh disable
        set system-execute-telnet disable
    next
end
```

2. Configure an administrator in the profile:

```
config system admin
    edit "admin1"
        set accprofile "test_accprofile"
        set vdom "root"
        set password **********
    next
end
```

3. Log in as the new administrator, and attempt to connect to another host using SSH or telnet:

```
# execute ssh root@172.16.200.55
You are not entitled to run the command.
Command fail. Return code -37
```

```
# execute ssh6 root@2000:172:16:200::55
You are not entitled to run the command.
Command fail. Return code -37
```

```
# execute telnet 172.16.200.55
You are not entitled to run the command.
Command fail. Return code -37
```

Enable automatic firmware updates - 7.2.1

The `auto-firmware-upgrade` option can be enabled to automatically update firmware based on the FortiGuard upgrade path. When enabled, the FortiGate will look for an upgrade path and perform an upgrade at a time within the time period specified by the administrator. The upgrade will only be performed on a patch within the same major release version.

```
config system fortiguard
    set auto-firmware-upgrade {enable | disable}
    set auto-firmware-upgrade-day {sunday monday tuesday wednesday thursday friday saturday}
    set auto-firmware-upgrade-start-hour <integer>
    set auto-firmware-upgrade-end-hour <integer>
end
```

`auto-firmware-upgrade {enable | disable}`	Enable/disable automatic patch-level firmware upgrade from FortiGuard.
`auto-firmware-upgrade-day {sunday monday tuesday wednesday thursday friday saturday}`	Enter the allowed day or days of the week to start the automatic patch-level firmware upgrade from FortiGuard.
`auto-firmware-upgrade-start-hour <integer>`	Set the start time of the designated time window for the automatic patch-level firmware upgrade from FortiGuard (in hours, 0 - 23, default = 2). The actual upgrade time is randomly selected in the time window.
`auto-firmware-upgrade-end-hour <integer>`	Set the end time of the designated time window for the automatic patch-level firmware upgrade from FortiGuard (in hours, 0 - 23, default = 4). When this value it is smaller than the start time, it will be treated as the same time in the next day. The actual upgrade time is randomly selected in the time window.

Example

To configure automatic firmware upgrades using the default schedule:

```
config system fortiguard
    set auto-firmware-upgrade enable
    set auto-firmware-upgrade-day sunday monday tuesday wednesday thursday friday saturday
    set auto-firmware-upgrade-start-hour 2
    set auto-firmware-upgrade-end-hour 4
end
```

Sample event log after enabling this option with a certain schedule:

```
date=2022-07-12 time=10:41:52 eventtime=1657647712247415816 tz="-0700" logid="0100032263"
type="event" subtype="system" level="notice" vd="vdom1" logdesc="Automatic firmware upgrade
schedule changed" user="system" msg="System patch-level auto-upgrade scheduled at local time
Wed Jul 13 02:18:36 2022, looking for patch-level upgrade only."
```

Performing the upgrade:

At the scheduled upgrade time, the FortiGate (forticldd daemon) will only try to upgrade to the latest patch in the same <major.minor> version in the image upgrade matrix.

For example, the following new releases are available in FortiGuard (fictitious build numbers are used to demonstrate the functionality of this feature):

```
FGTPlatform=FG201E|FGTCurrVersion=7.0.6|FGTCurrBuildNum=0366|FGTUpgVersion=7.2.2|FGTUpgBuild
Num=1602|BaselineVersion=DISABLE
```

```
FGTPlatform=FG201E|FGTCurrVersion=7.2.1|FGTCurrBuildNum=1224|FGTUpgVersion=7.2.2|FGTUpgBuild
Num=1602|BaselineVersion=DISABLE
```

Sample log event log after a successful upgrade:

```
date=2022-06-22 time=11:16:38 eventtime=1655921798859111708 tz="-0700" logid="0100032202"
type="event" subtype="system" level="critical" vd="root" logdesc="Image restored"
ui="forticldd" action="restore-image" status="success" msg="User  restored the image from
forticldd (v7.2.1,build1224 -> v7.2.2,build1602)"
```

Other scenarios

If `auto-firmware-upgrade` is changed to be disabled, the FortiGate (forticldd daemon) will not perform a scheduled upgrade.

Sample event log after disabling automatic firmware upgrades:

```
date=2022-06-22 time=10:31:25 eventtime=1655919085881435255 tz="-0700" logid="0100032263"
type="event" subtype="system" level="notice" vd="root" logdesc="Automatic firmware upgrade
schedule changed" user="system" msg="System patch-level auto-upgrade disabled."
```

If there is no upgrade image on the server, the forticldd daemon will reschedule the update to the next available time.

Sample debug output:

```
[874] sch_auto_update_done: No newer build found in the current major release.
[805] fds_schedule_auto_fmwr_upgrade: trace
[844] fds_schedule_auto_fmwr_upgrade: Automatic firmware upgrade is scheduled at (Local) Wed
Jun  1 15:52:30 2022
```

Sample event log after rescheduling the update:

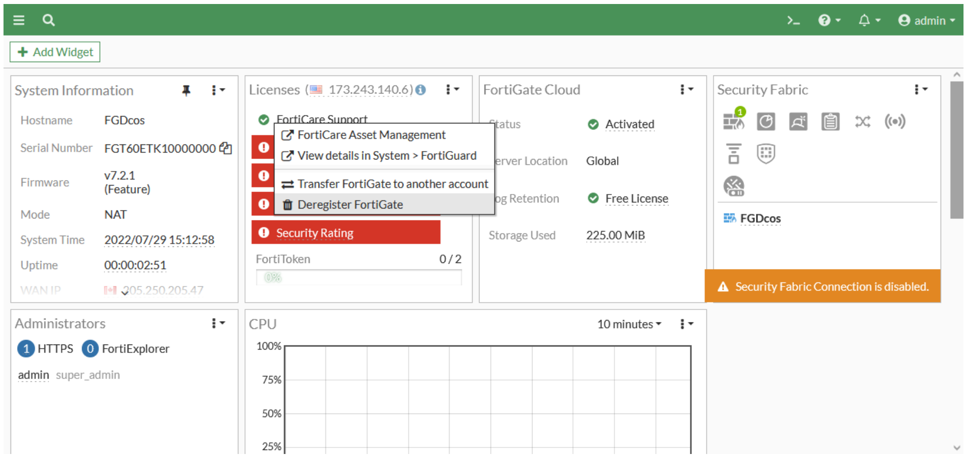
```
date=2022-06-22 time=12:31:17 eventtime=1655926278277347987 tz="-0700" logid="0100032263"
type="event" subtype="system" level="notice" vd="root" logdesc="Automatic firmware upgrade
schedule changed" user="system" msg="System patch-level auto-upgrade scheduled at local time
Thu Jun 23 12:40:21 2022, looking for patch-level upgrade only."
```

Deregistration from the GUI - 7.2.1

An administrator can deregister a FortiGate, if the device has been registered for three or more years, using the GUI or CLI, without having to contact FortiCare administration. After the device is deregistered, all associated contracts are also deregistered, and all of the administrator's information is wiped.

To deregister the FortiGate in the GUI:

1. Go to *Dashboard* > *Status*.
2. In the License widget, click *FortiGate Support* and select *Deregister FortiGate*.

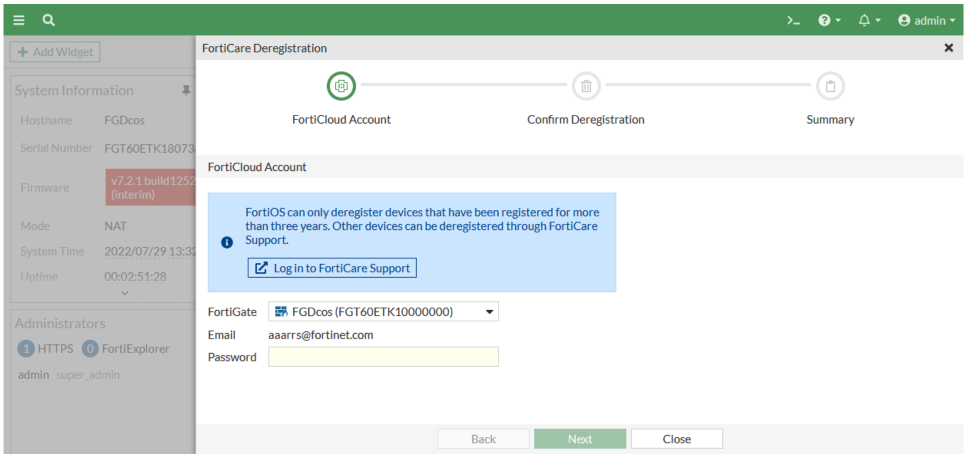


Hostname FGDcos
Serial Number FGT60ETK10000000
Firmware v7.2.1 (Feature)
Mode NAT
System Time 2022/07/29 15:12:58
Uptime 00:00:02:51
WAN IP 205.250.205.47

Status Activated
Server Location Global
Log Retention Free License
Storage Used 225.00 MiB

admin super_admin

The FortiCare Deregistration pane opens.



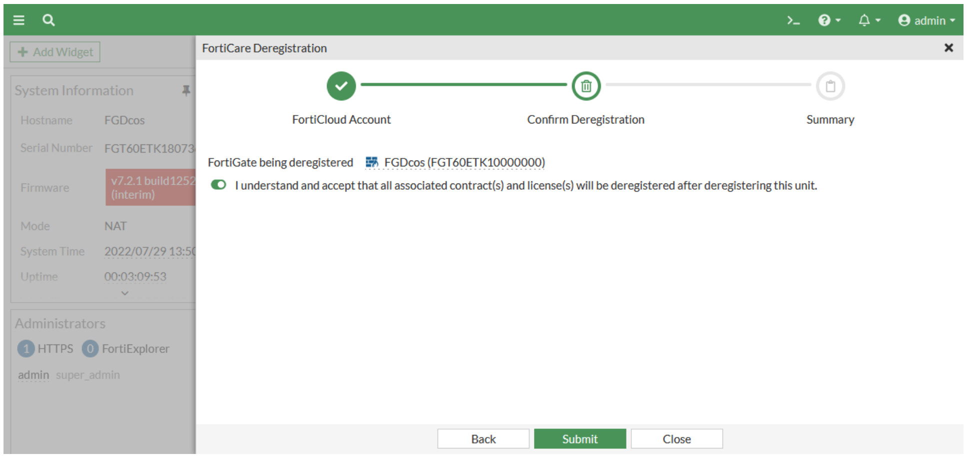
FortiCloud Account

FortiOS can only deregister devices that have been registered for more than three years. Other devices can be deregistered through FortiCare Support.

Log in to FortiCare Support

FortiGate FGDcos (FGT60ETK10000000)
Email aaarrs@fortinet.com
Password

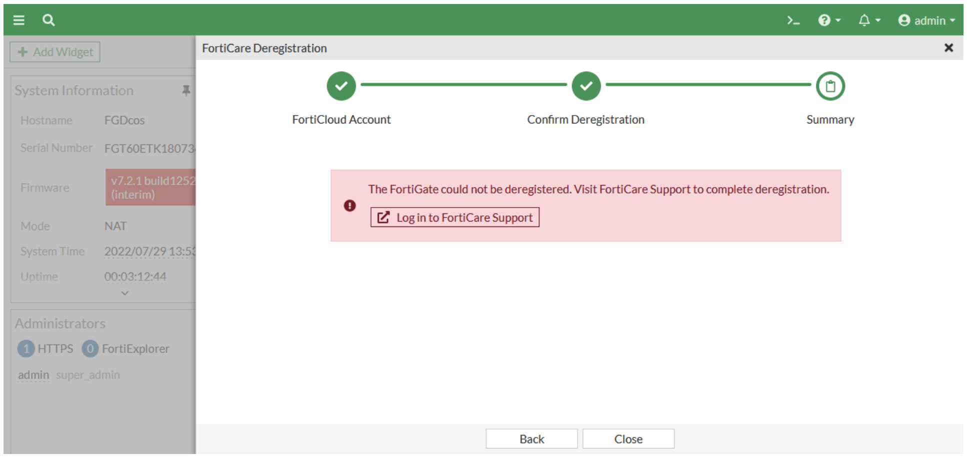
3. Enter your password then click *Next*.
4. Confirm the FortiGate deregistration then click *Submit*.



FortiGate being deregistered FGDcos (FGT60ETK10000000)

I understand and accept that all associated contract(s) and license(s) will be deregistered after deregistering this unit.

If the FortiGate has been registered for less then three years, the deregistration will fail.



The FortiGate could not be deregistered. Visit FortiCare Support to complete deregistration.

To deregister the FortiGate in the CLI:

```
# diagnose forticare direct-registration product-deregister <accountID> <password>
```

If the FortiGate has been registered for less then three years, the deregistration will fail:

```
forticare_product_deregister:1335: Failed to get response (rc = 0, http_code = 403)
Unit deregistration unsuccessful.
```

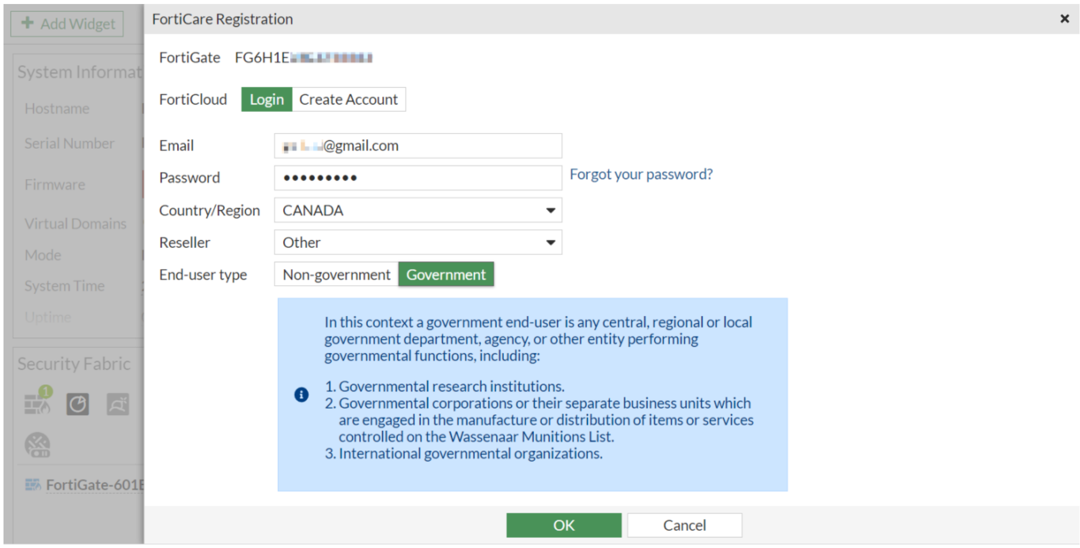
Add government end user option for FortiCare registration - 7.2.1

When registering using FortiCare, users can select a *Non-government* or *Government* end user type for parity with the registration process using the support portal.

To register as a government end user using FortiCare:

1. Go to *Dashboard* > *Status*.
2. In the *Licenses* widget, click *FortiCare Support* and select *Register*. The *FortiCare Registration* pane opens.
3. Enter your FortiCare *Email* address and *Password*.
4. Select your *Country/Region* and *Reseller*.

5. Set the *End-user type* to *Government*.



FortiCare Registration ×

FortiGate FG6H1E[redacted]

FortiCloud Login Create Account

Email [redacted]@gmail.com

Password ••••••••• Forgot your password?

Country/Region CANADA

Reseller Other

End-user type Non-government Government

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions, including:

1. Governmental research institutions.
2. Governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.
3. International governmental organizations.

OK Cancel

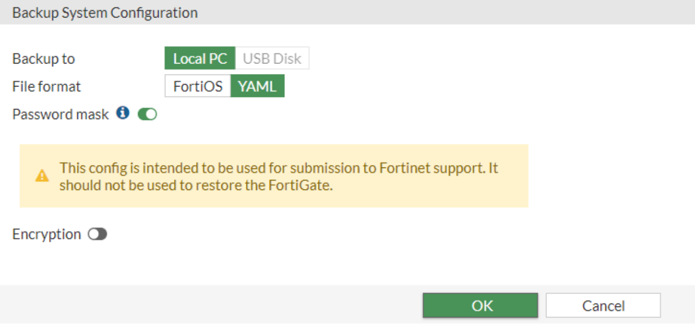
6. Click *OK*.

Support backing up configurations with password masking - 7.2.1

When backing up a configuration that will be shared with a third party, such as Fortinet Inc. Support, passwords and secrets should be obfuscated from the configuration to avoid information being unintentionally leaked. Password masking can be completed in the *Backup System Configuration* page and in the CLI. When password masking is enabled, passwords and secrets will be replaced in the configuration file with `FortinetPasswordMask`.

To mask passwords in the GUI:

1. Click on the username in the upper right-hand corner of the screen and select *Configuration* > *Backup*.
2. Select *YAML* as the *File format*.
3. Enable *Password mask*. A warning message is displayed.



Backup System Configuration

Backup to Local PC USB Disk

File format FortiOS YAML

Password mask

This config is intended to be used for submission to Fortinet support. It should not be used to restore the FortiGate.

Encryption

OK Cancel

4. Click *OK*. The full configuration file is saved to your computer with passwords and secrets obfuscated.

To mask passwords in a configuration backup in the CLI:

```
# execute backup obfuscated-config {flash | ftp | management-station | sftp | tftp | usb}
```

To mask passwords in the full configuration backup in the CLI:

```
# execute backup obfuscated-full-config {ftp | sftp | tftp | usb}
```

To mask passwords in a configuration backup with YAML formatting in the CLI:

```
# execute backup obfuscated-yaml-config {ftp | tftp}
```

If a configuration is being backed up on a server, server information must be included with the command. Other information that may be required with an `execute backup` command includes file names, passwords, and comments. See Configuration backups in the Administration Guide for more information.

Example configuration with password masking

The following is an example of output with password masking enabled:

```
config system admin
    edit "1"
        set accprofile "prof_admin"
        set vdom "root"
        set password FortinetPasswordMask
    next
end
config vpn ipsec phase1-interface
    edit "vpn-1"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: vpn-1 (Created by VPN wizard)"
        set wizard-type static-fortigate
        set remote-gw 172.16.200.55
        set psksecret FortinetPasswordMask
    next
end
config wireless-controller vap
    edit "ssid-1"
        set passphrase FortinetPasswordMask
        set schedule "always"
    next
end
```

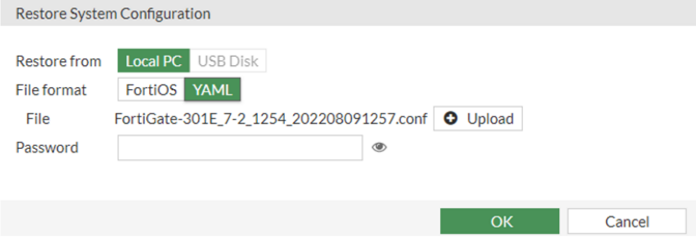
Restoring configurations

When restoring a configuration file that has password masking enabled, all obfuscated passwords and secrets will be restored as well.

Restoring the FortiGate with a configuration with passwords obfuscated is not recommended.

To restore an obfuscated configuration:

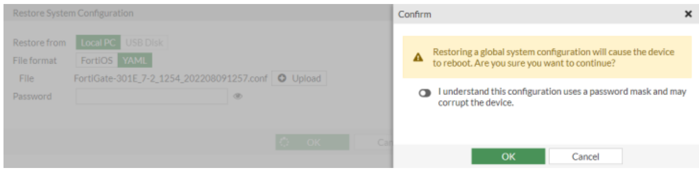
1. Click on the user name in the upper right-hand corner of the screen and select *Configuration* > *Restore*.
2. Select *YAML* as the *File format*.
3. Click *Upload*. The File Explorer is displayed.
4. Navigate to the configuration file and click *Open*.



Restore System Configuration

Restore from: Local PC
File format: YAML
File: FortiGate-301E_7-2_1254_202208091257.conf
Password:

5. (Optional) Enter the file password in the *Password* field.
6. Click *OK*. The *Confirm* pane is displayed with a warning.



Confirm

Restoring a global system configuration will cause the device to reboot. Are you sure you want to continue?

I understand this configuration uses a password mask and may corrupt the device.

7. Toggle the acknowledgment.
8. Click *OK*.

New default certificate for HTTPS administrative access - 7.2.1

By default, the FortiGate uses the certificate named Fortinet_GUI_Server for HTTPS administrative access. This certificate is generated and signed by the built-in Fortinet_CA_SSL certificate, which dynamically updates the SAN field of the Fortinet_GUI_Server certificate with the IP addresses of all interfaces enabled for HTTPS. After installing the Fortinet_CA_SSL CA certificate on a PC, administrators can access the FortiGate GUI through a browser without any warnings.

In previous versions of FortiOS, the FortiGate uses the self-signed certificate for default HTTPS administrative access. Because this certificate is untrusted and does not contain a valid SAN field, browsers will raise a warning by default when an administrator accesses the FortiGate GUI.

How the certificate works

The Fortinet_GUI_Server certificate is generated by the built-in certificate authority (CA) with the Fortinet_CA_SSL certificate, which is unique to each FortiGate. This CA certificate is also used in SSL deep inspection. When the Fortinet_GUI_Server certificate is generated, the SAN (Subject Alternative Name) extension field is populated with the IP addresses of all physical and logical (VLAN, loopback, and so on) interfaces enabled for HTTPS. It is also populated with the management IP address whenever this field is an IP address and not an FQDN. If there are any changes to the IP addresses on the interface or management IP, the Fortinet_GUI_Server certificate is updated and regenerated with the new IP. If the Fortinet_CA_SSL certificate itself is updated, the Fortinet_GUI_Server certificate is regenerated.

Because the root CA is not a public CA, the Fortinet_CA_SSL CA certificate must be installed in the trusted certificate store on the client PC in order for the trusted certificate chain to be recognized by a browser. This certificate can be downloaded from the FortiGate in several ways.

The Fortinet_GUI_Server certificate can only be used for HTTPS administrative access. It cannot be used anywhere else.

Example

The HTTPS server certificate can be configured in the GUI or CLI.

To configure the HTTPS server certificate in the GUI:

1. On an administrative PC, log in to the FortiGate GUI and go to *System* > *Settings*.
2. In the *Administration Settings* section, set the *HTTPS server certificate* to *Fortinet_GUI_Server*.
3. Download the Fortinet_CA_SSL certificate using one of the following methods:
   - On the *System* > *Settings* page, click *Download HTTPS CA certificate* (below the *HTTPS server certificate* option).
   - Go to *System* > *Certificates*. In the *Local CA Certificate* section, select *Fortinet_CA_SSL*, and click *Download*.
   - Go to *Dashboard* > *Status*. In the *Administrator* widget, click *Download HTTPS CA certificate*.
4. Install the certificate in the PC’s trusted certificate store. Refer to your OS documentation if needed.
5. Reload the FortiGate GUI. The browser now trusts the certificate and does not display a certificate warning.
6. If you are connecting to the FortiGate over DNAT or port forwarding, the certificate needs to add the NATed management IP into the SAN field so that the browser does not display a warning about an invalid CN. Configure the management IP in the global settings:

```
config system global
    set management-ip <IP_address>
end
```

To configure the HTTPS server certificate in the CLI:

1. Configure the HTTPS server certificate:

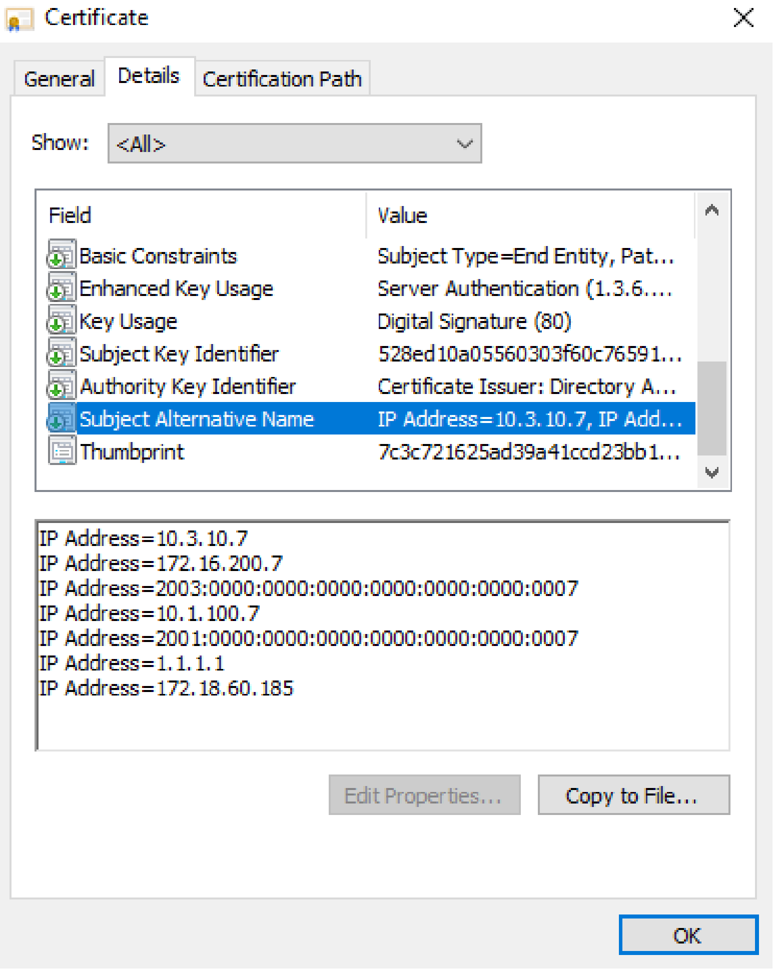
```
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

2. Download the Fortinet_CA_SSL certificate on the administrative PC through TFTP:

```
# execute vpn certificate local export tftp Fortinet_CA_SSL cer <file_name> <server_IP>

Done.
```

To verify the connection:

1. Access the FortiGate from a browser and verify the certificate information. For example, in Chrome:
   - **a.** In the left side of the address bar, click the icon to view the site information.
   - **b.** Click *Certificate*.
   - **c.** Click the *Details* tab.
   - **d.** Locate the *Subject Alternative Name* (SAN) field, and note the IP addresses that are listed (*1.1.1.1*).

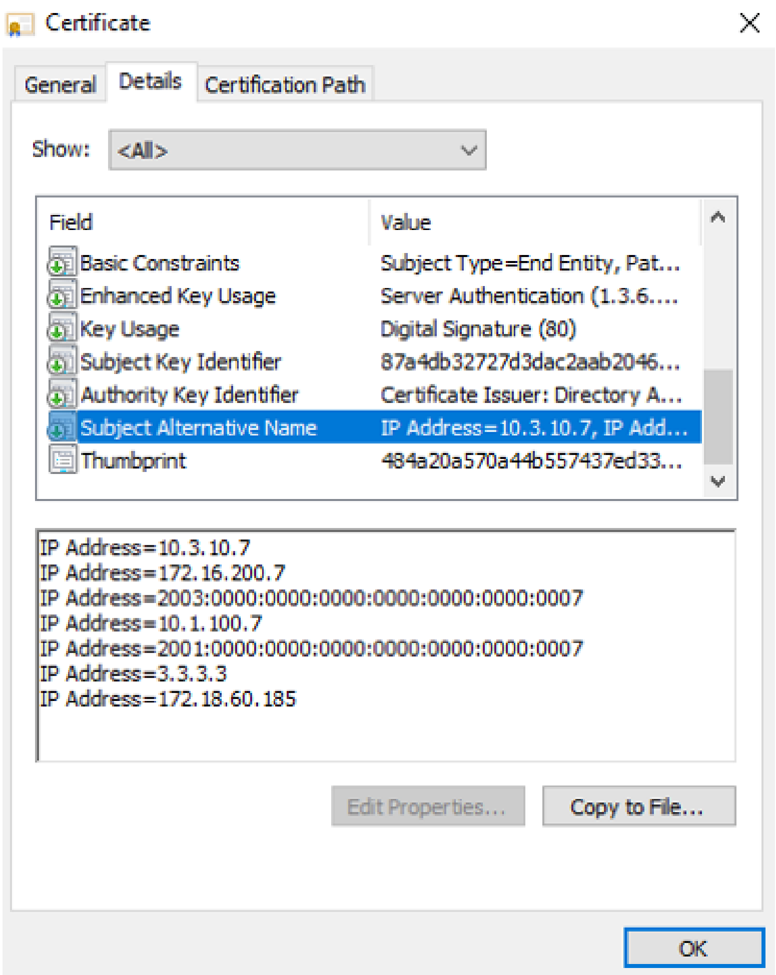


Show: <All>

Field	Value
Basic Constraints	Subject Type=End Entity, Pat...
Enhanced Key Usage	Server Authentication (1.3.6....
Key Usage	Digital Signature (80)
Subject Key Identifier	528ed10a05560303f60c76591...
Authority Key Identifier	Certificate Issuer: Directory A...
Subject Alternative Name	IP Address=10.3.10.7, IP Add...
Thumbprint	7c3c721625ad39a41ccd23bb1...

```
IP Address=10.3.10.7
IP Address=172.16.200.7
IP Address=2003:0000:0000:0000:0000:0000:0000:0007
IP Address=10.1.100.7
IP Address=2001:0000:0000:0000:0000:0000:0000:0007
IP Address=1.1.1.1
IP Address=172.18.60.185
```

   - **e.** Click *OK*.
2. In FortiOS, change one of the interface addresses. In this example, the port11 address is changed from 1.1.1.1 to 3.3.3.3.
3. Reload the browser and review the certificate information again. The IP 1.1.1.1 in the SAN field is updated to *3.3.3.3*.



Show: <All>

Field	Value
Basic Constraints	Subject Type=End Entity, Pat...
Enhanced Key Usage	Server Authentication (1.3.6....
Key Usage	Digital Signature (80)
Subject Key Identifier	87a4db32727d3dac2aab2046...
Authority Key Identifier	Certificate Issuer: Directory A...
Subject Alternative Name	IP Address=10.3.10.7, IP Add...
Thumbprint	484a20a570a44b557437ed33...

```
IP Address=10.3.10.7
IP Address=172.16.200.7
IP Address=2003:0000:0000:0000:0000:0000:0000:0007
IP Address=10.1.100.7
IP Address=2001:0000:0000:0000:0000:0000:0000:0007
IP Address=3.3.3.3
IP Address=172.18.60.185
```

4. In FortiOS, go to *System* > *Certificates* and double-click *Fortinet_GUI_Server* to view the *Certificate Details*.
5. At the bottom of the pane, the *X509v3 Subject Alternative Name* field displays the IP addresses from the certificate.
6. Verify the logs when the certificate is regenerated:

```
# execute log filter category 1
# execute log display
12 logs found.
10 logs returned.

1: date=2022-06-23 time=09:11:44 eventtime=1656000704674434910 tz="-0700"
logid="0100022205" type="event" subtype="system" level="information" vd="root"
logdesc="Certificate succeed to auto-generate" user="system" action="certificate-
generate" status="successful" name="Fortinet_GUI_Server" msg="Successfully generated GUI
management cert"

2: date=2022-06-23 time=09:11:44 eventtime=1656000704674432668 tz="-0700"
logid="0101041986" type="event" subtype="vpn" level="information" vd="root"
logdesc="Certificate regenerated" action="info" user="N/A" ui="forticron"
name="Fortinet_GUI_Server" msg="A certificate is regenerated" cert-type="Local"
status="success"

3: date=2022-06-23 time=09:11:31 eventtime=1656000691825397831 tz="-0700"
logid="0100044547" type="event" subtype="system" level="information" vd="root"
logdesc="Object attribute configured" user="admin" ui="ssh(172.16.200.254)"
```

```
action="Edit" cfgtid=35782662 cfgpath="system.interface" cfgobj="port11" cfgattr="ip
[1.1.1.1 255.255.255.0->3.3.3.3 255.255.255.0]" msg="Edit system.interface port11"
```

Remove maintainer account - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Factory resetting the FortiGate when the password is lost

The maintainer account, which allowed users to log in through the console after a hard reboot, has been removed. For security reasons, users who lose their password must have physical access to the FortiGate and perform a TFTP restore of the firmware in order to regain access to the FortiGate. They will not have access to the current running configurations through the FortiGate. Configurations will be reset to the factory default once the firmware is reloaded. See Installing firmware from system reboot in the FortiOS Administration Guide for detailed instructions. This process requires a connection to the TFTP server where the firmware image is stored.

To restore the FortiGate:

This procedure may vary depending on whether the FortiGate is a physical appliance or a VM.

1. Connect to the console port.
2. Ensure you can see the FortiGate prompt from the console terminal.
3. Physically power off the device, then power on the device.
4. Boot into the boot menu by pressing a key when prompted.
5. Follow the steps in Installing firmware from system reboot to reload the firmware. Configurations will be reset to the factory default once the firmware is installed.
6. Once the firmware reload is complete, log in to the FortiGate to reconfigure the settings.

It is recommended to preform regular configuration backups and to store the backup on a secure server (see Configuration changes in the FortiOS Best Practices for more details). In the event that a password is lost, the configuration backup can be used to restore a configuration after the user completes the firmware installation process. This assumes the user knows the password from the previous backed up configuration. If the user does not know the password, they can still reload the configuration if it is not encrypted.

The following procedure describes how to edit an unencrypted backup configuration file so that the administrator password can be replaced before restoring the file.

To edit the configuration file when a password is lost:

1. Locate the line in the configuration file where `config system admin` is defined.
2. Edit an administrator account with an `accprofile` set to `super_admin`. This will ensure you can log in and perform any operations afterward.
3. Locate the line with `set password ENC xxxxxx`, and edit it to set a temporary new password in clear text (such as `set password cleartextpassword`).

4. Reload the configuration file.
5. Log in to the console using the temporary password, and then change the password.

> The configuration backup allows the administrator to confirm the firmware that the FortiGate is running, so the same firmware can be restored. This information is listed in the first line of the configuration: `config-version=FGT61F-7.2.4-FW-build1396-230131:opmode=0:vdom=0:user=admin`.

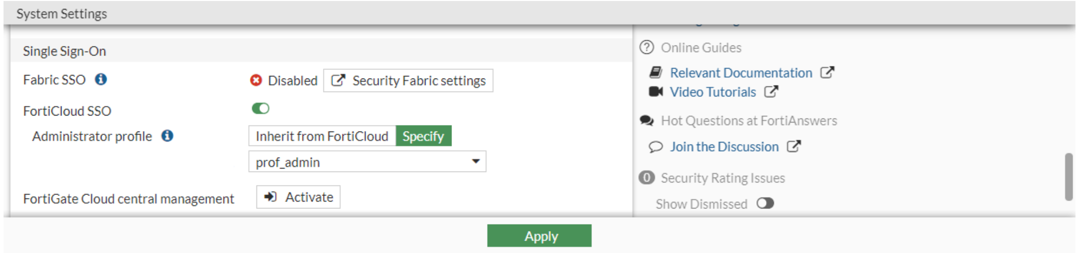
Allow the FortiGate to override FortiCloud SSO administrator user permissions - 7.2.4

> This information is also available in the FortiOS 7.2 Administration Guide:
> - Allowing the FortiGate to override FortiCloud SSO administrator user permissions

The FortiGate can allow single sign-on (SSO) from FortiCloud and FortiCloud IAM users with administrator profiles inherited from FortiCloud or overridden locally by the FortiGate. Similarly, users accessing the FortiGate remotely from FortiGate Cloud can have their permissions inherited or overridden by the FortiGate.

To enable FortiCloud SSO in the GUI:

1. Go to *System* > *Settings*.
2. In the *Single Sign-On* section, enable *FortiCloud SSO*.
3. Set the default *Administrator profile* to assign: *Inherit from FortiCloud*, or *Specify* and select a profile from the dropdown.



System Settings

Single Sign-On

Fabric SSO: ✖ Disabled

FortiCloud SSO: ●

Administrator profile: Inherit from FortiCloud | Specify

prof_admin

FortiGate Cloud central management: Activate

4. Click *Apply*.

To enable FortiCloud SSO in the CLI:

```
config system global
    set admin-forticloud-sso-login enable
    set admin-forticloud-sso-default-profile <profile>
end
```

The following administrator profiles are assigned based on the inherited or overwritten permissions:

User type	Inherited from FortiCloud/FortiGate Cloud	Specify
FortiCloud	Uses the super_admin profile.	Local user profile

User type	Inherited from FortiCloud/FortiGate Cloud	Specify
FortiCloud IAM	Is based on the IAM permission profile's FortiOS SSO portal settings: • If *Access* is disabled = no access • If *Access* is enabled and the *Access Type* is set to *SuperAdmin* = super_admin profile • If *Access* is enabled and the *Access Type* is set to *Read Only*= super_admin_readonly profile	Local user profile
FortiGate Cloud subscription tier	Uses the super_admin profile.	Local user profile
FortiGate Cloud free tier	Has read-only access.	Cannot override

This topic includes four use case examples:

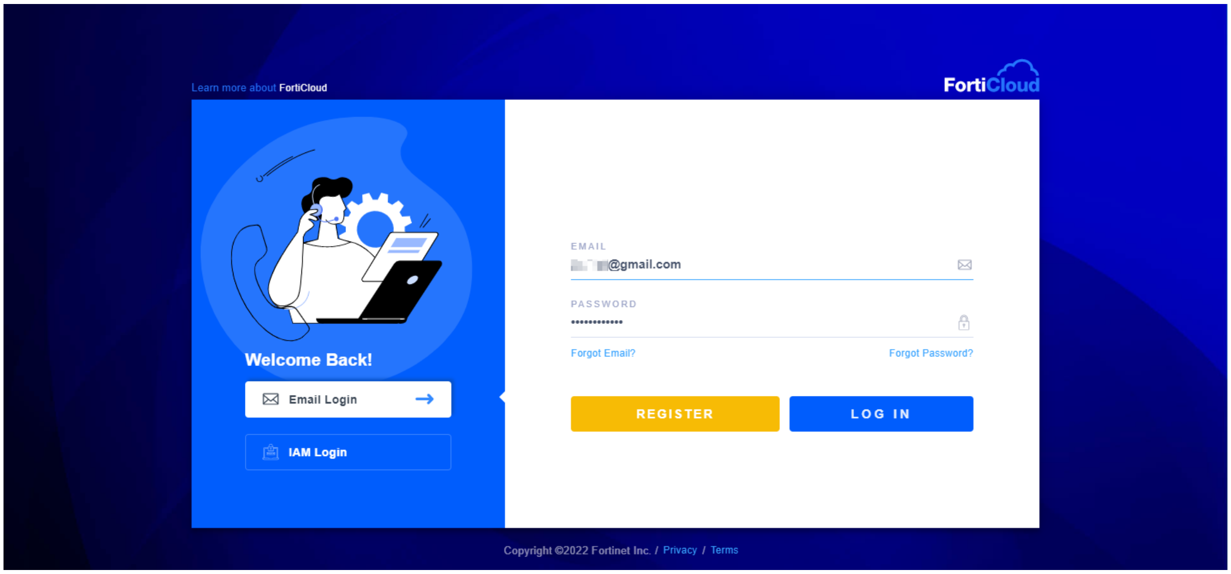
- Example 1: specifying permissions for a FortiCloud SSO user
- Example 2: inheriting FortiCloud permissions for a FortiCloud SSO user
- Example 3: specifying a local user profile for a FortiCloud IAM user
- Example 4: accessing a FortiGate remotely from FortiGate Cloud

Example 1: specifying permissions for a FortiCloud SSO user

In this example, a FortiCloud SSO user is configured to override permissions and use the prof_admin profile, which is a local read-only profile.

To configure the FortiCloud SSO user:

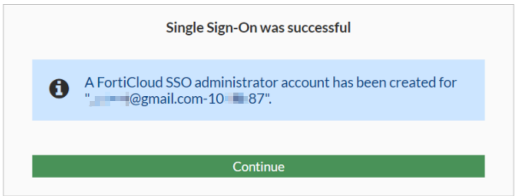
1. Go to *System* > *Settings*.
2. In the *Single Sign-On* section, enable *FortiCloud SSO*.
3. Set *Administrator profile* to *Specify*, and select *prof_admin*. The FortiCloud SSO user will be created upon the first login.
4. Get the user to log in to the FortiGate:
   a. On the FortiOS login screen, click *Sign in with FortiCloud*. The FortiCloud log in page opens.
   b. Click *Email Login*.
   c. Enter the FortiCloud account credentials and click *Log In*.



EMAIL
[redacted]@gmail.com

PASSWORD
••••••••••••

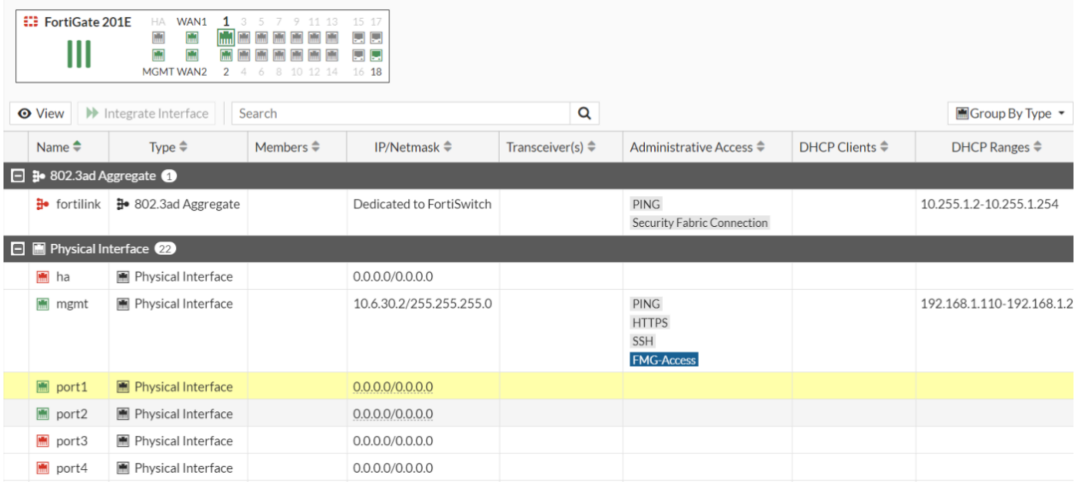
The new SSO user is created.



Single Sign-On was successful

A FortiCloud SSO administrator account has been created for "[redacted]@gmail.com-10[redacted]87".

Since the profile has read-only access, the SSO user can only view items (such as interfaces) and cannot edit them.



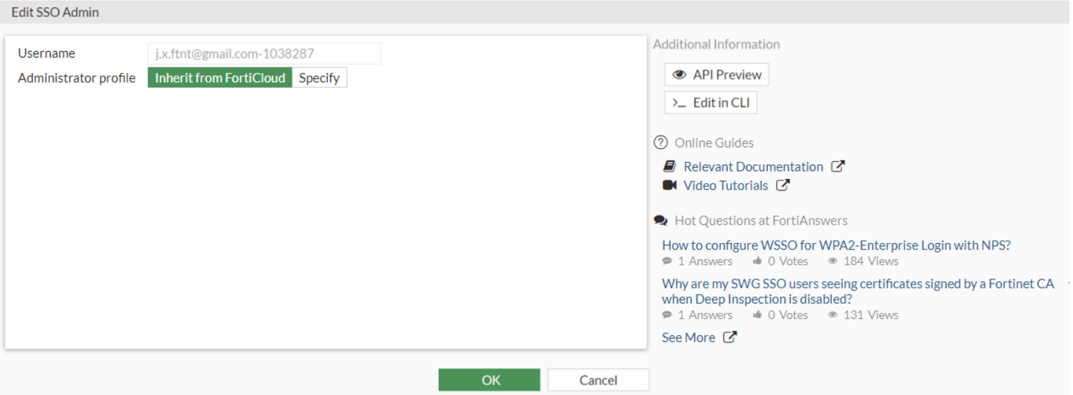
Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch		PING Security Fabric Connection		10.255.1.2-10.255.1.254
Physical Interface 22							
ha	Physical Interface		0.0.0.0/0.0.0.0				
mgmt	Physical Interface		10.6.30.2/255.255.255.0		PING HTTPS SSH FMG-Access		192.168.1.110-192.168.1.2
port1	Physical Interface		0.0.0.0/0.0.0.0				
port2	Physical Interface		0.0.0.0/0.0.0.0				
port3	Physical Interface		0.0.0.0/0.0.0.0				
port4	Physical Interface		0.0.0.0/0.0.0.0				

Example 2: inheriting FortiCloud permissions for a FortiCloud SSO user

In this example, a local administrator changes the permissions of an existing FortiCloud SSO user (created in the previous example) to *Inherit from FortiCloud*, which means the super_admin profile will be used.

To configure the existing SSO user:

1. Go to *System > Administrators* and edit the user in the *FortiCloud SSO Administrator* section (*********@gmail.com*).
2. Set *Administrator profile* to *Inherit from FortiCloud*.

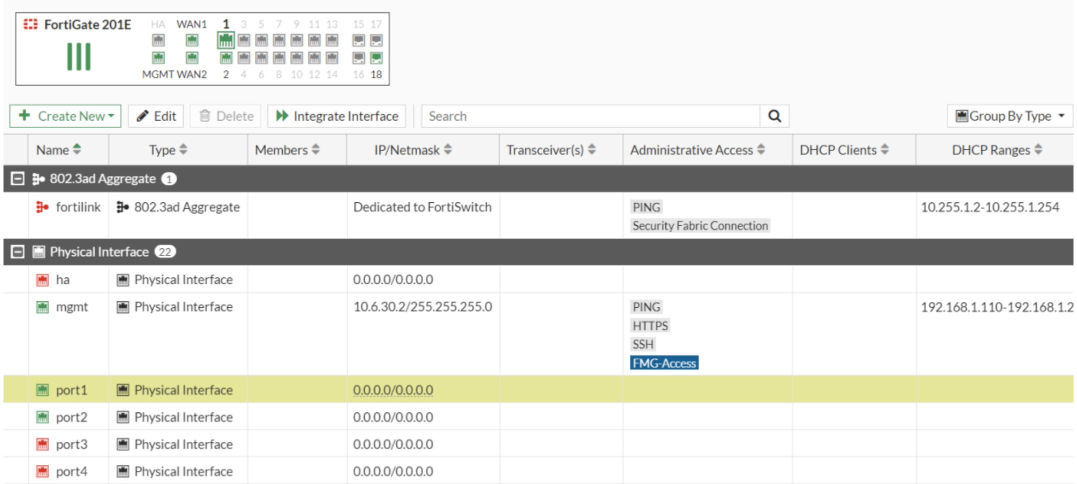


Edit SSO Admin

Username	j.x.ftnt@gmail.com-1038287
Administrator profile	Inherit from FortiCloud

Specify
Additional Information
API Preview
Edit in CLI
Online Guides
Relevant Documentation
Video Tutorials
Hot Questions at FortiAnswers
How to configure WSSO for WPA2-Enterprise Login with NPS?
1 Answers 0 Votes 184 Views
Why are my SWG SSO users seeing certificates signed by a Fortinet CA when Deep Inspection is disabled?
1 Answers 0 Votes 131 Views
See More
OK
Cancel

3. Click *OK*.
4. Get the user to log in to the FortiGate. Since the profile changed to super_admin, they can modify items (such as interfaces).



Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch		PING Security Fabric Connection		10.255.1.2-10.255.1.254
Physical Interface 22							
ha	Physical Interface		0.0.0.0/0.0.0.0				
mgmt	Physical Interface		10.6.30.2/255.255.255.0		PING HTTPS SSH FMG-Access		192.168.1.110-192.168.1.2
port1	Physical Interface		0.0.0.0/0.0.0.0				
port2	Physical Interface		0.0.0.0/0.0.0.0				
port3	Physical Interface		0.0.0.0/0.0.0.0				
port4	Physical Interface		0.0.0.0/0.0.0.0				

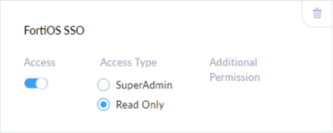
Example 3: specifying a local user profile for a FortiCloud IAM user

In this example, a FortiCloud IAM user is configured to have read-only SSO access based on the settings in the FortiOS SSO portal. Once the FortiCloud IAM user logs in, an administrator with super_admin access changes the permission of the IAM user to have super_admin access.

This example assumes the *FortiOS SSO* portal has already been added to the IAM permission profile. See Creating a permission profile and Managing permission profiles in the Identity & Access Management (IAM) Guide for more information about configuring permission profiles in FortiCloud.

To configure the FortiCloud IAM user:

1. In FortiCloud, configure the permission profile:
   a. Go to *Services* > *IAM*, then click *Permission Profiles*.
   b. Select a profile and click *Edit*.
   c. In the *FortiOS SSO* portal, enable *Access*. Set the *Access Type* to *Read Only*.



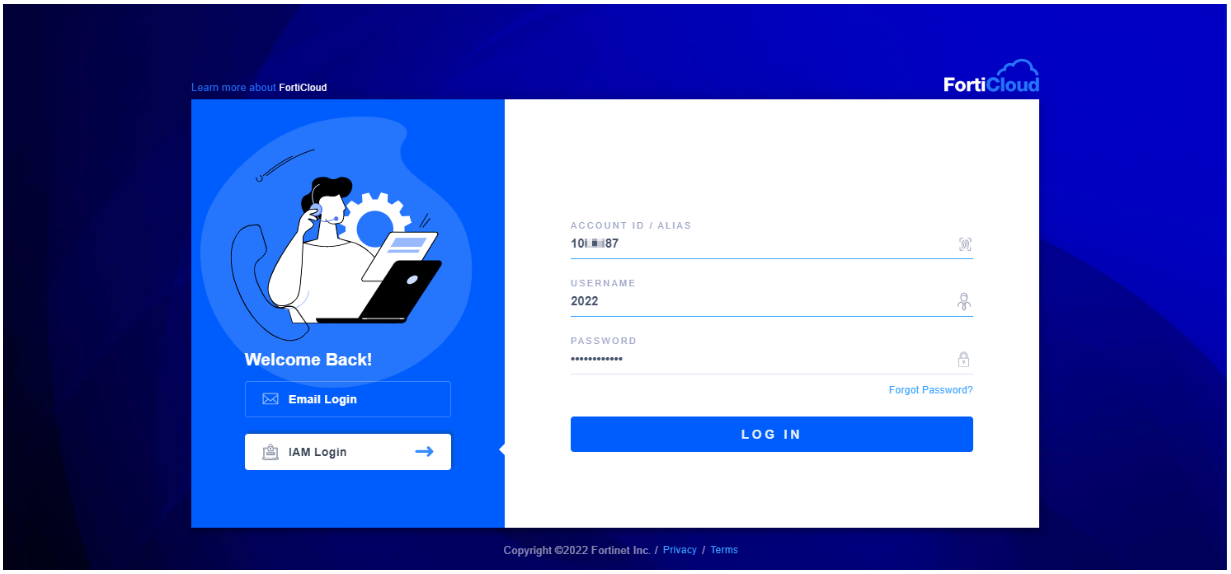
FortiOS SSO

Access: enabled

Access Type: ○ SuperAdmin ● Read Only

Additional Permission

   d. Click *Update*.
2. Get the user to log in to the FortiGate:
   a. On the FortiOS login screen, click *Sign in with FortiCloud*. The FortiCloud log in page opens.
   b. Click *IAM Login*.
   c. Enter the IAM account credentials and click *Log In*.



Learn more about FortiCloud

FortiCloud

Welcome Back!

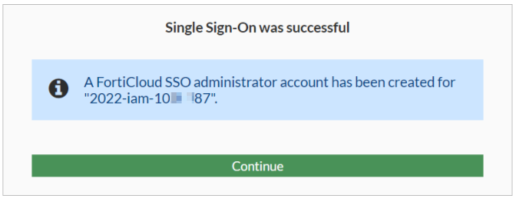
ACCOUNT ID / ALIAS: 10[redacted]87

USERNAME: 2022

PASSWORD: ••••••••••••

Copyright ©2022 Fortinet Inc. / Privacy / Terms

The new SSO user is created with a super_admin_readonly profile.



Single Sign-On was successful

A FortiCloud SSO administrator account has been created for "2022-iam-10[redacted]87".

3. Update the IAM user permission to have super_admin access:
   a. Log in to the FortiGate with a super_admin administrator account.
   b. Go to *System* > *Administrators* and edit the IAM user (*2022*).
   c. Set *Administrator profile* to *Specify* and select *super_admin*.
   d. Click *OK*.
4. Get the user to log in to the FortiGate again. Since the profile changed to super_admin, they can modify items.

Example 4: accessing a FortiGate remotely from FortiGate Cloud

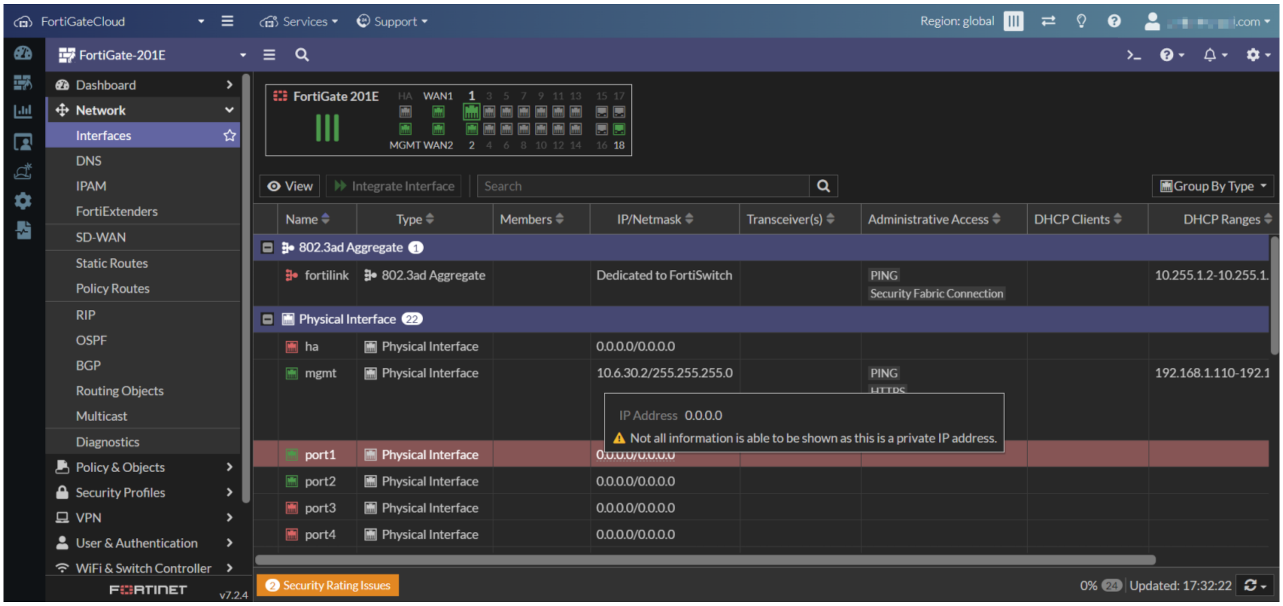
In this example, a FortiGate Cloud user with a paid subscription accesses the FortiGate remotely from FortiGate Cloud. When the user logs in with SSO, the profile has super_admin access. After the FortiGate Cloud user logs in, an administrator with super_admin access changes the permission of the FortiGate Cloud user to have prof_admin (read-only) access.

FortiGate Cloud must be accessed from a FortiGate Cloud 2.0 portal (also called FortiGate Cloud Premium) in order to have remote access using the FortiGate Cloud proxy. See Getting started with FortiGate Cloud 2.0 for more details.

To access a FortiGate remotely from FortiGate Cloud:

1. Log in to the FortiGate Cloud 2.0 portal.
2. Go to *Inventory* > *Asset List*. Select the desired FortiGate, then click *Remote Access*.

   FortiGate Cloud accesses the FortiGate using the FortiGate Cloud proxy and creates a super_admin user. The FortiOS interface is displayed in the current browser window.
3. Log out of FortiGate Cloud.
4. Update the FortiGate Cloud user permission to have prof_admin access:
   a. Log in to the FortiGate with a super_admin administrator account.
   b. Go to *System* > *Administrators* and edit the user in the *FortiGate Cloud SSO Administrator* section (*********@gmail.com*).
   c. Set *Administrator profile* to *Specify* and select *prof_admin*.
   d. Click *OK*.
5. Log in to the FortiGate Cloud 2.0 portal and access the FortiGate remotely again. Since the profile changed to prof_admin, they can only view items (such as interfaces).



Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch		PING Security Fabric Connection		10.255.1.2-10.255.1.
Physical Interface 22							
ha	Physical Interface		0.0.0.0/0.0.0.0				
mgmt	Physical Interface		10.6.30.2/255.255.255.0		PING HTTPS		192.168.1.110-192.1
port1	Physical Interface		0.0.0.0/0.0.0.0				
port2	Physical Interface		0.0.0.0/0.0.0.0				
port3	Physical Interface		0.0.0.0/0.0.0.0				
port4	Physical Interface		0.0.0.0/0.0.0.0				

IP Address 0.0.0.0
⚠ Not all information is able to be shown as this is a private IP address.

Display warnings for supported Fabric devices passing their hardware EOS date - 7.2.5

This information is also available in the FortiOS 7.2 Administration Guide:

- Downloading the EOS support package for supported Fabric devices

FortiGates, FortiSwitches, FortiAPs, and FortiExtenders can download an EOS (end of support) package automatically from FortiGuard during the bootup process or by using manual commands. Based on the downloaded EOS package files, when a device passes the EOS date, a warning message is displayed in the device's tooltip. The device is also highlighted in the following GUI locations:

- *System* > *Fabric Management* page
- *Security Fabric* > *Physical Topology* and *Logical Topology* pages
- *Security Fabric* > *Security Rating* page
- *Dashboard* > *Status* > *Security Fabric* widget
- *Dashboard* > *Status* > *System Information* widget

The End-of-Support security rating check rule audits the EOS of FortiGates and Fabric devices. This allows administrators to have clear visibility of their Security Fabric, and helps to prevent security gaps or vulnerabilities that may arise due to devices passing their hardware EOS date.

For more information about this feature, see Display warnings for supported Fabric devices passing their hardware EOS date.

Support checking for firmware updates daily when auto firmware upgrade is enabled - 7.2.6

When automatic firmware update is enabled, the FortiGate will check for firmware upgrades daily between a configured time interval. When a new patch release is available, a firmware upgrade will be scheduled. By actively searching for patch updates and performing patch upgrades, the system quality is improved as new security fixes are implemented and released.

You can define the installation delay using the `auto-firmware-upgrade-delay` command. This allows you to set the number of days before installing an automatic patch-level firmware upgrade from FortiGuard.

For more information about this feature, see Support checking for firmware updates daily when auto firmware upgrade is enabled.

Enable automatic firmware upgrades by default on entry-level FortiGates - 7.2.6

This information is also available in the FortiOS 7.2 Administration Guide:

- Automatic firmware upgrades on entry-level FortiGates

Automatic firmware upgrades are now enabled by default on entry-level FortiGates (lower than 100 series). Upgrades will be made to the next stable patch. However, if a FortiGate is part of a Fabric or managed by FortiManager, the `Automatic image upgrade` option is disabled.

For more information about this feature, see Enable automatic firmware upgrades by default on entry-level FortiGates.

Command to compute file hashes - 7.2.6

This information is also available in the FortiOS 7.2 Administration Guide:

- Computing file hashes

This command computes the SHA256 file hashes for all of the files in a directory or directories:

```
# diagnose sys filesystem hash <paths> -d [depth]
```

`<paths>`	Add up to 25 paths to show only the hash for the files at those paths.
`-d [depth]`	Specify the maximum depth of the traversal.

This command can be used for troubleshooting and debugging the system. The file hashes of system files can be compared against known good system files to help identify any compromises made on the system files.

For more information about this feature, see Command to compute file hashes.

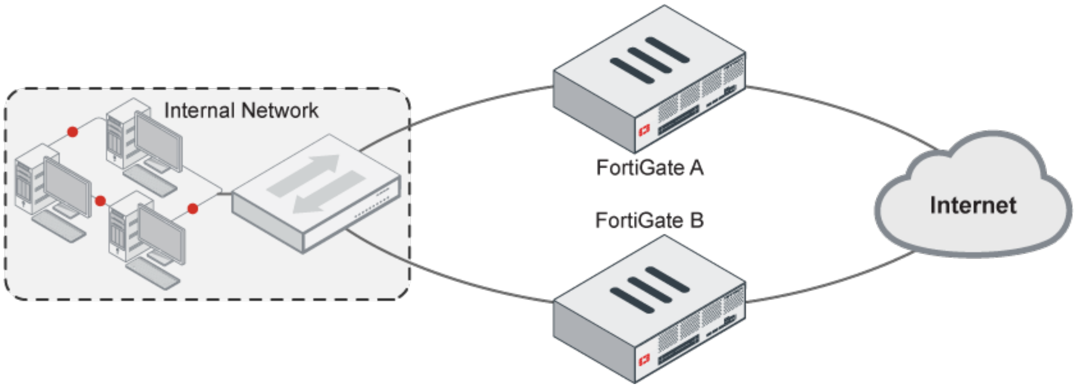
High availability

This section includes information about HA related new features:

- VRRP on EMAC-VLAN interfaces on page 269
- Abbreviated TLS handshake after HA failover on page 271
- HA failover support for ZTNA proxy sessions on page 272
- Add warnings when upgrading an HA cluster that is out of synchronization on page 275
- Support up to 30 virtual clusters on page 276
- Consolidate FGSP settings 7.2.1 on page 278
- FGSP per-tunnel failover for IPsec 7.2.1 on page 279
- FGCP over FGSP per-tunnel failover for IPsec 7.2.1 on page 285
- Allow IPsec DPD in FGSP members to support failovers 7.2.1 on page 294
- Applying the session synchronization filter only between FGSP peers in an FGCP over FGSP topology 7.2.1 on page 300

VRRP on EMAC-VLAN interfaces

Virtual Router Redundancy Protocol (VRRP) can be configured on EMAC-VLAN interfaces.



To configure the interfaces:

1. Configure FortiGate A:

```
config system interface
    edit "emac"
        set vdom "root"
        set ip 172.16.209.1 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm
        set type emac-vlan
        set vrrp-virtual-mac enable
        config vrrp
            edit 1
                set vrip 172.16.209.111
                set priority 200
            next
        end
        set snmp-index 61
        set interface "port1"
    next
end
```

2. Configure FortiGate B:

```
config system interface
    edit "emac"
        set vdom "root"
        set ip 172.16.209.2 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm
        set type emac-vlan
        set vrrp-virtual-mac enable
        config vrrp
            edit 1
                set vrip 172.16.209.111
                set priority 222
            next
        end
        set snmp-index 32
        set interface "port1"
    next
end
```

Check the VRRP information on the FortiGates:

Because FortiGate B has a higher priority, it is the primary device and FortiGate A is the backup.

1. FortiGate A:

```
# get router info vrrp
Interface: emac, primary IP address: 172.16.209.1
  UseVMAC: 1, SoftSW: 0, EmacVlan: 1 BrPortIdx: 0, PromiscCount: 0
  HA mode: primary (0:0:1) VRRP master number: 0
  VRID: 1 verion: 2
    vrip: 172.16.209.111, priority: 200 (200,0), state: BACKUP
    adv_interval: 1, preempt: 1, ignore_dft: 0 start_time: 3
    master_adv_interval: 100, accept: 1
    vrmac: 00:00:5e:00:01:01
    vrdst:
    vrgrp: 0
```

2. FortiGate B:

```
# get router info vrrp
Interface: emac, primary IP address: 172.16.209.2
  UseVMAC: 1, SoftSW: 0, EmacVlan: 1 BrPortIdx: 0, PromiscCount: 1
  HA mode: primary (0:0:1) VRRP master number: 1
  VRID: 1 verion: 2
    vrip: 172.16.209.111, priority: 222 (222,0), state: PRIMARY
    adv_interval: 1, preempt: 1, ignore_dft: 0 start_time: 3
    master_adv_interval: 100, accept: 1
    vrmac: 00:00:5e:00:01:01
    vrdst:
    vrgrp: 0
```

Abbreviated TLS handshake after HA failover

TLS sessions that pass through an HA A-A or A-P cluster can use an abbreviated TLS handshake instead of a full TLS handshake upon failover from a primary HA unit to a secondary HA unit. This reduces session pickup delays by reducing the time needed to renegotiate the TLS session, given that the TLS session ticket can be re-used.

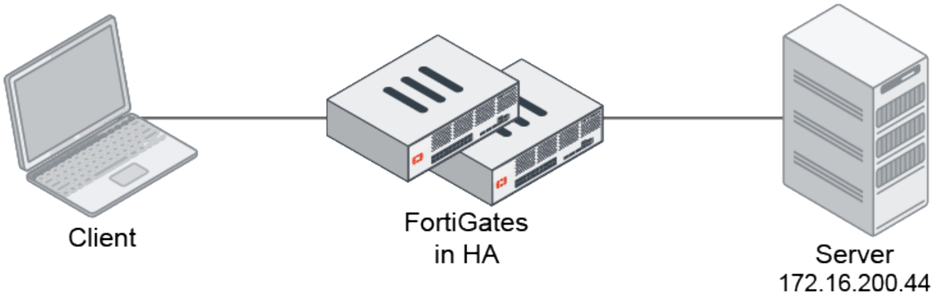
To accomplish this, FortiOS uses the web proxy global `ssl-ca-cert` to generate the key used in the TLS session ticket:

```
config web-proxy global
    set ssl-ca-cert "Fortinet_CA_SSL"
end
```

The certificate can be synchronized to the secondary HA unit, which allows the secondary unit to generate the same session key for a TLS session. When a TLS session reconnects after HA failover using the same session ticket as the first session, the new primary unit is able to generate the same key matching that session ticket and allow an abbreviated handshake.

Example

In this example, OpenSSL is used to create a TLS session between the client and the server through the primary FortiGate. The session ticket is outputted and saved. Upon failover, the same session ticket is reused to create a TLS session through the new primary unit. Because the new primary unit uses the same certificate to generate the key for the TLS session ticket, it allows the connection to be made using an abbreviated TLS handshake.



This example is for demonstration purposes only. In a normal failover, TLS sessions from clients will automatically be able to re-establish using an abbreviated handshake through the new primary unit.

To verify if an abbreviated TLS handshake is used after HA failover:

1. On the client using OpenSSL, open a new session to 172.16.200.44:443 and output the session ticket to a file called aaa.txt. This session will pass through the current HA primary unit:

   ```
   # openssl s_client -connect 172.16.200.44:443 -sess_out aaa.txt
   ```

2. Fail over the primary unit to the secondary unit. The HA secondary unit starts handling the traffic.
3. On the client, try connecting to 172.16.200.44:443 using the same saved session ticket as before (aaa.txt):

   ```
   # openssl s_client -connect 172.16.200.44:443 -sess_in aaa.txt
   ```

4. Verify whether the session succeeds in using the original session ticket:

   ```
   Reused, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
   Server public key is 4096 bit
   Secure Renegotiation IS NOT supported
   Compression: NONE
   Expansion: NONE
   No ALPN negotiated
   Early data was not sent
   Verify return code: 19 (self signed certificate in certificate chain)
   ...
   ```

   If the session is established using the same ticket, `Reused, TLSv1.3, Cipher is <name>` is displayed. If session is established using a new ticket, `New, TLSv1.3, Cipher is <name>` is displayed.

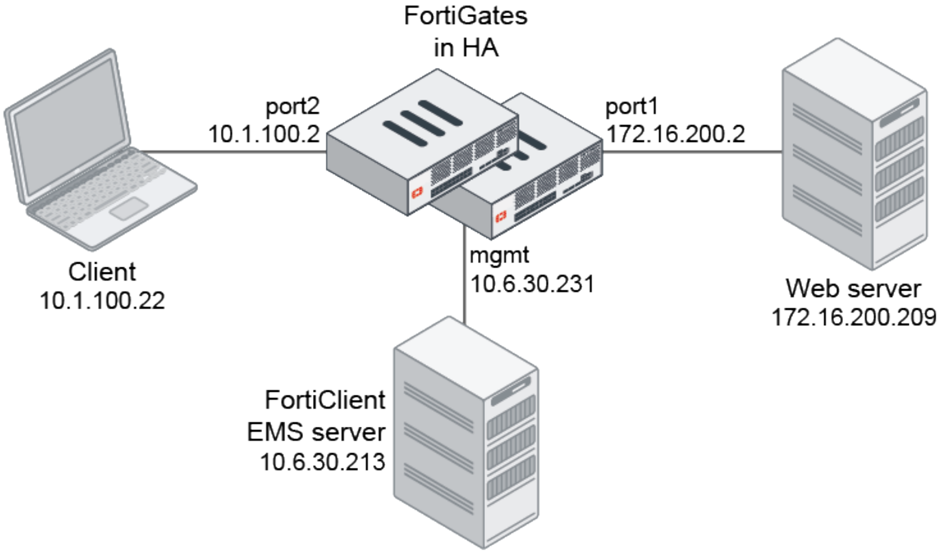
   The new primary is able to use the web proxy global `ssl-ca-cert` to generate the same key as the old primary that was used in the session ticket. So, the second TLS connection that reuses the TLS session ticket from the first session can complete an abbreviated TLS handshake.

HA failover support for ZTNA proxy sessions

User information and TLS sessions are synchronized between HA members for ZTNA proxy sessions. When a failover occurs, the new primary unit will continue allowing sessions from the logged in users without asking for the client certificate and re-authentication again.

Example

In this example, a FortiGate HA pair is acting as a ZTNA access proxy. Clients that are trying to access the web server on qa.test.com are proxied by the ZTNA access proxy. Remote clients must be registered to the EMS server, and pass a client certificate check and user authentication in order to connect. Upon HA member failure, a failover occurs and the new primary unit will continue to allow connections without requesting client certificate check and user authentication for existing users and devices.



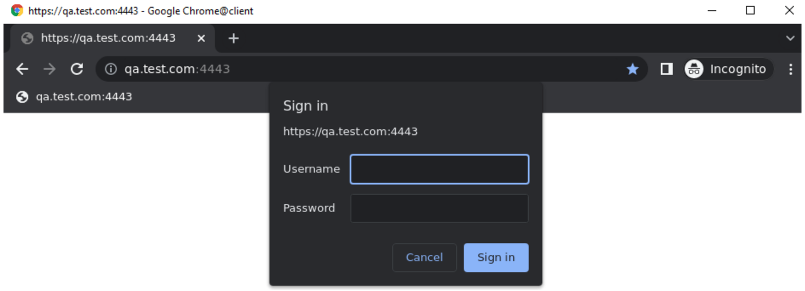
This example assumes ZTNA and EMS server settings are already configured.

To configure the HA settings:

```
config system ha
    set group-name "501E"
    set mode a-p
    set password **********
    set hbdev "ha" 0
    set session-pickup enable
    set override disable
    set monitor "port1" "port2"
end
```

To verify that the proxy sessions are synchronized between HA members:

1. On the client, access the web server. The ZTNA access proxy challenges the user for a client certificate and user authentication.



2. On the primary FortiGate, verify that the user information and TLS sessions are synchronized between HA members.
   a. Verify the list of proxy users:

```
501E-primary # diagnose wad user list
ID: 1, VDOM: root, IPv4: 10.1.100.22
  user name   : localuser1
  worker      : 0
  duration    : 8
  auth_type   : IP
  auth_method : Basic
  pol_id      : 1
  g_id        : 0
  user_based  : 1
  expire      : 597
  LAN:
    bytes_in=2093 bytes_out=5753
  WAN:
    bytes_in=2024 bytes_out=1235
```

   b. Apply a filter to WAD debug to diagnose the wad informer process:

```
501E-primary # diagnose test application wad 2400
Set diagnosis process: type=informer index=0 pid=305
```

   c. Show the user cache from the WAD informer. Verify that the localuser1 entry exists:

```
501E-primary # diagnose test application wad 110
users:
[1]     localuser1@10.1.100.22:0 upn_domain= from:worker worker:6 vf:0 ref:1 stale=0
ntlm:0, has_fsae:0, guest:0
                user_node:(0x7fe18dcf0048) user:1[max=65536](0x7fe18dd08048) ip:1
(0x7fe18dd00048) scheme:0 outofsync:0(0) id:1
...
```

   d. Verify using WAD real-time debugs on the secondary FortiGate. The user information is synchronized to the secondary FortiGate:

```
501E-secondary # diagnose wad debug enable category all
501E-secondary # diagnose wad debug enable level verbose
501E-secondary # diagnose debug enable
[I][p:296]              wad_proc_informer_ha_dgram_on_read:2811  Got HA msg: type=0,
sizeof(msg)=8, dlen=80, sz=88
[I][p:296]              wad_proc_informer_on_ha_user_add  :1493  reader:
ip=10.1.100.22:45852 vf=0 seq=0 grp_type=0 scheme=0 is_ntlm=0 has_fsae=0 concur_
user=65536 domain=''
[I][p:296]              wad_informer_update_user_ext      :782
ip=10.1.100.22:45852 name=localuser1 from=worker
[I][p:296]              wad_informer_find_user_ip_entries :621   find=false(1) vf=0
ip=10.1.100.22:45852 pr=(nil)
mapping user_node:0x7fc1c84dd048, user_ip:0x7fc1c84ed048(0), user:0x7fc1c84f5048(0).
```

3. Verify the user cache from the WAD informer:

```
501E-secondary # diagnose test application wad 110
users:
[1]     localuser1@10.1.100.22:0 upn_domain= from:worker worker:-126 vf:0 ref:1 stale=0
ntlm:0, has_fsae:0, guest:0
                user_node:(0x7fa3eb07d048) user:1[max=65536](0x7fa3eb095048) ip:1
```

```
(0x7fa3eb08d048) scheme:0 outofsync:0(0) id:7
...
```

If the client tries to access the web server again after failover occurs, the client certificate check and authentication prompt does not appear. ZTNA allows the traffic to pass.

The ZTNA logs for both FortiGates contain the same user information.

Primary FortiGate log:

```
1: date=2022-03-23 time=11:49:57 eventtime=1648061397548444970 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.1.100.22 srcname="client"
srcport=45826 srcintf="port2" srcintfrole="lan" dstcountry="Reserved" srccountry="Reserved"
dstip=172.16.200.209 dstport=443 dstintf="port1" dstintfrole="lan" sessionid=4786
service="HTTPS" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="ea7a8a04-a56e-51ec-9d7b-90d24b3a28e9" policyname="ztna" duration=5
user="localuser1" gatewayid=1 vip="ztna" accessproxy="ztna"
clientdeviceid="EF73C831C3FE4FF195A5B2030B******" clientdevicetags="FCTEMS8821000000_all_
registered_clients/MAC_FCTEMS8821000000_all_registered_clients/FCTEMS8821000000_ZT_FILE_
CERTFILE" wanin=2024 rcvdbyte=2024 wanout=1325 lanin=1511 sentbyte=1511 lanout=1075
fctuid="EF73C831C3FE4FF195A5B2030B******" unauthuser="fosqa" unauthusersource="forticlient"
appcat="unscanned"
```

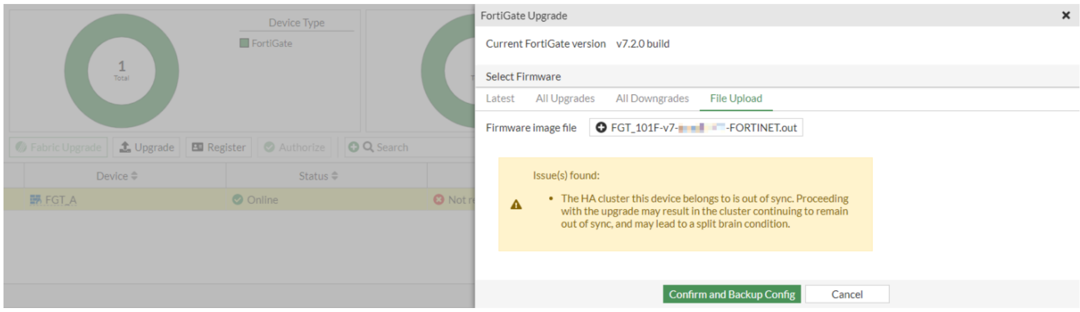
Secondary FortiGate log:

```
1: date=2022-03-23 time=11:55:01 eventtime=1648061701628425041 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.1.100.22 srcname="client"
srcport=45830 srcintf="port2" srcintfrole="lan" dstcountry="Reserved" srccountry="Reserved"
dstip=172.16.200.209 dstport=443 dstintf="port1" dstintfrole="lan" sessionid=676
service="HTTPS" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="ea7a8a04-a56e-51ec-9d7b-90d24b3a28e9" policyname="ztna" duration=5
user="localuser1" gatewayid=1 vip="ztna" accessproxy="ztna"
clientdeviceid="EF73C831C3FE4FF195A5B2030B******" clientdevicetags="FCTEMS8821000000_all_
registered_clients/MAC_FCTEMS8821000000_all_registered_clients/FCTEMS8821000000_ZT_FILE_
CERTFILE" wanin=2024 rcvdbyte=2024 wanout=1325 lanin=1511 sentbyte=1511 lanout=1075
fctuid="EF73C831C3FE4FF195A5B2030B******" unauthuser="fosqa" unauthusersource="forticlient"
appcat="unscanned"
```

Add warnings when upgrading an HA cluster that is out of synchronization

A warning is displayed in the GUI and CLI when upgrading a device in an HA cluster that is out of synchronization.

- GUI warning on the *System > Fabric Management* page:



FortiGate Upgrade

Current FortiGate version v7.2.0 build

Select Firmware

Firmware image file: FGT_101F-v7-[redacted]-FORTINET.out

Issue(s) found:

- The HA cluster this device belongs to is out of sync. Proceeding with the upgrade may result in the cluster continuing to remain out of sync, and may lead to a split brain condition.

- CLI warning:

  ```
  # execute restore image ftp <filename> <ftp_ip>
  This operation will replace the current firmware version!
  Do you want to continue? (y/n)y

  The HA cluster this device belongs to is out of sync. Proceeding with the upgrade may
  result in the cluster continuing to remain out of sync, and may lead to a split brain
  condition
  Do you want to continue? (y/n)
  ```

Support up to 30 virtual clusters

In FortiOS 7.2.0, up to 30 virtual clusters are supported, which allows more VDOMs to be spread across different virtual clusters without overlapping. Each virtual cluster supports its own failover conditions. Previously, only two virtual clusters were supported.

When configuring virtual clusters, the `group-id` is limited to a value from 0 to 7. If the HA `group-id` is greater than 7, use the command line first to change the `group-id` before enabling virtual clusters.

```
config system ha
    set group-id <integer>
end
```

⚠ When upgrading, old virtual clusters will be lost if the `group-id` is larger than 7.

Example

In this example, there are 30 customers managed by an MSSP on an HA cluster, and each customer VDOM needs to failover independently of other customer VDOMs. Each customer is assigned to a different virtual cluster with its own virtual cluster configurations. This may include different monitored interfaces, ping servers, and priority for the primary and secondary cluster members. Each virtual cluster will fail over according to their own virtual cluster configurations.

```
config system ha
    set vcluster-status enable
    config vcluster
        edit <id>
            set override {enable | disable}
            set priority <integer>
            set vdom <vdom_1>, ... <vdom_n>
            set monitor <interface_1>, ... <interface_n>
            set pingserver-monitor-interface <interface_1>, ... <interface_n>
        next
    end
end
```

`override {enable	disable}`	Enable/disable override and increase the priority of the unit that should always be the primary.
`priority <integer>`	Increase the priority to select the primary unit (0 - 255, default = 128).

`vdom <vdom_1>, ... <vdom_n>`	Set the virtual domains in the virtual cluster.
`monitor <interface_1>, ... <interface_n>`	Set the interfaces to check for port monitoring (or link failure).
`pingserver-monitor-interface <interface_1>, ... <interface_n>`	Set the interfaces to check for remote IP monitoring.

This example assumes an A-P cluster and VDOMs have already been configured. See HA active-passive cluster setup and Virtual domains in the FortiOS Administration Guide for more information.

For each virtual cluster, this example assumes that unit 1 has an HA priority of 200, while unit 2 has an HA priority of 100. By default, unit 1 will be the primary cluster member of all the virtual clusters.

To configure multiple virtual clusters in the GUI:

1. Go to *System* > *HA* and enable *VDOM Partitioning*.
2. Create a virtual cluster:
   a. In the table, click *Create New*. The *New Virtual Cluster* pane opens.
   b. Set the *Device priority* to *200*.
   c. Click the + and add the *Virtual domains*.
   d. Optionally, click the + and add the *Monitor interfaces*.
   e. Click *OK*.
3. Repeat step 2 to create the remaining virtual clusters.
4. Click *OK* to save the HA configuration. The *HA* page summary displays the multiple virtual clusters, each with a *Primary* and *Secondary* HA member.
5. Edit the priority settings for the secondary members to be 100:
   a. Select the *Secondary* member in the table, and click *Edit*.
   b. Set the *Priority* to *100*.
   c. Click *OK*.
6. Repeat step 5 for the remaining secondary members.

To configure multiple virtual clusters in the CLI:

1. Configure the primary FortiGate:

```
config system ha
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 200
            set vdom "vdom1"
        next
        edit 2
            set override disable
            set priority 200
            set vdom "vdom2"
        next
        ...
```

```
            edit 30
                set override disable
                set priority 200
                set vdom "vdom30"
            next
        end
    end
```

2. Configure the secondary FortiGate:

```
config system ha
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 100
            set vdom "vdom1"
        next
        edit 2
            set override disable
            set priority 100
            set vdom "vdom2"
        next
        ...
        edit 30
            set override disable
            set priority 100
            set vdom "vdom30"
        next
    end
end
```

Consolidate FGSP settings - 7.2.1

The FGSP settings are consolidated by moving the previous `config system cluster-sync` settings into a subtable under `config system standalone-cluster`. There are no changes to the FGSP behavior.

Old configuration	New configuration
`config system cluster-sync`	`config system standalone-cluster`
`    edit <id>`	`    config cluster-peer`
`        set peervd <VDOM>`	`        edit <id>`
`        set peerip <address>`	`            set peervd <VDOM>`
`        set syncvd <VDOM>`	`            set peerip <address>`
`        config session-sync-filter`	`            set syncvd <VDOM>`
`            ...`	`            config session-sync-filter`
`        end`	`                ...`
`    next`	`            end`
`end`	`        next`
	`    end`
	`end`

To configure FGSP:

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 1
    set layer2-connection available
    config cluster-peer
        edit 1
            set peerip 10.2.2.2
            config session-sync-filter
                set srcintf "port2"
                set dstintf "wan1"
                set srcaddr 10.1.100.0 255.255.255.0
                config custom-service
                    edit 3
                    next
                end
            end
        next
    end
end
```

FGSP per-tunnel failover for IPsec - 7.2.1

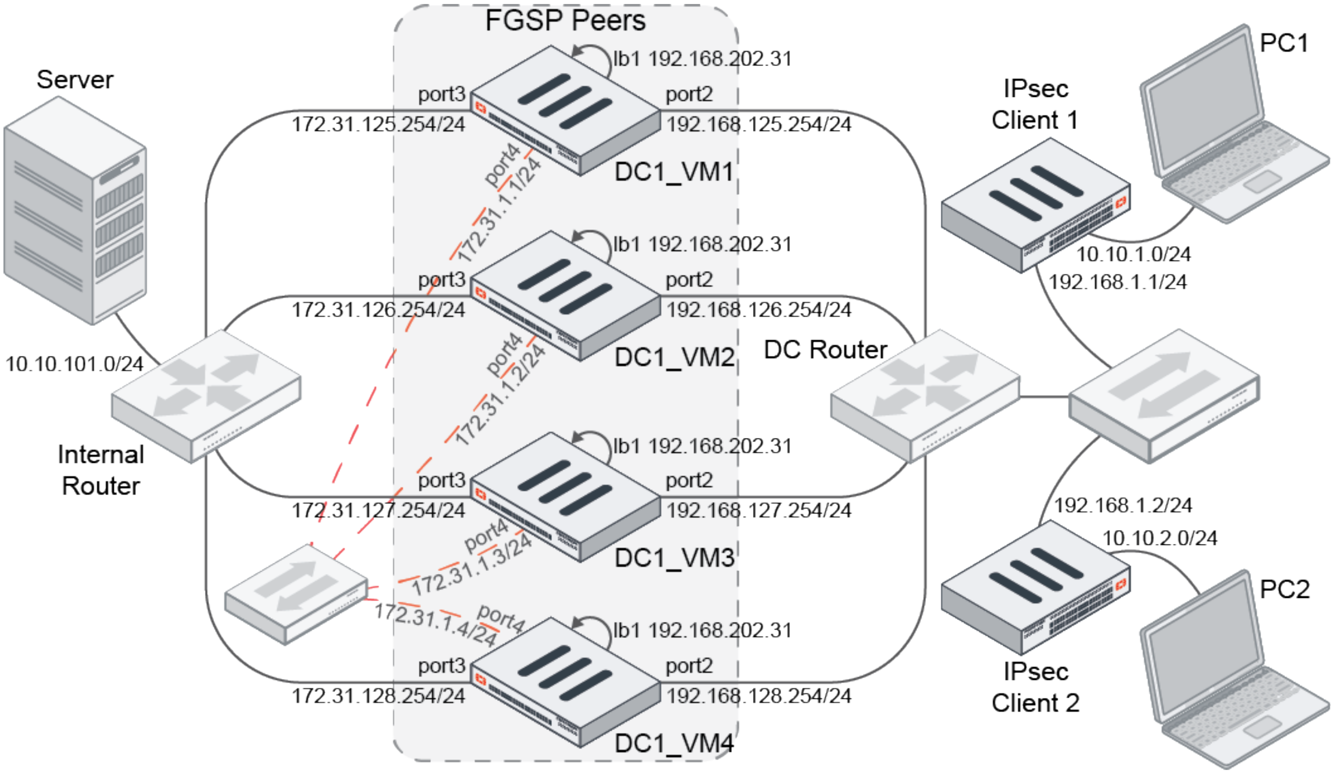
During FGSP per-tunnel failover for IPsec, the same IPsec dialup server configured on each FGSP member may establish tunnels with dialup clients as the primary gateway. The IPsec SAs are synchronized to all other FGSP peers that have FGSP synchronization for IPsec enabled. Other FGSP members may establish a tunnel with other clients on the same dialup server and synchronize their SAs to other peers.

Upon the failure of the FGSP member that is the primary gateway for a tunnel, the upstream router will fail over the tunnel traffic to another FGSP member. The other FGSP member will move from standby to the primary gateway for that tunnel and continue to forward traffic.

```
config vpn ipsec phase1-interface
    edit <name>
        set fgsp-sync {enable | disable}
    next
end
```

Example

In this example, the FGSP peers are connected on port4 over 172.31.1.1-4/24. Each peer has a loopback interface, lb1, with the same IP address. This loopback interface is used as the local gateway on each of the phase 1 connections to avoid each FGSP member having different IPs on port2. The DC Router uses ECMP to distribute traffic to each FGSP peer. It is assumed that the networking addresses are already configured properly.



Interface/setting	DC1_VM1	DC1_VM2	DC1_VM3	DC1_VM4
port2	192.168.125.254/24	192.168.126.254/24	192.168.127.254/24	192.168.128.254/24
port3	172.31.125.254/24	172.31.126.254/24	172.31.127.254/24	172.31.128.254/24
port4	172.31.1.1/24	172.31.1.2/24	172.31.1.3/24	172.31.1.4/24
lb1	192.168.202.31/32	192.168.202.31/32	192.168.202.31/32	192.168.202.31/32
`fgsp-sync`	Enabled	Enabled	Enabled	Disabled

Out of the four FGSP peers, DC1_VM1, DC1_VM2, and DC1_VM3 have `fgsp-sync` enabled in their IPsec phase 1 configurations. This allows the three FGSP members to synchronize IPsec SAs as clients establish dialup tunnels to them individually. DC1_VM4, which does not have `fgsp-sync` configured, will not participate in synchronizing IPsec SAs or establishing tunnels. The DC Router uses ECMP to route traffic to the destination 192.168.202.31 through each of the participating FGSP peers.

In a larger scale there may be many more IPsec dialup clients connecting, with each eligible FGSP peer being the primary gateway for a set of dialup tunnels, and is in standby for the rest of the tunnels. If an FGSP peer fails, traffic will fail over to other peers, and these peers will become primary gateways for the respective dialup tunnels.

To configure the FGSP peers (DC1_VM1):

The following steps are to configure DC1_VM1. The other peers have similar configurations based on the preceding table. In the `config vpn ipsec phase1-interface` settings, all peers should have the same local gateway external interface (192.168.202.31).

1. Configure the FGSP settings:

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 1
    config cluster-peer
        edit 1
            set peerip 172.31.1.2
        next
        edit 2
            set peerip 172.31.1.3
        next
        edit 3
            set peerip 172.31.1.4
        next
    end
end
```

2. Configure the VPN tunnel phase 1 settings:

```
config vpn ipsec phase1-interface
    edit "vpn1"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set local-gw 192.168.202.31
        set keylife 90000
        set peertype one
        set net-device disable
        set proposal aes128-sha1
        set dpd on-idle
        set dhgrp 2
        set fgsp-sync enable
        set nattraversal disable
        set peerid "Nokia_Peer"
        set psksecret xxxxx
        set dpd-retryinterval 60
    next
end
```

3. Configure the VPN tunnel phase 2 settings:

```
config vpn ipsec phase2-interface
    edit "vpn1"
        set phase1name "vpn1"
        set proposal aes128-sha1
        set keylifeseconds 10800
    next
end
```

To verify the configuration:

1. Once the FGSP members establish peering with each other, verify the standalone peers on DC1_VM1:

```
DC1_VM1 # diagnose sys ha standalone-peers
Group=1, ID=1
Detected-peers=3
Kernel standalone-peers: num=3.
```

```
peer0: vfid=0, peerip:port = 172.31.1.2:708, standalone_id=2
        session-type: send=0, recv=0
         packet-type: send=0, recv=0
peer1: vfid=0, peerip:port = 172.31.1.3:708, standalone_id=3
        session-type: send=0, recv=0
         packet-type: send=0, recv=0
peer2: vfid=0, peerip:port = 172.31.1.4:708, standalone_id=4
        session-type: send=0, recv=0
         packet-type: send=0, recv=0
Kernel standalone dev_base:
        standalone_id=0:
        standalone_id=1:
                phyindex=0: mac=00:0c:29:22:00:6b, linkfail=1
                phyindex=1: mac=00:0c:29:22:00:75, linkfail=1
                phyindex=2: mac=00:0c:29:22:00:7f, linkfail=1
                phyindex=3: mac=00:0c:29:22:00:89, linkfail=1
                phyindex=4: mac=00:0c:29:22:00:93, linkfail=1
                phyindex=5: mac=00:0c:29:22:00:9d, linkfail=1
                phyindex=6: mac=00:0c:29:22:00:a7, linkfail=1
                phyindex=7: mac=00:0c:29:22:00:b1, linkfail=1
                phyindex=8: mac=00:0c:29:22:00:bb, linkfail=1
                phyindex=9: mac=00:0c:29:22:00:c5, linkfail=1
        standalone_id=2:
                phyindex=0: mac=00:0c:29:06:4e:d6, linkfail=1
                phyindex=1: mac=00:0c:29:06:4e:e0, linkfail=1
                phyindex=2: mac=00:0c:29:06:4e:ea, linkfail=1
                phyindex=3: mac=00:0c:29:06:4e:f4, linkfail=1
                phyindex=4: mac=00:0c:29:06:4e:fe, linkfail=1
                phyindex=5: mac=00:0c:29:06:4e:08, linkfail=1
                phyindex=6: mac=00:0c:29:06:4e:12, linkfail=1
                phyindex=7: mac=00:0c:29:06:4e:1c, linkfail=1
                phyindex=8: mac=00:0c:29:06:4e:26, linkfail=1
                phyindex=9: mac=00:0c:29:06:4e:30, linkfail=1
        standalone_id=3:
                phyindex=0: mac=00:0c:29:70:b9:6c, linkfail=1
                phyindex=1: mac=00:0c:29:70:b9:76, linkfail=1
                phyindex=2: mac=00:0c:29:70:b9:80, linkfail=1
                phyindex=3: mac=00:0c:29:70:b9:8a, linkfail=1
                phyindex=4: mac=00:0c:29:70:b9:94, linkfail=1
                phyindex=5: mac=00:0c:29:70:b9:9e, linkfail=1
                phyindex=6: mac=00:0c:29:70:b9:a8, linkfail=1
                phyindex=7: mac=00:0c:29:70:b9:b2, linkfail=1
                phyindex=8: mac=00:0c:29:70:b9:bc, linkfail=1
                phyindex=9: mac=00:0c:29:70:b9:c6, linkfail=1
        standalone_id=4:
                phyindex=0: mac=00:0c:29:5c:d3:23, linkfail=1
                phyindex=1: mac=00:0c:29:5c:d3:2d, linkfail=1
                phyindex=2: mac=00:0c:29:5c:d3:37, linkfail=1
                phyindex=3: mac=00:0c:29:5c:d3:41, linkfail=1
                phyindex=4: mac=00:0c:29:5c:d3:4b, linkfail=1
                phyindex=5: mac=00:0c:29:5c:d3:55, linkfail=1
                phyindex=6: mac=00:0c:29:5c:d3:5f, linkfail=1
                phyindex=7: mac=00:0c:29:5c:d3:69, linkfail=1
                phyindex=8: mac=00:0c:29:5c:d3:73, linkfail=1
                phyindex=9: mac=00:0c:29:5c:d3:7d, linkfail=1
        standalone_id=5:
```

```
...
standalone_id=15:
```

2. Initiate a dialup tunnel connection from the IPsec Client 2 FortiGate (192.168.1.2).
3. Verify the tunnel list for vpn1_1 on each peer. The output shows the bi-directional SAs for that particular tunnel are synchronized to all participating FGSP peers.
   a. DC1_VM1:

```
DC1_VM1 # diagnose vpn tunnel list name vpn1_1
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=a4 192.168.202.31:0->192.168.1.2:0 tun_id=192.168.1.2 tun_
id6=::10.0.0.15 dst_mtu=1500 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8840 options
[2288]=npu rgwy-chg frag-rfc  run_state=0 role=sync-primary accept_traffic=1 overlay_
id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=6 olast=6 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=20
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=3 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=682 type=00 soft=0 mtu=1438 expire=10480/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=10788/10800
  dec: spi=a575b631 esp=aes key=16 5de449f75c7d70258f4972506dd164e2
       ah=sha1 key=20 7e65d641be6bc52655619ff542c67c61713de523
  enc: spi=10aa45b0 esp=aes key=16 65ad3b4849386deb4f3028079a657257
       ah=sha1 key=20 b5f1e1c6786f69482b5d271347a69a0cbb83ed58
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.1.2 npu_lgwy=192.168.202.31 npu_selid=b2 dec_npuid=0
enc_npuid=0
```

   b. DC1_VM2:

```
DC1_VM2 # diagnose vpn tunnel list name vpn1_1
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=a3 192.168.202.31:0->192.168.1.2:0 tun_id=192.168.1.2 tun_
id6=::10.0.0.15 dst_mtu=0 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options
[2208]=npu frag-rfc  run_state=0 role=standby accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=43063501 olast=43063501 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=3 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=682 type=00 soft=0 mtu=1280 expire=10466/0B replaywin=2048
       seqno=10000001 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_
len=1
  life: type=01 bytes=0/0 timeout=10788/10800
  dec: spi=a575b631 esp=aes key=16 5de449f75c7d70258f4972506dd164e2
       ah=sha1 key=20 7e65d641be6bc52655619ff542c67c61713de523
  enc: spi=10aa45b0 esp=aes key=16 65ad3b4849386deb4f3028079a657257
       ah=sha1 key=20 b5f1e1c6786f69482b5d271347a69a0cbb83ed58
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.1.2 npu_lgwy=192.168.202.31 npu_selid=ab dec_npuid=0
enc_npuid=0
```

c. DC1_VM3:

```
DC1_VM3 # diagnose vpn tunnel list name vpn1_1
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=ac 192.168.202.31:0->192.168.1.2:0 tun_id=192.168.1.2 tun_
id6=::10.0.0.15 dst_mtu=0 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options
[2208]=npu frag-rfc  run_state=0 role=standby accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=43063499 olast=43063499 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=2 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=682 type=00 soft=0 mtu=1280 expire=10462/0B replaywin=2048
       seqno=10000001 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_
len=1
  life: type=01 bytes=0/0 timeout=10788/10800
  dec: spi=a575b631 esp=aes key=16 5de449f75c7d70258f4972506dd164e2
       ah=sha1 key=20 7e65d641be6bc52655619ff542c67c61713de523
  enc: spi=10aa45b0 esp=aes key=16 65ad3b4849386deb4f3028079a657257
       ah=sha1 key=20 b5f1e1c6786f69482b5d271347a69a0cbb83ed58
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.1.2 npu_lgwy=192.168.202.31 npu_selid=b4 dec_npuid=0
enc_npuid=0
```

d. DC1_VM4:

```
DC1_VM4 # diagnose vpn tunnel list name vpn1_1
list ipsec tunnel by names in vd 0
```

The IPsec tunnel `role=sync-primary`on DC1_VM1 indicates that the IPsec tunnel was established on the FortiGate and traffic is being forwarded. On DC1_VM2 and DC1_VM3, the IPsec tunnel `role=standby` indicates that they are synchronized from the FGSP peer and are in standby for traffic forwarding.

The IPsec SAs do not synchronize to DC1_VM4 because `fgsp-sync` is disabled.

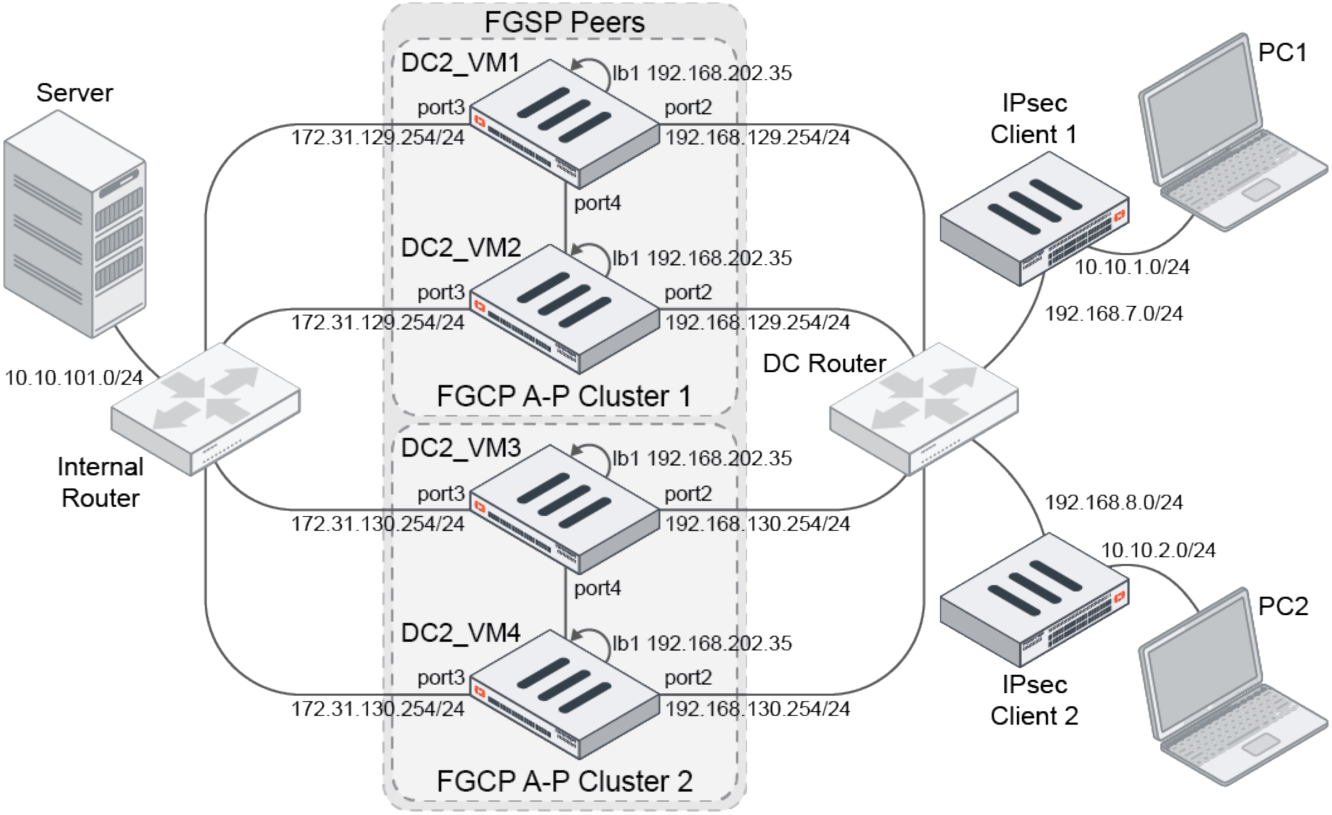
4. When a failure occurs on DC1_VM1, the tunnel traffic will fail over to either DC1_VM2 or DC1_VM3. Its tunnel role will become `role=sync-primary`.

FGCP over FGSP per-tunnel failover for IPsec - 7.2.1

For additional redundancy, an FGCP cluster on one site may form FGSP peering with FGCP clusters on other sites. The FGCP over FGSP peers can still synchronize IPsec SAs and act as the primary gateway for individual tunnels for the same dialup servers. When failover happens within an FGCP cluster, tunnel traffic will failover to the other FGCP cluster member. When an FGCP cluster fails, tunnel traffic will failover to the other FGSP peer.

Example

In this example, each FGCP A-P cluster is connected on port4 as the heartbeat interface. The FGSP peers are connected on port5 over 172.31.2.1-2/24. Each FGSP peer and FGCP cluster has a loopback interface, lb1, with the same IP address. This loopback interface is used as the local gateway on each of the phase 1 connections to avoid each FGSP member having different IPs on port2. The DC Router uses ECMP to distribute traffic to each FGSP peer. It is assumed that the networking addresses are already configured properly.



Interface/setting	DC2_VM1	DC2_VM2	DC2_VM3	DC2_VM4
port2	192.168.129.254/24	192.168.129.254/24	192.168.130.254/24	192.168.130.254/24
port3	172.31.129.254/24	172.31.129.254/24	172.31.130.254/24	172.31.130.254/24
port4	FGCP HA heartbeat interface	FGCP HA heartbeat interface	FGCP HA heartbeat interface	FGCP HA heartbeat interface
port5	172.31.2.1/24	172.31.2.1/24	172.31.2.2/24	172.31.2.2/24

Interface/setting	DC2_VM1	DC2_VM2	DC2_VM3	DC2_VM4
lb1	192.168.202.35/32	192.168.202.35/32	192.168.202.35/32	192.168.205.35/32
`fgsp-sync`	Enabled	Enabled	Enabled	Enabled

There are two pairs of FGCP A-P HA clusters that form FGSP peering with each other. This is a typical FGCP over FGSP configuration used in large enterprises and service provider environments where high redundancy is needed. Each cluster uses the same loopback address for the local gateway. The DC Router uses ECMP to route traffic to the destination 192.168.202.31 through each of the participating FGSP peers.

In a larger scale there may be many more members in the FGCP clusters, more FGSP peers, and more IPsec dialup clients connecting. Each eligible FGSP peer will be the primary gateway for a set of dialup tunnels, and is in standby for the rest of the tunnels. When the FGCP cluster is configured in A-P mode, the tunnels will be established on the primary unit and synchronized to the standby unit.

The following configurations and example demonstrates PC1 initiating traffic to the Server. First, a dialup tunnel is formed between FortiGate IPsec Client 1 and DC2_VM1, which allows traffic to go through. IPsec SAs are synchronized to the FGCP standby unit, and to the FGSP peer. Upon failure of DC2_VM1, DC2_VM2 takes over as the primary of the HA cluster, and assumes the primary role for the failover tunnels.

If both DC2_VM1 and DC2_VM2 fail, the tunnels that were formed on this FGSP peer will now be re-routed to the other FGSP peer. The primary FGCP cluster member, DC2_VM3, will now pick up the tunnel traffic and assume the primary role for the failover tunnels.

To configure the HA clusters:

1. Configure FGCP A-P Cluster 1 (use the same configuration for DC2_VM1 and DC2_VM2):

```
config system ha
    set group-id 1
    set group-name "DC2_VM12"
    set mode a-p
    set password ********
    set hbdev "port4" 50
    set session-pickup enable
    set uninterruptible-upgrade disable
    set override disable
    set priority 100
end
```

2. Configure FGCP A-P Cluster 2 (use the same configuration for DC2_VM3 and DC2_VM4):

```
config system ha
    set group-id 2
    set group-name "DC2_VM34"
    set mode a-p
    set password ********
    set hbdev "port4" 50
    set session-pickup enable
    set uninterruptible-upgrade disable
    set override disable
    set priority 100
end
```

To configure the FGSP peers:

1. Configure DC2_VM1:

   ```
   config system standalone-cluster
       set standalone-group-id 2
       set group-member-id 1
       config cluster-peer
           edit 1
               set peerip 172.31.2.2
           next
       end
   end
   ```

   The configuration is automatically synchronized to DC2_VM2.
2. Configure DC2_VM3:

   ```
   config system standalone-cluster
       set standalone-group-id 2
       set group-member-id 2
       config cluster-peer
           edit 1
               set peerip 172.31.2.1
           next
       end
   end
   ```

   The configuration is automatically synchronized to DC2_VM4.
3. To configure the IPsec VPN settings (use the same configuration for DC2_VM1 and DC2_VM3).
   1. Configure the VPN tunnel phase 1 settings:

      ```
      config vpn ipsec phase1-interface
          edit "vpn1"
              set type dynamic
              set interface "port2"
              set ike-version 2
              set local-gw 192.168.202.35
              set keylife 90000
              set peertype one
              set net-device disable
              set proposal aes128-sha1
              set add-route disable
              set dpd on-idle
              set dhgrp 2
              set fgsp-sync enable
              set nattraversal disable
              set peerid "Nokia_Peer"
              set psksecret ********
              set dpd-retryinterval 60
          next
      end
      ```

   2. Configure the VPN tunnel phase 2 settings:

      ```
      config vpn ipsec phase2-interface
          edit "vpn1"
              set phase1name "vpn1"
      ```

```
        set proposal aes128-sha1
        set keylifeseconds 10800
    next
end
```

To verify the configuration:

1. The FGCP HA cluster and the FGSP peering have formed. Verify the respective HA statuses.
   a. Verify the FGCP cluster status on DC2_VM1:

```
DC2_VM1 # diagnose sys ha status

HA information
Statistics
        traffic.local = s:0 p:439253 b:89121494
        traffic.total = s:0 p:440309 b:89242174
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80006, Mode=2 Group=1 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM02TM22000002:      Primary, serialno_prio=0, usr_priority=100, hostname=DC2_VM2
FGVM02TM22000001:    Secondary, serialno_prio=1, usr_priority=200, hostname=DC2_VM1

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.1, primary_id=0
FGVM02TM22000002:      Primary, ha_prio/o_ha_prio=0/0
FGVM02TM22000001:    Secondary, ha_prio/o_ha_prio=1/1
```

   b. Verify the FGSP peering status on DC2_VM1:

```
DC2_VM1 # diagnose sys ha standalone-peers
Group=2, ID=1
Detected-peers=1
Kernel standalone-peers: num=1.
peer0: vfid=0, peerip:port = 172.31.2.2:708, standalone_id=2
        session-type: send=3, recv=4
         packet-type: send=0, recv=0
Kernel standalone dev_base:
        standalone_id=0:
        standalone_id=1:
                phyindex=0: mac=00:0c:29:fc:a3:17, linkfail=1
                phyindex=1: mac=00:0c:29:fc:a3:21, linkfail=1
                phyindex=2: mac=00:0c:29:fc:a3:2b, linkfail=1
                phyindex=3: mac=00:0c:29:fc:a3:35, linkfail=1
                phyindex=4: mac=00:0c:29:fc:a3:3f, linkfail=1
                phyindex=5: mac=00:0c:29:fc:a3:49, linkfail=1
                phyindex=6: mac=00:0c:29:fc:a3:53, linkfail=1
                phyindex=7: mac=00:0c:29:fc:a3:5d, linkfail=1
                phyindex=8: mac=00:0c:29:fc:a3:67, linkfail=1
                phyindex=9: mac=00:0c:29:fc:a3:71, linkfail=1
        standalone_id=2:
                phyindex=0: mac=00:09:0f:09:02:00, linkfail=1
                phyindex=1: mac=00:09:0f:09:02:01, linkfail=1
                phyindex=2: mac=00:09:0f:09:02:02, linkfail=1
                phyindex=3: mac=00:09:0f:09:02:03, linkfail=1
                phyindex=4: mac=00:09:0f:09:02:04, linkfail=1
                phyindex=5: mac=00:09:0f:09:02:05, linkfail=1
                phyindex=6: mac=00:09:0f:09:02:06, linkfail=1
                phyindex=7: mac=00:09:0f:09:02:07, linkfail=1
                phyindex=8: mac=00:09:0f:09:02:08, linkfail=1
                phyindex=9: mac=00:09:0f:09:02:09, linkfail=1
        standalone_id=3:
        ...
        standalone_id=15:
```

c. Verify the FGCP cluster status on DC2_VM3:

```
DC2_VM3 # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:443999 b:89037989
        traffic.total = s:0 p:445048 b:89157373
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80006, Mode=2 Group=2 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM02TM22000004:      Primary, serialno_prio=0, usr_priority=100, hostname=DC2_VM4
FGVM02TM22000003:    Secondary, serialno_prio=1, usr_priority=200, hostname=DC2_VM3

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.1, primary_id=0
FGVM02TM22000004:      Primary, ha_prio/o_ha_prio=0/0
FGVM02TM22000003:    Secondary, ha_prio/o_ha_prio=1/1
```

d. Verify the FGSP peering status on DC2_VM3:

```
DC2_VM3 # diagnose sys ha standalone-peers
Group=2, ID=2
Detected-peers=1
Kernel standalone-peers: num=1.
peer0: vfid=0, peerip:port = 172.31.2.1:708, standalone_id=1
        session-type: send=2, recv=6
         packet-type: send=0, recv=0
Kernel standalone dev_base:
        standalone_id=0:
        standalone_id=1:
                phyindex=0: mac=00:09:0f:09:01:00, linkfail=1
                phyindex=1: mac=00:09:0f:09:01:01, linkfail=1
                phyindex=2: mac=00:09:0f:09:01:02, linkfail=1
                phyindex=3: mac=00:09:0f:09:01:03, linkfail=1
                phyindex=4: mac=00:09:0f:09:01:04, linkfail=1
                phyindex=5: mac=00:09:0f:09:01:05, linkfail=1
                phyindex=6: mac=00:09:0f:09:01:06, linkfail=1
                phyindex=7: mac=00:09:0f:09:01:07, linkfail=1
                phyindex=8: mac=00:09:0f:09:01:08, linkfail=1
                phyindex=9: mac=00:09:0f:09:01:09, linkfail=1
        standalone_id=2:
                phyindex=0: mac=00:0c:29:bb:77:af, linkfail=1
                phyindex=1: mac=00:0c:29:bb:77:b9, linkfail=1
                phyindex=2: mac=00:0c:29:bb:77:c3, linkfail=1
                phyindex=3: mac=00:0c:29:bb:77:cd, linkfail=1
                phyindex=4: mac=00:0c:29:bb:77:d7, linkfail=1
                phyindex=5: mac=00:0c:29:bb:77:e1, linkfail=1
                phyindex=6: mac=00:0c:29:bb:77:eb, linkfail=1
                phyindex=7: mac=00:0c:29:bb:77:f5, linkfail=1
                phyindex=8: mac=00:0c:29:bb:77:ff, linkfail=1
                phyindex=9: mac=00:0c:29:bb:77:09, linkfail=1
        standalone_id=3:
        ...
        standalone_id=15:
```

2. Initiate traffic from PC1 to the Server. This initiates a tunnel from the IPsec Client 1 FortiGate to DC2_VM1.
3. Verify the tunnel list for vpn1_1 on each peer.
   a. DC2_VM1:

```
DC2_VM1 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=4 192.168.202.35:0->192.168.7.2:0 tun_id=192.168.7.2 tun_
id6=::10.0.0.4 dst_mtu=1500 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8840 options
[2288]=npu rgwy-chg frag-rfc  run_state=0 role=sync-primary accept_traffic=1 overlay_
id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=41 olast=41 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=156
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=602 type=00 soft=0 mtu=1438 expire=1424/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=10791/10800
  dec: spi=37f426a1 esp=aes key=16 3671c9303b6295fc73b11765811bdf96
       ah=sha1 key=20 41b98cb541dc9c76311ddec4b23584ee35d31915
  enc: spi=10aa4d3a esp=aes key=16 cc8529ee16de6e4ac42b0ce506d7cdd1
       ah=sha1 key=20 0c2d9edd0fdbe45942cf718ac2ebb4d59c2760c6
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.7.2 npu_lgwy=192.168.202.35 npu_selid=1c dec_npuid=0
enc_npuid=0
```

   b. DC2_VM2:

```
DC2_VM2 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=4 192.168.202.35:0->192.168.7.2:0 tun_id=192.168.7.2 tun_
id6=::10.0.0.4 dst_mtu=0 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options
```

```
[2208]=npu frag-rfc  run_state=0 role=standby accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=42975898 olast=42975898 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=602 type=00 soft=0 mtu=1280 expire=1325/0B replaywin=2048
       seqno=10000001 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_
len=1
  life: type=01 bytes=0/0 timeout=10791/10800
  dec: spi=37f426a1 esp=aes key=16 3671c9303b6295fc73b11765811bdf96
       ah=sha1 key=20 41b98cb541dc9c76311ddec4b23584ee35d31915
  enc: spi=10aa4d3a esp=aes key=16 cc8529ee16de6e4ac42b0ce506d7cdd1
       ah=sha1 key=20 0c2d9edd0fdbe45942cf718ac2ebb4d59c2760c6
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.7.2 npu_lgwy=192.168.202.35 npu_selid=1c dec_npuid=0
enc_npuid=0
```

c. DC2_VM3:

```
DC2_VM3 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=4 192.168.202.35:0->192.168.7.2:0 tun_id=192.168.7.2 tun_
id6=::10.0.0.4 dst_mtu=0 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options
[2208]=npu frag-rfc  run_state=0 role=standby accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=42975982 olast=42975982 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=602 type=00 soft=0 mtu=1280 expire=1215/0B replaywin=2048
       seqno=10000001 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_
len=1
  life: type=01 bytes=0/0 timeout=10791/10800
  dec: spi=37f426a1 esp=aes key=16 3671c9303b6295fc73b11765811bdf96
       ah=sha1 key=20 41b98cb541dc9c76311ddec4b23584ee35d31915
  enc: spi=10aa4d3a esp=aes key=16 cc8529ee16de6e4ac42b0ce506d7cdd1
       ah=sha1 key=20 0c2d9edd0fdbe45942cf718ac2ebb4d59c2760c6
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.7.2 npu_lgwy=192.168.202.35 npu_selid=1c dec_npuid=0
enc_npuid=0
```

d. DC2_VM4:

```
DC2_VM4 # diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
```

```
------------------------------------------------------
name=vpn1_1 ver=2 serial=4 192.168.202.35:0->192.168.7.2:0 tun_id=192.168.7.2 tun_
id6=::10.0.0.4 dst_mtu=0 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options
[2208]=npu frag-rfc  run_state=0 role=standby accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=42975768 olast=42975768 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=602 type=00 soft=0 mtu=1280 expire=1433/0B replaywin=2048
       seqno=10000001 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_
len=1
  life: type=01 bytes=0/0 timeout=10791/10800
  dec: spi=37f426a1 esp=aes key=16 3671c9303b6295fc73b11765811bdf96
       ah=sha1 key=20 41b98cb541dc9c76311ddec4b23584ee35d31915
  enc: spi=10aa4d3a esp=aes key=16 cc8529ee16de6e4ac42b0ce506d7cdd1
       ah=sha1 key=20 0c2d9edd0fdbe45942cf718ac2ebb4d59c2760c6
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.7.2 npu_lgwy=192.168.202.35 npu_selid=1c dec_npuid=0
enc_npuid=0
```

The IPsec tunnel `role=sync-primary`on DC2_VM1 indicates that it is being used to carry IPsec traffic. On DC2_VM2, DC2_VM3, and DC2_VM4, the IPsec tunnel `role=standby` indicates that they are in standby for traffic forwarding.

To test failover scenarios:

1. Verify the sniffer trace on DC2_VM1 before FGCP HA failover:

   ```
   DC2_VM1 # diagnose sniffer packet any icmp 4
   Using Original Sniffing Mode
   interfaces=[any]
   filters=[icmp]
   0.171753 vpn1 in 10.10.1.2 -> 10.10.101.2: icmp: echo request
   0.171763 port3 out 10.10.1.2 -> 10.10.101.2: icmp: echo request
   0.171941 port3 in 10.10.101.2 -> 10.10.1.2: icmp: echo reply
   0.171947 vpn1 out 10.10.101.2 -> 10.10.1.2: icmp: echo reply
   ```

   Traffic passes through DC2_VM1.
2. Reboot the primary FortiGate, DC2_VM1.
3. Verify the sniffer trace on DC2_VM2 after FGCP HA failover:

   ```
   DC2_VM2 # diagnose sniffer packet any icmp 4
   Using Original Sniffing Mode
   interfaces=[any]
   filters=[icmp]
   0.111107 vpn1 in 10.10.1.2 -> 10.10.101.2: icmp: echo request
   0.111118 port3 out 10.10.1.2 -> 10.10.101.2: icmp: echo request
   0.111293 port3 in 10.10.101.2 -> 10.10.1.2: icmp: echo reply
   0.111298 vpn1 out 10.10.101.2 -> 10.10.1.2: icmp: echo reply
   ```

```
^C
16 packets received by filter
0 packets dropped by kernel
```

Traffic passes through DC2_VM2.

4. Verify the tunnel list for vpn1_1 on DC2_VM2:

```
DC2_VM2 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=4 192.168.202.35:0->192.168.7.2:0 tun_id=192.168.7.2 tun_
id6=::10.0.0.4 dst_mtu=1500 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8840 options[2288]=npu
rgwy-chg frag-rfc  run_state=0 role=sync-primary accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=58 txp=31 rxb=4872 txb=2604
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=169
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=3 serial=3
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=602 type=00 soft=0 mtu=1438 expire=10730/0B replaywin=2048
       seqno=20 esn=0 replaywin_lastseq=0000003b qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=10790/10800
  dec: spi=37f426c1 esp=aes key=16 ef61b49078b6ab3e00a4d3a048d779f5
       ah=sha1 key=20 ee2e8de9c522d89b6481c37faa73a7bb54163645
  enc: spi=10aa4d58 esp=aes key=16 4cb95f12657ca8e269b9f8a25f9b19c1
       ah=sha1 key=20 326744c4e5b4a0758397725464593d94ba9390dc
  dec:pkts/bytes=116/9744, enc:pkts/bytes=62/7316
  npu_flag=00 npu_rgwy=192.168.7.2 npu_lgwy=192.168.202.35 npu_selid=1e dec_npuid=0 enc_
npuid=0
```

The role has changed to `role=sync-primary`.

5. Shut down DC2_VM1 and the DC2_VM2 IPsec uplink interface.
6. Verify the sniffer trace on DC2_VM3. As expected, traffic now passes through DC2_VM3:

```
DC2_VM3 # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.165088 vpn1 in 10.10.1.2 -> 10.10.101.2: icmp: echo request
0.165102 port3 out 10.10.1.2 -> 10.10.101.2: icmp: echo request
0.165294 port3 in 10.10.101.2 -> 10.10.1.2: icmp: echo reply
0.165301 vpn1 out 10.10.101.2 -> 10.10.1.2: icmp: echo reply
^C
14 packets received by filter
0 packets dropped by kernel
```

7. Verify the tunnel list for vpn1_1 on DC2_VM3:

```
DC2_VM3 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=4 192.168.202.35:0->192.168.7.2:0 tun_id=192.168.7.2 tun_
```

```
id6=::10.0.0.4 dst_mtu=1500 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options[2208]=npu
frag-rfc  run_state=0 role=sync-primary accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=53 txp=53 rxb=4452 txb=4452
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=3 serial=3
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=602 type=00 soft=0 mtu=1438 expire=10347/0B replaywin=2048
       seqno=10000155 esn=0 replaywin_lastseq=000001b0 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=10790/10800
  dec: spi=37f426c1 esp=aes key=16 ef61b49078b6ab3e00a4d3a048d779f5
       ah=sha1 key=20 ee2e8de9c522d89b6481c37faa73a7bb54163645
  enc: spi=10aa4d58 esp=aes key=16 4cb95f12657ca8e269b9f8a25f9b19c1
       ah=sha1 key=20 326744c4e5b4a07583977254645 93d94ba9390dc
  dec:pkts/bytes=88/7392, enc:pkts/bytes=88/10384
  npu_flag=00 npu_rgwy=192.168.7.2 npu_lgwy=192.168.202.35 npu_selid=1e dec_npuid=0 enc_
npuid=0
```

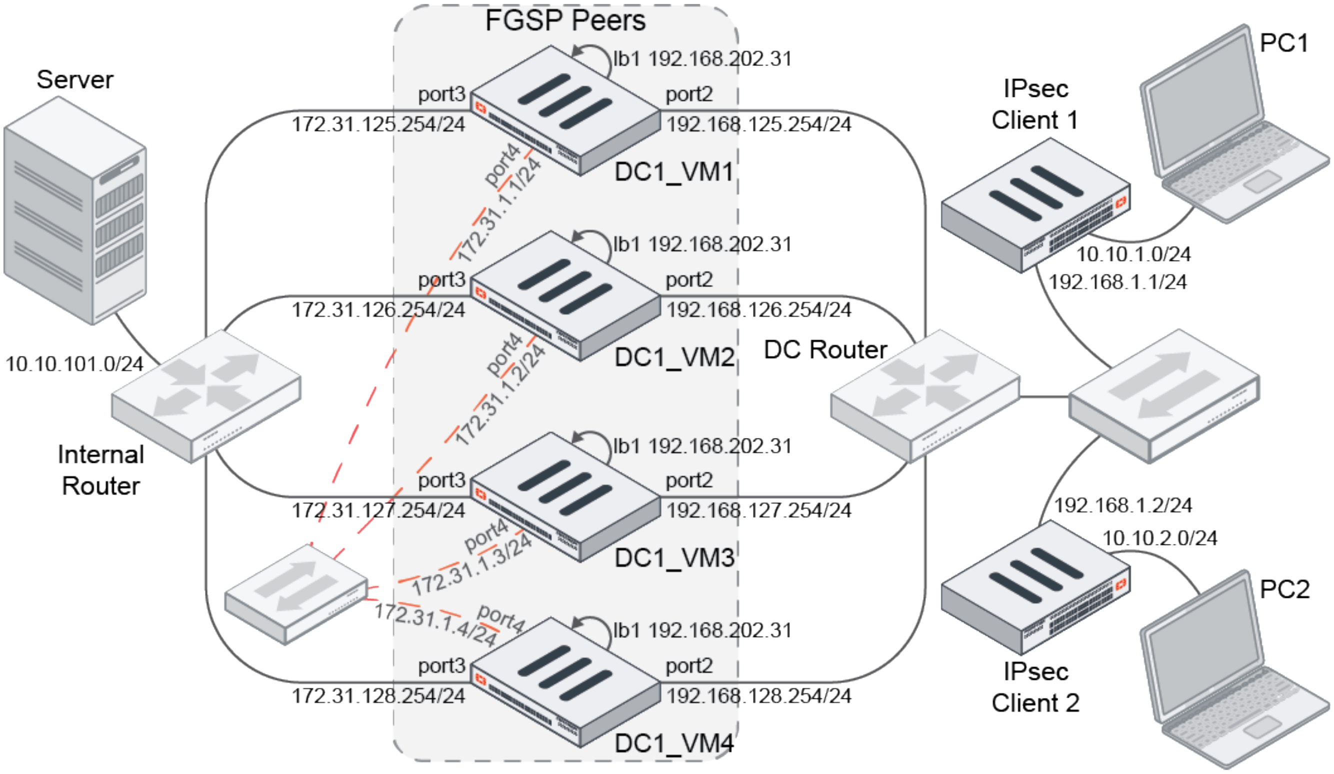
The role has changed to `role=sync-primary`.

Allow IPsec DPD in FGSP members to support failovers - 7.2.1

In conjunction with support for FGSP per-tunnel failover for IPsec 7.2.1 on page 279, configuring DPD (dead peer detection) on an FGSP member is permitted. This allows a failed FGSP member to send out DPD probes during failover to detect unreachable remote peers and to flush the corresponding tunnels.

Example

In this example, using the same configuration as in FGSP per-tunnel failover for IPsec 7.2.1 on page 279, a tunnel can be established from one of the remote IPsec clients to one of the FGSP members (DC1_VM1). DPD can be set to `on-idle`, with a configured `dpd-retryinterval` of 60 seconds. When a client disappears, whether it is due to remote client failures or server-side routing failures, the FGSP member or gateway (DC1_VM1) will send out DPD probes for detection. Once the three iterations are complete and no responses are detected, the FGSP member will flush the tunnel and remove any routing to that peer.



Interface/setting	DC1_VM1	DC1_VM2	DC1_VM3	DC1_VM4
port2	192.168.125.254/24	192.168.126.254/24	192.168.127.254/24	192.168.128.254/24
port3	172.31.125.254/24	172.31.126.254/24	172.31.127.254/24	172.31.128.254/24
port4	172.31.1.1/24	172.31.1.2/24	172.31.1.3/24	172.31.1.4/24
lb1	192.168.202.31/32	192.168.202.31/32	192.168.202.31/32	192.168.202.31/32
`fgsp-sync`	Enabled	Enabled	Enabled	Disabled

To configure the FGSP peers (DC1_VM1):

The following steps are to configure DC1_VM1. The other peers have similar configurations based on the preceding table. In the `config vpn ipsec phase1-interface` settings, all peers should have the same local gateway external interface (192.168.202.31). For DC1_VM4, `fgsp-sync` is disabled in the VPN tunnel phase 1 settings.

1. Configure the FGSP settings:

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 1
    config cluster-peer
        edit 1
            set peerip 172.31.1.2
        next
        edit 2
            set peerip 172.31.1.3
        next
        edit 3
            set peerip 172.31.1.4
        next
    end
end
```

2. Configure the VPN tunnel phase 1 settings:

```
config vpn ipsec phase1-interface
    edit "vpn1"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set local-gw 192.168.202.31
        set keylife 90000
        set peertype one
        set net-device disable
        set proposal aes128-sha1
        set dpd on-idle
        set dhgrp 2
        set fgsp-sync enable
        set nattraversal disable
        set peerid "Nokia_Peer"
        set psksecret xxxxx
        set dpd-retryinterval 60
    next
end
```

3. Configure the VPN tunnel phase 2 settings:

```
config vpn ipsec phase2-interface
    edit "vpn1"
        set phase1name "vpn1"
        set proposal aes128-sha1
        set keylifeseconds 10800
    next
end
```

To verify the configuration:

1. Once the FGSP members establish peering with each other, verify the standalone peers on DC1_VM1:

```
DC1_VM1 # diagnose sys ha standalone-peers
Group=1, ID=1
Detected-peers=3
Kernel standalone-peers: num=3.
peer0: vfid=0, peerip:port = 172.31.1.2:708, standalone_id=2
        session-type: send=0, recv=0
         packet-type: send=0, recv=0
peer1: vfid=0, peerip:port = 172.31.1.3:708, standalone_id=3
        session-type: send=0, recv=0
         packet-type: send=0, recv=0
peer2: vfid=0, peerip:port = 172.31.1.4:708, standalone_id=4
        session-type: send=0, recv=0
         packet-type: send=0, recv=0
```

```
Kernel standalone dev_base:
        standalone_id=0:
        standalone_id=1:
                phyindex=0: mac=00:0c:29:22:00:6b, linkfail=1
                phyindex=1: mac=00:0c:29:22:00:75, linkfail=1
                phyindex=2: mac=00:0c:29:22:00:7f, linkfail=1
                phyindex=3: mac=00:0c:29:22:00:89, linkfail=1
                phyindex=4: mac=00:0c:29:22:00:93, linkfail=1
                phyindex=5: mac=00:0c:29:22:00:9d, linkfail=1
                phyindex=6: mac=00:0c:29:22:00:a7, linkfail=1
                phyindex=7: mac=00:0c:29:22:00:b1, linkfail=1
                phyindex=8: mac=00:0c:29:22:00:bb, linkfail=1
                phyindex=9: mac=00:0c:29:22:00:c5, linkfail=1
        standalone_id=2:
                phyindex=0: mac=00:0c:29:06:4e:d6, linkfail=1
                phyindex=1: mac=00:0c:29:06:4e:e0, linkfail=1
                phyindex=2: mac=00:0c:29:06:4e:ea, linkfail=1
                phyindex=3: mac=00:0c:29:06:4e:f4, linkfail=1
                phyindex=4: mac=00:0c:29:06:4e:fe, linkfail=1
                phyindex=5: mac=00:0c:29:06:4e:08, linkfail=1
                phyindex=6: mac=00:0c:29:06:4e:12, linkfail=1
                phyindex=7: mac=00:0c:29:06:4e:1c, linkfail=1
                phyindex=8: mac=00:0c:29:06:4e:26, linkfail=1
                phyindex=9: mac=00:0c:29:06:4e:30, linkfail=1
        standalone_id=3:
                phyindex=0: mac=00:0c:29:70:b9:6c, linkfail=1
                phyindex=1: mac=00:0c:29:70:b9:76, linkfail=1
                phyindex=2: mac=00:0c:29:70:b9:80, linkfail=1
                phyindex=3: mac=00:0c:29:70:b9:8a, linkfail=1
                phyindex=4: mac=00:0c:29:70:b9:94, linkfail=1
                phyindex=5: mac=00:0c:29:70:b9:9e, linkfail=1
                phyindex=6: mac=00:0c:29:70:b9:a8, linkfail=1
                phyindex=7: mac=00:0c:29:70:b9:b2, linkfail=1
                phyindex=8: mac=00:0c:29:70:b9:bc, linkfail=1
                phyindex=9: mac=00:0c:29:70:b9:c6, linkfail=1
        standalone_id=4:
                phyindex=0: mac=00:0c:29:5c:d3:23, linkfail=1
                phyindex=1: mac=00:0c:29:5c:d3:2d, linkfail=1
                phyindex=2: mac=00:0c:29:5c:d3:37, linkfail=1
                phyindex=3: mac=00:0c:29:5c:d3:41, linkfail=1
                phyindex=4: mac=00:0c:29:5c:d3:4b, linkfail=1
                phyindex=5: mac=00:0c:29:5c:d3:55, linkfail=1
                phyindex=6: mac=00:0c:29:5c:d3:5f, linkfail=1
                phyindex=7: mac=00:0c:29:5c:d3:69, linkfail=1
                phyindex=8: mac=00:0c:29:5c:d3:73, linkfail=1
                phyindex=9: mac=00:0c:29:5c:d3:7d, linkfail=1
        standalone_id=5:
        ...
        standalone_id=15:
```

2. Initiate a dialup tunnel connection from the IPsec Client 2 FortiGate (192.168.1.2).
3. Verify the tunnel list for vpn1_1 on each peer.
   a. DC1_VM1:

   ```
   DC1_VM1 # diagnose vpn tunnel list name vpn1_1
   list ipsec tunnel by names in vd 0
   ```

```
------------------------------------------------------
name=vpn1_1 ver=2 serial=a4 192.168.202.31:0->192.168.1.2:0 tun_id=192.168.1.2 tun_
id6=::10.0.0.15 dst_mtu=1500 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8840 options
[2288]=npu rgwy-chg frag-rfc  run_state=0 role=sync-primary accept_traffic=1 overlay_
id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=6 olast=6 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=20
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=3 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=682 type=00 soft=0 mtu=1438 expire=10480/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=10788/10800
  dec: spi=a575b631 esp=aes key=16 5de449f75c7d70258f4972506dd164e2
       ah=sha1 key=20 7e65d641be6bc52655619ff542c67c61713de523
  enc: spi=10aa45b0 esp=aes key=16 65ad3b4849386deb4f3028079a657257
       ah=sha1 key=20 b5f1e1c6786f69482b5d271347a69a0cbb83ed58
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.1.2 npu_lgwy=192.168.202.31 npu_selid=b2 dec_npuid=0
enc_npuid=0
```

b. DC1_VM2:

```
DC1_VM2 # diagnose vpn tunnel list name vpn1_1
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=a3 192.168.202.31:0->192.168.1.2:0 tun_id=192.168.1.2 tun_
id6=::10.0.0.15 dst_mtu=0 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options
[2208]=npu frag-rfc  run_state=0 role=standby accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=43063501 olast=43063501 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=3 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=682 type=00 soft=0 mtu=1280 expire=10466/0B replaywin=2048
       seqno=10000001 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_
len=1
  life: type=01 bytes=0/0 timeout=10788/10800
  dec: spi=a575b631 esp=aes key=16 5de449f75c7d70258f4972506dd164e2
       ah=sha1 key=20 7e65d641be6bc52655619ff542c67c61713de523
  enc: spi=10aa45b0 esp=aes key=16 65ad3b4849386deb4f3028079a657257
       ah=sha1 key=20 b5f1e1c6786f69482b5d271347a69a0cbb83ed58
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.1.2 npu_lgwy=192.168.202.31 npu_selid=ab dec_npuid=0
enc_npuid=0
```

c. DC1_VM3:

```
DC1_VM3 # diagnose vpn tunnel list name vpn1_1
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=vpn1_1 ver=2 serial=ac 192.168.202.31:0->192.168.1.2:0 tun_id=192.168.1.2 tun_
id6=::10.0.0.15 dst_mtu=0 dpd-link=on weight=1
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/8712 options
[2208]=npu frag-rfc  run_state=0 role=standby accept_traffic=1 overlay_id=0

parent=vpn1 index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=43063499 olast=43063499 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=vpn1 proto=0 sa=1 ref=2 serial=2 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.1.0-10.10.1.255:0
  SA:  ref=3 options=682 type=00 soft=0 mtu=1280 expire=10462/0B replaywin=2048
       seqno=10000001 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_
len=1
  life: type=01 bytes=0/0 timeout=10788/10800
  dec: spi=a575b631 esp=aes key=16 5de449f75c7d70258f4972506dd164e2
       ah=sha1 key=20 7e65d641be6bc52655619ff542c67c61713de523
  enc: spi=10aa45b0 esp=aes key=16 65ad3b4849386deb4f3028079a657257
       ah=sha1 key=20 b5f1e1c6786f69482b5d271347a69a0cbb83ed58
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=192.168.1.2 npu_lgwy=192.168.202.31 npu_selid=b4 dec_npuid=0
enc_npuid=0
```

4. When a shut down occurs on the VPN client to vpn1_2, verify the IKE debug messages on DC1_VM2. There are three iterations of DPD probes:

```
DC1_VM2 # diagnose debug enable
DC1_VM2 # diagnose debug application ike -1
...
ike 0:vpn1_2: link is idle 6 192.168.202.31->192.168.4.2:0 dpd=1 seqno=72 rr=0
ike 0:vpn1_2:171: send IKEv2 DPD probe, seqno 114
ike 0:vpn1_2:158: sending NOTIFY msg
ike 0:vpn1_2:171:158: send informational
ike 0:vpn1_2:171: sent IKE msg (INFORMATIONAL): 192.168.202.31:500->192.168.4.2:500,
len=76, vrf=0, id=87458c81a3be17f9/c8db7d3f2c70e638:00000004
ike 0: comes 192.168.1.2:500->192.168.202.31:500,ifindex=6,vrf=0...
ike 0:vpn1_2: link is idle 6 192.168.202.31->192.168.4.2:0 dpd=1 seqno=72 rr=0
ike 0:vpn1_2:171: send IKEv2 DPD probe, seqno 114
ike 0:vpn1_2:158: sending NOTIFY msg
ike 0:vpn1_2:171:158: send informational
ike 0:vpn1_2:171: sent IKE msg (INFORMATIONAL): 192.168.202.31:500->192.168.4.2:500,
len=76, vrf=0, id=87458c81a3be17f9/c8db7d3f2c70e638:00000004
ike 0: comes 192.168.1.2:500->192.168.202.31:500,ifindex=6,vrf=0....
ike 0:vpn1_2: link is idle 6 192.168.202.31->192.168.4.2:0 dpd=1 seqno=72 rr=0
ike 0:vpn1_2:171: send IKEv2 DPD probe, seqno 114
ike 0: comes 192.168.1.2:500->192.168.202.31:500,ifindex=6,vrf=0....
ike 0:vpn1_2:171: 87458c81a3be17f9/c8db7d3f2c70e638 negotiation of IKE SA failed due to
retry timeout
ike 0:vpn1_2:171: expiring IKE SA 87458c81a3be17f9/c8db7d3f2c70e638
ike 0:vpn1_2: deleting
ike 0:vpn1_2: flushing
ike 0:vpn1_2: deleting IPsec SA with SPI 85700354
ike 0:vpn1_2:vpn1: deleted IPsec SA with SPI 85700354, SA count: 0
ike 0:vpn1_2: sending SNMP tunnel DOWN trap for vpn1
ike 0:vpn1_2: sending tunnel down event for addr 10.10.4.0
ike 0:vpn1_2:vpn1: delete
ike 0:vpn1:152: del route 10.10.4.0/255.255.255.0 tunnel 192.168.4.2 oif vpn1(21) metric
15 priority 1
ike 0:vpn1_2: flushed
ike 0:vpn1_2:171: HA send IKE SA del 87458c81a3be17f9/c8db7d3f2c70e638
ike 0:vpn1_2:171:159: send informational
ike 0:vpn1_2:171: sent IKE msg (INFORMATIONAL): 192.168.202.31:500->192.168.4.2:500,
len=76, vrf=0, id=87458c81a3be17f9/c8db7d3f2c70e638:00000005
ike 0:vpn1_2: delete dynamic
ike 0:vpn1_2: deleted
```

Applying the session synchronization filter only between FGSP peers in an FGCP over FGSP topology - 7.2.1

This enhancement ensures that session synchronization happens correctly in an FGCP over FGSP topology:

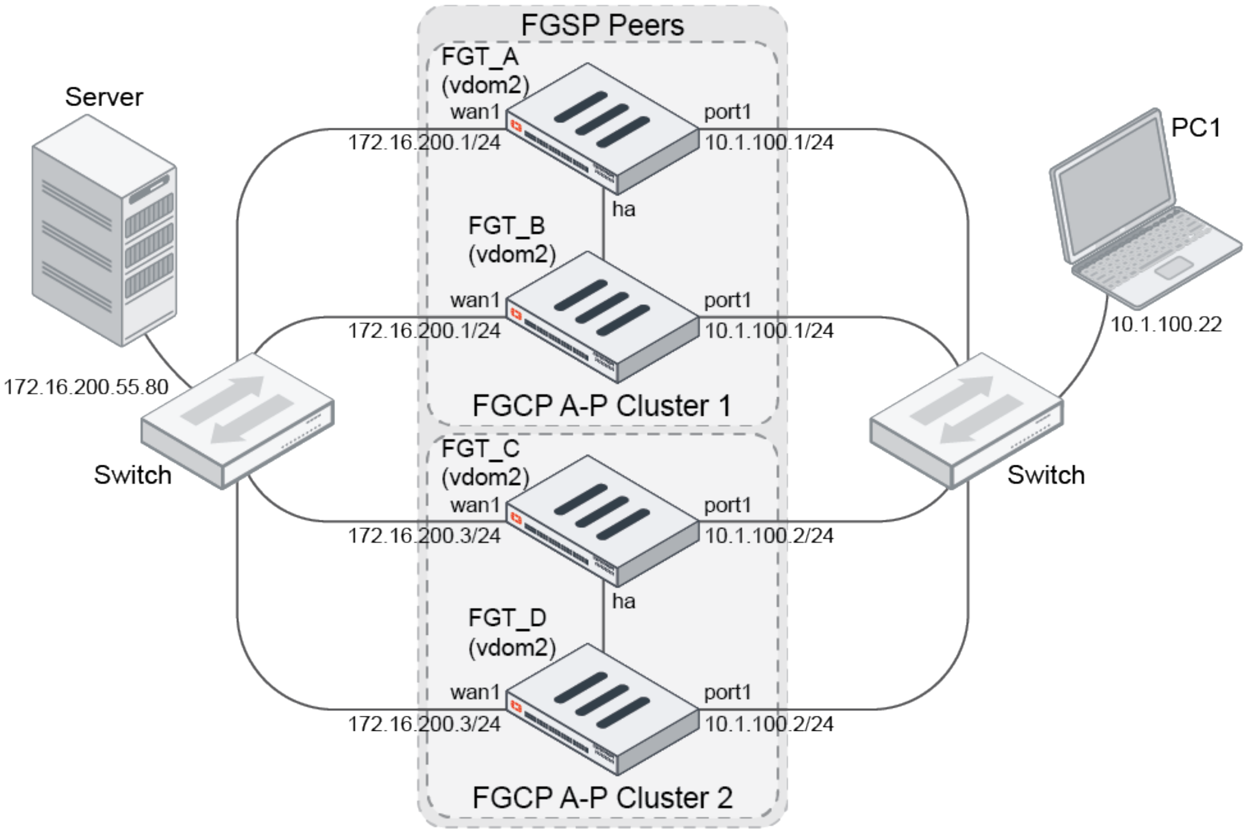
- When the session synchronization filter is applied on FGSP, the filter will only affect sessions synchronized between the FGSP peers.
- When virtual clustering is used, sessions synchronized between each virtual cluster can also be synchronized to FGSP peers. All peers' `syncvd` must be in the same HA virtual cluster.

Example

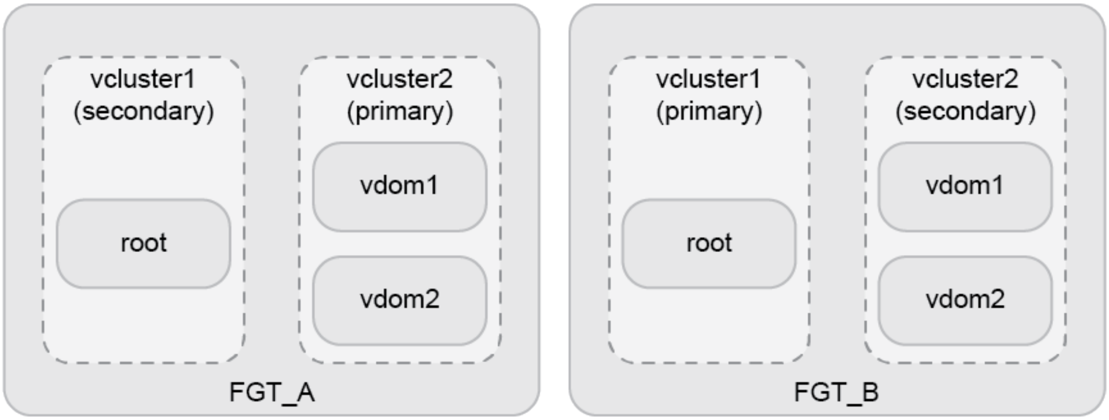
In this example, there is a simplified configuration where there is no router or load balancer performing balancing between the FGSP peers, but it demonstrates the following:

- When sessions pass through FGCP A-P Cluster 1, all sessions are synchronized between the FGT_A and FGT_B regardless of the session synchronization filter.
- Session synchronization between the FGSP peers (FGCP A-P Cluster 1 and 2) only occurs for the service specified in the filter, which is HTTP/80.
- The preceding behavior is applicable when virtual clustering is configured. This example focuses on vdom2, which belongs to vcluster2. FGT_A is the primary for vcluster2.

Each FGSP A-P cluster is connected on ha as the FGCP cluster heartbeat device. The FGSP peers are connected on mgmt over 10.1.1.1-2/24.



Virtual clustering between FGT_A and FGT_B:



Interface	FGT_A	FGT_B	FGT_C	FGT_D
wan1	172.16.200.1/24	172.16.200.1/24	172.16.200.3/24	172.16.200.3/24
port1	10.1.100.1/24	10.1.100.1/24	10.1.100.2/24	10.1.100.2/24
mgmt	10.1.1.1/24	10.1.1.1/24	10.1.1.2/24	10.1.1.2/24
ha	FGCP cluster heartbeat device		FGCP cluster heartbeat device	

To configure the HA clusters:

1. Configure FGCP A-P Cluster 1 (use the same configuration for FGT_A and FGT_B):

```
config system ha
    set group-id 146
    set group-name "FGT_HA1"
    set mode a-p
    set hbdev "wan2" 100 "ha" 50
    set session-pickup enable
    set vcluster-status enable
    config vcluster
        edit 1
            set override enable
            set priority 25
            set monitor "wan1" "port1"
            set vdom "root"
        next
        edit 2
            set override disable
            set priority 150
            set monitor "wan1"
            set vdom "vdom2" "vdom1"
        next
    end
end
```

2. Configure FGCP A-P Cluster 2 (use the same configuration for FGT_C and FGT_D):

```
config system ha
    set group-id 200
    set group-name "FGT_HA2"
    set mode a-p
    set hbdev "wan2" 100 "ha" 50
    set session-pickup enable
    set vcluster-status enable
    config vcluster
        edit 1
            set override enable
            set priority 120
            set monitor "wan1" "port1"
            set vdom "root"
        next
        edit 2
            set override disable
            set priority 150
            set monitor "wan1"
            set vdom "vdom2" "vdom1"
        next
    end
end
```

To configure the FGSP peers:

1. Configure FGT_A:

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 1
    config cluster-peer
        edit 1
            set peervd "vdom2"
            set peerip 10.1.1.2
            set syncvd "vdom2"
            config session-sync-filter
                config custom-service
                    edit 1
                        set dst-port-range 80-80
                    next
                end
            end
        next
    end
end
```

   The configuration is automatically synchronized to FGT_B.

2. Configure FGT_C:

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 2
    config cluster-peer
        edit 1
            set peervd "vdom2"
            set peerip 10.1.1.1
            set syncvd "vdom2"
            config session-sync-filter
                config custom-service
                    edit 1
                        set dst-port-range 80-80
                    next
                end
            end
        next
    end
end
```

   The configuration is automatically synchronized to FGT_D.

To verify the configuration:

1. Verify the FGSP peer information on Cluster 1:

```
FGT_A (global) # diagnose sys ha fgsp-zone
Local standalone-member-id: 1
FGSP peer_num = 1
        peer[1]: standalone-member-id=2, IP=10.1.1.2, vd=vdom2, prio=1
```

2. Verify the FGSP peer information on Cluster 2:

```
FGT_C (global) # diagnose sys ha fgsp-zone
Local standalone-member-id: 1
FGSP peer_num = 1
        peer[1]: standalone-member-id=1, IP=10.1.1.1, vd=vdom2, prio=1
```

3. Initiate two sessions, HTTP and SSH.
4. Verify that the HTTP session is synchronized from Cluster 1 to Cluster 2.
   a. Verify the session list of vdom2 on FGT_A:

```
FGT_A (vdom2) # diagnose sys session list

session info: proto=6 proto_state=01 duration=693 expire=3593 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=1:0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu synced f00
statistic(bytes/packets/allow_err): org=87531/1678/1 reply=7413876/6043/1 tuples=2
tx speed(Bps/kbps): 134/1 rx speed(Bps/kbps): 11357/90
orgin->sink: org pre->post, reply pre->post dev=11->7/7->11
gwy=172.16.200.55/10.1.100.22
hook=post dir=org act=snat 10.1.100.22:44260->172.16.200.55:80(172.16.200.1:44260)
hook=pre dir=reply act=dnat 172.16.200.55:80->172.16.200.1:44260(10.1.100.22:44260)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=7 pol_uuid_idx=579 auth_info=0 chk_client_info=0 vd=2
serial=000a79df tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=66/70, ipid=70/66,
vlan=0x0000/0x0000
vlifid=70/66, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=1/0

session info: proto=6 proto_state=01 duration=326 expire=3589 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=1:0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu synced f00
statistic(bytes/packets/allow_err): org=4721/41/1 reply=5681/36/1 tuples=2
tx speed(Bps/kbps): 14/0 rx speed(Bps/kbps): 17/0
orgin->sink: org pre->post, reply pre->post dev=11->7/7->11
gwy=172.16.200.55/10.1.100.22
hook=post dir=org act=snat 10.1.100.22:50234->172.16.200.55:22(172.16.200.1:50234)
hook=pre dir=reply act=dnat 172.16.200.55:22->172.16.200.1:50234(10.1.100.22:50234)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=7 pol_uuid_idx=579 auth_info=0 chk_client_info=0 vd=2
serial=000a7d90 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=66/70, ipid=70/66,
vlan=0x0000/0x0000
vlifid=70/66, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=6/6
total session 2
```

b. Verify the session list of vdom2 on FGT_B:

```
FGT_B (vdom2) # diagnose sys session list

session info: proto=6 proto_state=01 duration=736 expire=3100 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=1:0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty npu f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->7/7->11 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.1.100.22:44260->172.16.200.55:80(172.16.200.1:44260)
hook=pre dir=reply act=dnat 172.16.200.55:80->172.16.200.1:44260(10.1.100.22:44260)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=7 pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=2
serial=000a79df tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:

session info: proto=6 proto_state=01 duration=369 expire=3230 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=1:0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty npu f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->7/7->11 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.1.100.22:50234->172.16.200.55:22(172.16.200.1:50234)
hook=pre dir=reply act=dnat 172.16.200.55:22->172.16.200.1:50234(10.1.100.22:50234)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=7 pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=2
serial=000a7d90 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
total session 2
```

c. Verify the session list of vdom2 on FGT_C:

```
FGT_C (vdom2) # diagnose sys session filter dst 172.16.200.55
FGT_C (vdom2) # diagnose sys session filter src 10.1.100.22
FGT_C (vdom2) # diagnose sys session list

session info: proto=6 proto_state=01 duration=837 expire=2762 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
```

```
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=1:0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty npu f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->7/7->11 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.1.100.22:44260->172.16.200.55:80(172.16.200.1:44260)
hook=pre dir=reply act=dnat 172.16.200.55:80->172.16.200.1:44260(10.1.100.22:44260)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=7 pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=2
serial=000a79df tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
total session 1
```

d. Verify the session list of vdom2 on FGT_D:

```
FGT-D (vdom2) # diagnose sys session filter dst 172.16.200.55
FGT-D (vdom2) # diagnose sys session filter src 10.1.100.22
FGT-D (vdom2) # diagnose sys session list

session info: proto=6 proto_state=01 duration=902 expire=2697 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=1:0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty npu f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->7/7->11 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.1.100.22:44260->172.16.200.55:80(172.16.200.1:44260)
hook=pre dir=reply act=dnat 172.16.200.55:80->172.16.200.1:44260(10.1.100.22:44260)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=7 pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=2
serial=000a79df tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
total session 1
```

Session synchronization filters are designed to be configured symmetrically on all of the FGSP peers. In cases where the filters are configured asymmetrically, note the following differences:

- In an FGCP over FGSP topology, session filtering will be applied on the FGSP peer that has the filtering configured and is receiving the session synchronization.
- In an FGSP topology between standalone peers, the filtering will be applied on the FGSP peer that has the filtering configured and is sending out the session synchronization.

FortiGuard

This section includes information about FortiGuard related new features:

FDS-only ISDB package in firmware images

FortiOS firmware images include Fortinet objects in the built-in Internet Service Database (ISDB).

```
# diagnose firewall internet-service list
List internet service in kernel(global):
Internet Service Database Kernel Table: size 14974 bytes, Entry size 5844 bytes, number of
index entries 165 number of IP range entries 0

Group(0): Weight(15), number of entries(162)
......
```

This lightweight ISDB package allows firewall rules and policy routes that use ISDB to access FortiGuard servers to continue working after upgrading FortiOS. For example, the following policy will work after an upgrade:

```
config firewall policy
    edit 440
        set name "Fortinet Updates"
        set srcintf "port25"
        set dstintf "port1"
        set srcaddr "FortiAnalyzer" "FortiAuthenticator" "Tesla Management Interface"
"BackupFortinet" "SipFW" "ConnectVPNMgmt"
        set internet-service enable
        set internet-service-id 1245187 1245326 1245324 1245325 1245193 1245192 1245190
1245185
        set action accept
        set schedule "always"
        set logtraffic all
        set fsso disable
    next
end
```

After the FortiGate reboots after a firmware update, an automatic update will run in five minutes so that the FortiGate can get the ISDB, whether or not scheduled update is enabled.

```
# diagnose autoupdate versions | grep Internet -A 6

Internet-service Full Database
---------
Version: 7.02217 signed
Contract Expiry Date: n/a
Last Updated using manual update on Thu Mar 10 12:06:58 2022
Last Update Attempt: Thu Mar 10 12:07:27 2022
```

Verifying and accepting signed AV and IPS packages

AV and IPS packages are now signed by the Fortinet CA to ensure authenticity of the packages. The FortiGate will execute the following checks based on the method used to perform updates:

- During automatic updates, only signed and validated packages are accepted.
- During manual package updates, signed and validated packages will be accepted. If a package is not signed, the following applies:
  - Level-0: accept the new package even if it is unsigned.
  - Level-1: display a warning and request a user confirmation to accept.
  - Level-2: display an error and reject the image.
  - If no level is configured, apply Level-1.
- For HA and configuration synchronization, the secondary device will synchronize signature files from the primary in the presence of a saved signed package.

Security levels are pre-configured on the BIOS.

The FortiGuard Distribution Network (FDN) will maintain signed and unsigned packages for 7.2 and pre-7.2 compatibility. FortiManagers used for package distribution will also download signed and unsigned packages for backwards compatibility.

All AV and IPS packages are forced to use the signature (others packages are optional):

- APPDB
- AVDB
- AVEN
- DBDB
- FLDB
- FLEN
- ISDB
- MMDB
- MUDB
- NIDS

When checking the versions of updated objects, verified versions are labeled as `signed`.

To verify the status for all object signatures:

```
# diagnose autoupdate signature check-all
aven(7,28) signature is valid.
virdb(2,2) signature is valid.
etdb(2,7) signature is valid.
exdb(2,4) signature is valid.
avai(2,19) signature is valid.
fcni(9,0) signature check passed.
contract(10,0) signature check passed.
idsen(30,78) signature is valid.
ipscfgscr(30,50) signature is missing.
fldb(34,2) signature is valid.
idsdb(4,24) signature is valid.
idsetdb(4,26) signature is valid.
idsurldb(5,1) signature is valid.
appdb(38,1) signature is valid.
isdb(39,1) signature is valid.
geoip(28,0) signature check passed.
```

```
ffdb_low(31,11) signature is valid.
ffdb_med(31,9) signature is valid.
ffdb_high(31,10) signature is valid.
uwdb(32,1) signature check passed.
certdb(33,0) signature check passed.
mmdb(35,1) signature is valid.
dnsbot(36,1) signature is valid.
sfas(40,0) signature check passed.
mcdb(42,1) signature check passed.
anphipats(49,1) signature check passed.
update objects signature check finished.
```

To verify the status for all object versions:

```
# diagnose autoupdate versions

AV Engine
---------
Version: 6.00272 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using scheduled update on Wed Feb 23 00:48:25 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates

Virus Definitions
---------
Version: 89.09892 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Wed Feb 23 11:34:52 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: Updates Installed

Extended set
---------
Version: 89.09892 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Wed Feb 23 11:34:52 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: Updates Installed

Mobile Malware Definitions
---------
Version: 89.09892 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Wed Feb 23 11:34:52 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: Updates Installed

IPS Attack Engine
---------
Version: 7.00208 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Tue Feb 22 23:51:15 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates
...
```

```
Attack Definitions
---------
Version: 19.00264 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Wed Feb 23 00:06:22 2022
Last Update Attempt: Wed Feb 23 05:10:23 2022
Result: No Updates

Attack Extended Definitions
---------
Version: 19.00264 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Tue Feb 22 23:51:15 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates

Application Definitions
---------
Version: 19.00262 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Tue Feb 22 23:51:15 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates

Industrial Attack Definitions
---------
Version: 19.00262 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Tue Feb 22 23:51:15 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates

IPS Malicious URL Database
---------
Version: 3.00272 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Tue Feb 22 23:51:15 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates

Flow-based Virus Definitions
---------
Version: 89.09892 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Wed Feb 23 11:34:52 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: Updates Installed

Botnet Domain Database
---------
Version: 2.00935 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using manual update on Tue Feb 22 23:51:15 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates
```

```
Internet-service Full Database
---------
Version: 7.02162 signed
Contract Expiry Date: n/a
Last Updated using manual update on Fri Feb  4 14:24:00 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates
...

AI/Machine Learning Malware Detection Model
---------
Version: 2.04622 signed
Contract Expiry Date: Wed Jan  1 2031
Last Updated using scheduled update on Wed Feb 23 00:48:25 2022
Last Update Attempt: Wed Feb 23 11:34:52 2022
Result: No Updates
...
```

Signed packages and signatures are saved to disk with a special extension (.x) to distinguish them from unsigned packages. This extension allows the HA primary device to synchronize packages directly to secondary devices without further package validation. For example, an unsigned AV signature file would be saved as /data2/vir, and a signed file as /data2/vir.x.

The following examples contain output obtained from running the following debugs while the package is being updated:

```
# diagnose debug app updated -1
```

```
# diagnose debug enable
```

Automatic update from FDN or FortiManager

The packages are only accepted if they are signed.

To verify the automatic AV and IPS package updates:

```
# diagnose debug app updated -1
# diagnose debug enable
...
doInstallUpdatePackage[1023]-Full obj found for NIDS026
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
[331] ftnt_code_signing_verify_and_split:
[282] __ftnt_code_signing_verify:
[56] __dump_ctx: CS INFO: 544e544601000c8fee5f46f8aadf2d
[59] __dump_ctx: Sig len: 3215
[60] __dump_ctx: Raw len: 1200241
[190] __cms_verify: Verification succeeded.
installUpdateObject[310]-Signature verified for obj 4, ret=0, data_len=1203472, obj_
len=1200241, sig_len=3231.
...
```

Sample log

```
1: date=2022-02-23 time=16:16:36 eventtime=1645661796729851387 tz="-0800" logid="0100041000"
type="event" subtype="system" level="notice" vd="vd1" logdesc="FortiGate update succeeded"
```

```
status="update" msg="Fortigate update now fcni=yes fdni=yes fsci=yes idsdb(19.00264) idsetdb(19.00264) from 192.168.100.205:443"
```

Manual updates

An update can be performed manually after downloading the update file from the support.fortinet.com portal.

To execute the update:

```
# execute restore ips tftp nids-720-19.261.pkg 172.16.200.55
```

To verify the manual AV and IPS package updates:

```
# diagnose debug app updated -1
# diagnose debug enable
```

Manual update of a signed and validated package

This example shows a successful update where the update package is signed and validated.

Sample debugs for a successful update:

```
...
upd_manual_idsdb[219]-Updating ids db
doInstallUpdatePackage[1023]-Full obj found for NIDS024
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
installUpdateObject[310]-Signature verified for obj 4, ret=0, data_len=756201, obj_len=752970, sig_len=3231.
installUpdateObject[347]-Step 2:Prepare temp file for obj 4
installUpdObjRest[757]-Step 5:Backup /etc/ips.rules->/tmp/update.backup
installUpdObjRest[785]-Step 6:Copy new object /tmp/upd4MNOqr->/etc/ips.rules
installUpdObjRest[864]-Step 7:Validate object
...
doInstallUpdatePackage[1023]-Full obj found for NIDS026
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
installUpdateObject[310]-Signature verified for obj 4, ret=0, data_len=1165633, obj_len=1162402, sig_len=3231.
installUpdateObject[347]-Step 2:Prepare temp file for obj 4
installUpdObjRest[757]-Step 5:Backup /etc/ips.et.rules->/tmp/update.backup
installUpdObjRest[785]-Step 6:Copy new object /tmp/updf80vEs->/etc/ips.et.rules
installUpdObjRest[864]-Step 7:Validate object
...
__update_status[1237]-NIDS024(idsdb) installed successfully
__update_status[1237]-NIDS026(idsetdb) installed successfully
upd_status_save_status[131]-try to save on status file
upd_status_save_status[197]-Wrote status file
upd_manual_idsdb[269]-Update successful on NIDS24(idsdb))
upd_manual_idsdb[269]-Update successful on NIDS26(idsetdb))
```

Sample log

```
1: date=2022-02-23 time=20:58:05 eventtime=1645678685369622860 tz="-0800" logid="0100032217"
type="event" subtype="system" level="notice" vd="vdom1" logdesc="IPS package - Admin update
successful" status="update" msg="Fortigate updated idsdb(19.00262) idsetdb(19.00262)"
```

Manual update of an unsigned package with level-0 configured

This example shows an unsigned package update being accepted without any warning when the device BIOS has security level-0.

To execute the update:

```
# execute restore ips tftp nids-720-19.261.pkg 172.16.200.55
```

To verify the manual AV and IPS package updates:

```
# diagnose debug app updated -1
# diagnose debug enable
...
upd_manual_idsdb[219]-Updating ids db
doInstallUpdatePackage[1023]-Full obj found for NIDS024
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
installUpdateObject[310]-Signature verified for obj 4, ret=0, data_len=756201, obj_
len=752970, sig_len=3231.
installUpdateObject[347]-Step 2:Prepare temp file for obj 4
installUpdObjRest[757]-Step 5:Backup /etc/ips.rules->/tmp/update.backup
installUpdObjRest[785]-Step 6:Copy new object /tmp/upd4MNOqr->/etc/ips.rules
installUpdObjRest[864]-Step 7:Validate object
...
doInstallUpdatePackage[1023]-Full obj found for NIDS026
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
installUpdateObject[310]-Signature verified for obj 4, ret=0, data_len=1165633, obj_
len=1162402, sig_len=3231.
installUpdateObject[347]-Step 2:Prepare temp file for obj 4
installUpdObjRest[757]-Step 5:Backup /etc/ips.et.rules->/tmp/update.backup
installUpdObjRest[785]-Step 6:Copy new object /tmp/updf80vEs->/etc/ips.et.rules
installUpdObjRest[864]-Step 7:Validate object
...
__update_status[1237]-NIDS024(idsdb) installed successfully
__update_status[1237]-NIDS026(idsetdb) installed successfully
upd_status_save_status[131]-try to save on status file
upd_status_save_status[197]-Wrote status file
upd_manual_idsdb[269]-Update successful on NIDS24(idsdb))
upd_manual_idsdb[269]-Update successful on NIDS26(idsetdb))
```

Sample log

```
1: date=2022-02-23 time=20:58:05 eventtime=1645678685369622860 tz="-0800" logid="0100032217"
type="event" subtype="system" level="notice" vd="vdom1" logdesc="IPS package - Admin update
successful" status="update" msg="Fortigate updated idsdb(19.00262) idsetdb(19.00262)"
```

Manual update of an unsigned package with level-1 configured

A warning message is displayed in the console, and requests a user confirmation to accept the update of an unsigned package.

To execute the update:

```
# execute restore ips tftp nids-720-19.261.pkg 172.16.200.55
This operation will overwrite the current IPS package!
Do you want to continue? (y/n)y

Please wait...

Connect to tftp server 172.16.200.55 ...
##

Get IPS database from tftp server OK.
******WARNING: This package file has no signature for validation.******
Fortinet cannot verify the authenticity of this package and therefore
there may be a risk that the package contains code unknown to Fortinet.
In short, Fortinet cannot validate the package and makes no warranties
or representations concerning the package.
Please continue only if you understand and are willing to accept the risks.
Do you want to continue? (y/n)y
```

To verify the manual AV and IPS package updates:

```
# diagnose debug app updated -1
# diagnose debug enable
...
upd_manual_idsdb[219]-Updating ids db
doInstallUpdatePackage[1023]-Full obj found for NIDS024
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
installUpdateObject[310]-Signature verified for obj 4, ret=0, data_len=756204, obj_
len=756204, sig_len=0.
...
installUpdObjRest[864]-Step 7:Validate object
...
doInstallUpdatePackage[1023]-Full obj found for NIDS026
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
installUpdateObject[310]-Signature verified for obj 4, ret=0, data_len=1370909, obj_
len=1370909, sig_len=0.
...
installUpdObjRest[864]-Step 7:Validate object
...
__update_status[1237]-NIDS024(idsdb) installed successfully
__update_status[1237]-NIDS026(idsetdb) installed successfully
upd_status_save_status[131]-try to save on status file
upd_status_save_status[197]-Wrote status file
upd_manual_idsdb[269]-Update successful on NIDS24(idsdb))
upd_manual_idsdb[269]-Update successful on NIDS26(idsetdb))
```

Sample log

```
1: date=2022-02-23 time=16:19:49 eventtime=1645661989789578130 tz="-0800" logid="0100032217"
type="event" subtype="system" level="notice" vd="vd1" logdesc="IPS package - Admin update
successful" status="update" msg="Fortigate updated idsdb(19.00261) idsetdb(19.00261)"
```

Manual update of an unsigned package with level-2 configured

A warning message is displayed in the console, and the image is rejected.

To execute the update:

```
# execute restore ips tftp nids-720-19.261.pkg 172.16.200.55
This operation will overwrite the current IPS package!
Do you want to continue? (y/n)y

Please wait...

Connect to tftp server 172.16.200.55 ...
##

Get IPS database from tftp server OK.
```

To verify the manual AV and IPS package updates:

```
upd_manual_idsdb[219]-Updating ids db
doInstallUpdatePackage[1023]-Full obj found for NIDS024
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
__upd_obj_signature_split[2853]-Signature verify and split failed, result=2.
installUpdateObject[302]-Failed signature verifying for obj 4, ret=-1, forced=1, len=756204
doInstallUpdatePackage[1023]-Full obj found for NIDS026
doInstallUpdatePackage[1033]-Updating obj NIDS
installUpdateObject[278]-Step 1:Unpack obj 4, Total=1, cur=0
__upd_obj_signature_split[2853]-Signature verify and split failed, result=2.
installUpdateObject[302]-Failed signature verifying for obj 4, ret=-1, forced=1, len=1370909
upd_status_save_status[131]-try to save on status file
upd_status_save_status[202]-Status file is up-to-date
upd_manual_idsdb[247]-Update failed on NIDS24(idsdb) (-5,2)
upd_manual_idsdb[247]-Update failed on NIDS26(idsetdb) (-5,2)
Command fail. Return code -64
```

Sample logs

```
5: date=2022-02-23 time=17:00:29 eventtime=1645664429516742853 tz="-0800" logid="0100032231"
type="event" subtype="system" level="notice" vd="vdom1" logdesc="FortiGuard service failed
to restore" user="admin" ui="jsconsole(172.16.15.254)" action="restore-ips-package"
msg="User admin failed to restore IPS package file from jsconsole(172.16.15.254)"
```

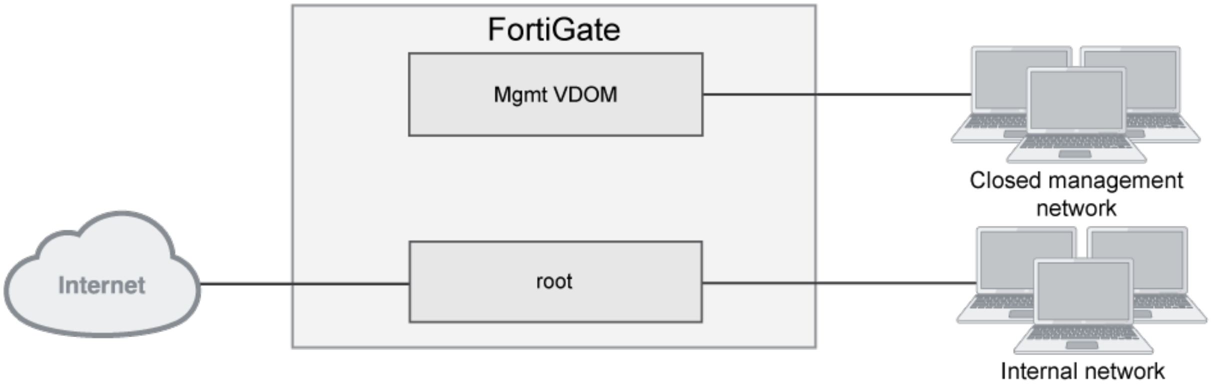
```
6: date=2022-02-23 time=17:00:29 eventtime=1645664429515611471 tz="-0800" logid="0100041009"
type="event" subtype="system" level="critical" vd="vdom1" logdesc="FortiGate database
signature invalid" user="admin" ui="jsconsole(172.16.15.254)" action="restore-ips"
status="failure" msg="Fortigate idsetdb signature invalid."
```

```
7: date=2022-02-23 time=17:00:29 eventtime=1645664429515606594 tz="-0800" logid="0100041009"
type="event" subtype="system" level="critical" vd="vdom1" logdesc="FortiGate database
```

```
signature invalid" user="admin" ui="jsconsole(172.16.15.254)" action="restore-ips"
status="failure" msg="Fortigate idsdb signature invalid."
```

Allow FortiGuard services and updates to initiate from a traffic VDOM

In multi VDOM mode, users can choose from which VDOM FortiGuard services and updates are initiated from, instead of being locked to the management VDOM. This allows deployment scenarios where the management VDOM is a closed network.



When the management VDOM is a closed network, it does not have internet access. However, FortiGuard services (FortiGuard updates, web filters, DNS proxy, DDNS, and so on) can be configured if a traffic VDOM is used as the root VDOM.

To configure FortiGuard services on a traffic VDOM:

1. Set up a traffic VDOM for FortiGuard services:

```
config global
    config system fortiguard
        set vdom "root"
    end
end
```

2. Ensure the traffic VDOM has the correct gateway to reach the internet:

```
config vdom
    edit root
        config router static
            edit 1
                set gateway 172.16.200.254
                set device "wan1"
            next
        end
    next
end
```

3. Configure the DNS servers to ensure the FortiGuard services can resolve the server name through the traffic VDOM:

```
config vdom
    edit root
```

```
            config system vdom-dns
                set vdom-dns enable
                set primary 208.91.112.53
                set secondary 208.91.112.52
            end
        next
    end
```

FortiManager as override server for IoT query services - 7.2.1

FortiGate can use FortiManager as an override server for IoT query services. The FortiManager must be running 7.2.1 or later.

All IoT daemon query and collected data can be sent to a FortiManager, instead of directly to FortiGuard. This is useful when there are strict policies controlling the kind of traffic that can go to the internet.

To send all IoT daemon query and collected data to a FortiManager:

```
config system central-management
    config server-list
        edit 1
            set server-type iot-query iot-collect
            set server-address <x.x.x.x>
        next
    end
end
```

`server-type iot-query iot-collect`	Set the FortiGuard service types: • `iot-query`: IoT query server. • `iot-collect`: IoT device collection server.
`server-address <x.x.x.x>`	IPv4 address of the FortiManager.

Security

This section includes information about security system related new features:

- Enhance BIOS-level signature and file integrity checking 7.2.5 on page 317
- Real-time file system integrity checking 7.2.5 on page 318
- Add built-in entropy source 7.2.6 on page 318

Enhance BIOS-level signature and file integrity checking - 7.2.5

This information is also available in the FortiOS 7.2 Administration Guide:

- BIOS-level signature and file integrity checking

The BIOS-level signature and integrity checking has been enhanced by enforcing each FortiOS GA firmware image, AV engine file, and IPS engine file to be dually-signed by the Fortinet CA and a third-party CA. The BIOS verifies that each file matches their secure hash as indicated by their certificates. Users are warned when there is a failed integrity check, and the system may be prevented from booting depending on the severity and the BIOS security level.

Signature checking occurs when the FortiOS firmware, AV, and IPS engine files are uploaded. This allows the FortiGate to warn users of potential risks involved with uploading an unauthenticated file.

The outcome of the signature and integrity check depends on the security level configured in BIOS and the certificate authority that signed the file.

For more information about this feature, see Enhance BIOS-level signature and file integrity checking.

Real-time file system integrity checking - 7.2.5

This information is also available in the FortiOS 7.2 Administration Guide:

- Real-time file system integrity checking

Real-time file system integrity checking has two main purposes:

- Prevent unauthorized modification of important binaries.
- Detect unauthorized binaries and prevent them from running.

When the FortiGate boots, the system performs a BIOS level integrity check on important internal files, the AV engine file, and the IPS engine file. These files are signed by the process described in Enhance BIOS-level signature and file integrity checking 7.2.5 on page 317, and the BIOS verifies their signature against their certificates.

Once these files are verified to be authentic, the BIOS can boot the root filesystem and other executables and libraries. Once loaded, real-time protection begins. The important executables and binaries are protected from write access and any modifications. It also blocks the kernel from loading any modules. Any unauthorized loading of modules is blocked. If violations are found, logs are triggered.

For more information about this feature, see Real-time file system integrity checking.

Add built-in entropy source - 7.2.6

This information is also available in the FortiOS 7.2 Administration Guide:

- Built-in entropy source

FortiOS includes a built-in entropy source, which eliminates the need for a physical USB entropy token when booting up in FIPS mode on any platform. This enhancement continues to meet the requirements of FIPS 140-3 Certification by changing the source of entropy to CPU jitter entropy.

The `entropy-token` parameter under `config system fips-cc` is removed if the FortiGate is a SoC3, SoC4, or CP9 device.

For more information about this feature, see Add built-in entropy source.

Policy and Objects

This section includes information about policy and object related new features:

Zero Trust Network Access

This section includes information about ZTNA related new features:

ZTNA scalability support for up to 50 thousand concurrent endpoints

ZTNA scalability is increased to support up to 50 thousand concurrent endpoints. Communication between FortiOS and FortiClient EMS is improved with more efficient queries that request incremental updates. Retrieved device information can be written to the FortiClient NAC daemon cache.

FortiOS can receive tag information from the EMS common tags API. This feature requires FortiClient EMS 7.0.3 or later.

The APIs `api/v1/report/fct/uid_tags` and `api/v1/report/fct/tags` replace the API `api/v1/report/fct/host_tags`.

To use the common tags API capability:

1. Enable the common tags API when connecting the EMS:

```
config endpoint-control fctems
    edit "local.ems"
        set server "10.6.30.213"
        set capabilities fabric-auth silent-approval websocket websocket-malware push-
ca-certs common-tags-api
    next
end
```

2. The FortiGate uses the new APIs to obtain device information from the EMS:

```
[ec_ems_context_submit_work:414] Call submitted successfully.
    obj-id: 11, desc: REST API to get updates of tag endpoints., entry:
api/v1/report/fct/tags.
[ec_ems_context_submit_work:414] Call submitted successfully.
    obj-id: 12, desc: REST API to get updates of tags associated with FCT UID., entry:
api/v1/report/fct/uid_tags.
[ec_ez_worker_process:334] Processing call for obj-id: 11, entry:
"api/v1/report/fct/tags"
[dynamic_addr_ha_act:215] called (EMS SN N/A).
[dynamic_addr_ha_act:215] called (EMS SN N/A).
[ec_ez_worker_process:441] Call completed successfully.
    obj-id: 11, desc: "REST API to get updates of tag endpoints.", entry:
"api/v1/report/fct/tags".
[ec_ez_worker_process:334] Processing call for obj-id: 12, entry:
"api/v1/report/fct/uid_tags"
[ec_record_sync_tags_info_store:1419] Received 1 tags for
3D86DF70B85E16CBAD67908A897B4494 with sn FCTEMS8888888888
[ec_record_sync_tags_info_store:1419] Received 1 tags for
DA12930442F13F84D2441F03FCB6A10E with sn FCTEMS8888888888
[ec_record_sync_tags_info_store:1419] Received 1 tags for
25C59C275F257F4C5FBC7F6F5F56788E with sn FCTEMS8888888888
[ec_ez_worker_process:441] Call completed successfully.
    obj-id: 12, desc: "REST API to get updates of tags associated with FCT UID.", entry:
"api/v1/report/fct/uid_tags".
[ec_ems_context_submit_work:414] Call submitted successfully.
    obj-id: 7, desc: REST API to get updates about system info., entry:
api/v1/report/fct/sysinfo.
[ec_ems_context_submit_work:414] Call submitted successfully.
    obj-id: 11, desc: REST API to get updates of tag endpoints., entry:
api/v1/report/fct/tags.
[ec_ez_worker_process:334] Processing call for obj-id: 11, entry:
"api/v1/report/fct/tags"
[ec_ez_worker_process:441] Call completed successfully.
    obj-id: 11, desc: "REST API to get updates of tag endpoints.", entry:
"api/v1/report/fct/tags".
(......)
```

3. Confirm that the device information from the EMS is written to the FortiClient NAC daemon cache:

```
# diagnose endpoint record list
    ...
          Avatar source: OS
            Phone number:
            Number of Routes: (1)
                    Gateway Route #0:
                            - IP:10.1.91.6, MAC: 4f:8d:c2:73:dd:fe, Indirect: no
                            - Interface:port2, VFID:1, SN: FG5H1E5999999999
online records: 37174; offline records: 0; quarantined records: 0; out-of-sync records:
0
```

4. Use the tags that are pulled from the EMS in a firewall address:

```
config firewall address
    edit "FCTEMS8888888888_ZT_AD_MGMT"
        set type dynamic
        set sub-type ems-tag
        set obj-tag "ZT_AD_MGMT"
        set tag-type "zero_trust"
    next
end
```

5. Check the tags' resolved IP and MAC addresses:

```
# diagnose firewall fqdn getinfo-ip FCTEMS8888888888_ZT_AD_MGMT
getinfo FCTEMS8888888888_ZT_AD_MGMT id:114 generation:106 count:187 data_len:6160 flag 0
```

```
# diagnose firewall fqdn getinfo-mac MAC_FCTEMS8888888888_ZT_AD_MGMT
getinfo MAC_FCTEMS8888888888_ZT_AD_MGMT id:163 generation:105 count:371 data_len:2226
flag 0
```

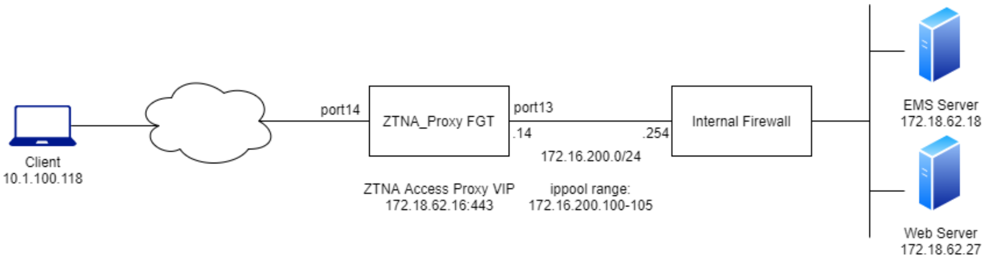
```
# diagnose firewall dynamic address  FCTEMS8888888888_ZT_AD_MGMT
CMDB name: FCTEMS8888888888_ZT_AD_MGMT
TAG name: ZT_AD_MGMT
FCTEMS8888888888_ZT_AD_MGMT: ID(114)
        ADDR(10.1.10.4)
(......)
        ADDR(10.1.99.195)
Total IP dynamic range blocks: 190.
Total IP dynamic addresses: 281.
```

```
# diagnose firewall dynamic address MAC_FCTEMS8888888888_ZT_AD_MGMT
CMDB name: MAC_FCTEMS8888888888_ZT_AD_MGMT
TAG name: ZT_AD_MGMT
MAC_FCTEMS8888888888_ZT_AD_MGMT: ID(163)
        MAC(52:f1:9d:06:1c:db)
        MAC(4b:77:2b:db:82:15)
        MAC(df:6e:9e:d9:04:1e)
Total MAC dynamic addresses: 393.
```

Using the IP pool or client IP address in a ZTNA connection to backend servers

By default, the connection from the ZTNA access proxy to the backend servers uses the IP address of the outgoing interface as the source. This enhancement enables customers to use an IP pool as the source IP address, or use the client's original IP address as the source IP address. This allows ZTNA to support more sessions without source port conflicts.

These example show the basic configurations for using an IP pool or transparent mode in a ZTNA proxy policy.



This topology uses a HTTP access proxy to forward traffic to the web server at 172.18.62.27. The IP pool range is 172.16.200.100-105, so this effectively allows for six times more connections using the six source addresses in the pool.

If transparent mode is used, the FortiGate uses the client's address (10.1.100.118) as the source IP when connecting to the servers.

Basic ZTNA configuration

To configure the FortiGate:

1. Configure the access proxy VIP:

```
config firewall vip
    edit "ZTNA_S1"
        set type access-proxy
        set extip 172.18.62.16
        set extintf "any"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the virtual host:

```
config firewall access-proxy-virtual-host
    edit "auto-ZTNA_S1-0"
        set ssl-certificate "Fortinet_SSL"
        set host "v1.qa.fortinet.com"
    next
end
```

3. Configure the server and path mapping:

```
config firewall access-proxy
    edit "ZTNA_S1"
        set vip "ZTNA_S1"
        set client-cert enable
        set auth-portal enable
        set log-blocked-traffic enable
        config api-gateway
            edit 1
                set virtual-host "auto-ZTNA_S1-0"
                config realservers
                    edit 1
                        set ip 172.18.62.27
                    next
                end
            next
        end
    next
end
```

Example 1: IP pool

To configure the FortiGate:

1. Configure the IP pool:

```
config firewall ippool
    edit "ztna_pool1"
        set startip 172.16.200.100
        set endip 172.16.200.105
    next
end
```

2. Configure the proxy policy:

```
config firewall proxy-policy
    edit 1
        set name "ZTNA_R1"
        set proxy access-proxy
        set access-proxy "ZTNA_S1"
        set srcintf "port14"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "FCTEMS8821000000_ems140_av_tag"
        set action accept
        set schedule "always"
        set logtraffic all
        set poolname "ztna_pool1"
        set utm-status enable
        set ssl-ssh-profile "custom-deep-inspection"
        set av-profile "test-av"
        set webfilter-profile "test_wf"
        set file-filter-profile "g-default"
        set ips-sensor "test_ips"
        set application-list "test_app"
    next
end
```

Once the ZTNA client generates traffic, run the WAD debug commands on the FortiGate. The outgoing IP address should be from the IP pool.

To test the configuration:

```
# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable
...
[V]2022-03-22 17:53:45.026384 [p:356][s:339191][r:50334048] wad_http_session_disconn_srv
 :1456  hcs=0x7f993d7877e8 http_svr=(nil)
[I]2022-03-22 17:53:45.026387 [p:356][s:339191][r:50334048] wad_http_connect_original_server
 :6253  http ses=0x7f993d7877e8 req=0x7f993d610780 ses_ctx=0x7f993d759218 connect svr orig
10.1.100.118:61694->172.18.62.16:443 out 10.1.100.118:61694->172.18.62.16:443
[I]2022-03-22 17:53:45.026390 [p:356][s:339191][r:50334048] wad_http_upd_ses_ctx_by_req
 :838   wad http session 0x7f993d7877e8  forward (nil) fwd_srv_ip=0.0.0.0
[I]2022-03-22 17:53:45.026455 [p:356][s:339191][r:50334048] wad_ippool_get_ip
 :842   clt:10.1.100.118 got ip:172.16.200.102 from ip pool, logic/phy intf(27/27)
[V]2022-03-22 17:53:45.026459 [p:356][s:339191][r:50334048] wad_http_connect_original_server
```

```
 :6268  [0x7f993d610780] Connect to server: 172.18.62.27:443/172.18.62.27:443
[I]2022-03-22 17:53:45.026461 [p:356][s:339191][r:50334048] wad_tcp_port_alloc
 :1434  alloc tcp_port=0x7f993ac55188
[V]2022-03-22 17:53:45.026470 [p:356][s:339191][r:50334048] wad_tcp_port_bind
 :527   tcp_port=0x7f993ac55188 src ip:172.16.200.102 is bind, create sess:1
[V]2022-03-22 17:53:45.026472 [p:356][s:339191][r:50334048] wad_tcp_port_connect_with_fd
 :2179  oif =27, src_addr_unkown=0
[I]2022-03-22 17:53:45.026495 [p:356][s:339191][r:50334048] wad_tcp_port_connect_with_fd
 :2221  TCP port=0x7f993ac55188 sock=63 vrf=0 connecting 172.16.200.102:12764-
>172.18.62.27:443
[V]2022-03-22 17:53:45.026506 [p:356][s:339191][r:50334048] wad_http_port_connect
 :1815  connect to SSL terminator.
[V]2022-03-22 17:53:45.026509 [p:356][s:339191][r:50334048] wad_tcp_port_out_read_block
 :975   tcp_port 0x7f993ac55048 fd=62 on=1 n_out_block=0~>1 in(/out)_shutdown=0/0 closed=0
state=2.
[V]2022-03-22 17:53:45.026511 [p:356][s:339191][r:50334048] wad_tcp_port_transport_read_
block :930   tcp_port 0x7f993ac55048 fd=62 on=1 n_out_block=0~>1 in(/out)_shutdown=0/0
closed=0 events=0x1.
[V]2022-03-22 17:53:45.026513 [p:356][s:339191][r:50334048] wad_tcp_port_transport_read_
block :944   sock 62 read_block enforced, turn off readability.
```

Example 2: transparent mode

To configure transparent mode in a proxy policy:

```
config firewall proxy-policy
    edit 1
        set name "ZTNA_R1"
        set proxy access-proxy
        set access-proxy "ZTNA_S1"
        set srcintf "port14"
        set srcaddr "all"
        set transparent enable
        set dstaddr "all"
        set ztna-ems-tag "FCTEMS8821000000_ems140_av_tag"
        set action accept
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile "custom-deep-inspection"
        set av-profile "test-av"
        set webfilter-profile "test_wf"
        set file-filter-profile "g-default"
        set ips-sensor "test_ips"
        set application-list "test_app"
    next
end
```

Once the ZTNA client generates traffic, run the WAD debug commands on the FortiGate. The client's address (10.1.100.118) should be used as the source IP address when connecting to the servers.

To test the configuration:

```
# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable
...
[V]2022-03-22 18:11:34.968351 [p:356][s:343987][r:50334156] wad_http_connect_server
 :6363  http session 0x7f993d7877e8 req=0x7f993d611a60
[V]2022-03-22 18:11:34.968354 [p:356][s:343987][r:50334156] wad_http_srv_still_good
 :6135  srv((nil)) nontp(0) dst_type(3)
req: dst:172.18.62.27:443, proto:10)
hcs: dst:N/A:0, proto:1)
[V]2022-03-22 18:11:34.968357 [p:356][s:343987][r:50334156] wad_http_session_disconn_srv
 :1456  hcs=0x7f993d7877e8 http_svr=(nil)
[I]2022-03-22 18:11:34.968360 [p:356][s:343987][r:50334156] wad_http_connect_original_server
 :6253  http ses=0x7f993d7877e8 req=0x7f993d611a60 ses_ctx=0x7f993d758ec8 connect svr orig
10.1.100.118:62113->172.18.62.16:443 out 10.1.100.118:62113->172.18.62.16:443
[I]2022-03-22 18:11:34.968363 [p:356][s:343987][r:50334156] wad_http_upd_ses_ctx_by_req
 :838   wad http session 0x7f993d7877e8  forward (nil) fwd_srv_ip=0.0.0.0
[V]2022-03-22 18:11:34.968367 [p:356][s:343987][r:50334156] wad_http_connect_original_server
 :6268  [0x7f993d611a60] Connect to server: 172.18.62.27:443/172.18.62.27:443
[I]2022-03-22 18:11:34.968369 [p:356][s:343987][r:50334156] wad_tcp_port_alloc
 :1434  alloc tcp_port=0x7f993ac55908
[V]2022-03-22 18:11:34.968379 [p:356][s:343987][r:50334156] wad_tcp_port_bind
 :527   tcp_port=0x7f993ac55908 src ip:10.1.100.118 is bind, create sess:1
[V]2022-03-22 18:11:34.968381 [p:356][s:343987][r:50334156] wad_tcp_port_connect_with_fd
 :2179  oif =27, src_addr_unkown=0
[I]2022-03-22 18:11:34.968403 [p:356][s:343987][r:50334156] wad_tcp_port_connect_with_fd
 :2221  TCP port=0x7f993ac55908 sock=64 vrf=0 connecting 10.1.100.118:2182->172.18.62.27:443
[V]2022-03-22 18:11:34.968412 [p:356][s:343987][r:50334156] wad_http_port_connect
 :1815  connect to SSL terminator.
```

ZTNA device certificate verification from EMS for SSL VPN connections - 7.2.1

When connecting to a FortiGate SSL VPN in tunnel mode, the `ztna-trusted-client` setting enforces a ZTNA trusted client before the user can successfully establish an SSL VPN tunnel. A ZTNA trusted client is a device that is registered to FortiClient EMS and has a device certificated issued by EMS.

```
config vpn ssl setting
    set ztna-trusted-client {enable | disable}
end
```

If a PKI user is also configured, then the user can specify their certificate to get authenticated without providing a certificate that is signed by EMS.

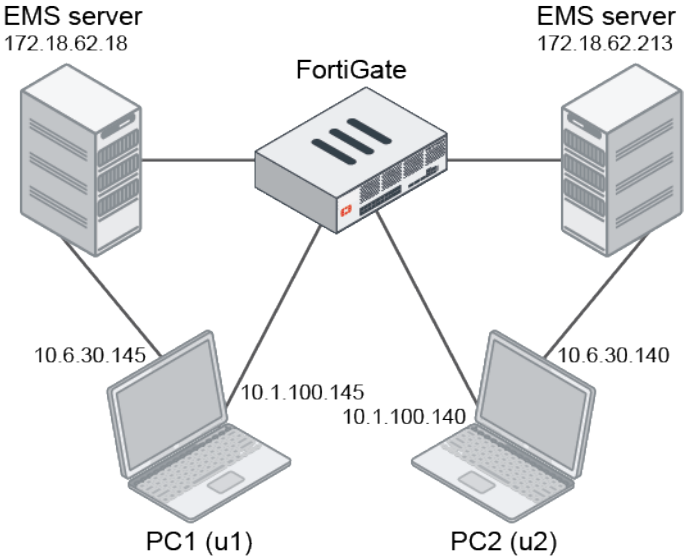
If a SAML log in is also configured, then the user can finish authentication without providing a certificate that is signed by EMS.

Example

In this example, a FortiGate is registered to two EMS servers: 172.18.62.18 and 172.18.62.213. The following conditions are required to access to the SSL VPN tunnel:

- The device must have FortiClient installed.
- FortiClient must register to an EMS that the FortiGate is also registered to.
- The user must specify a certificate that is signed by EMS to log in.

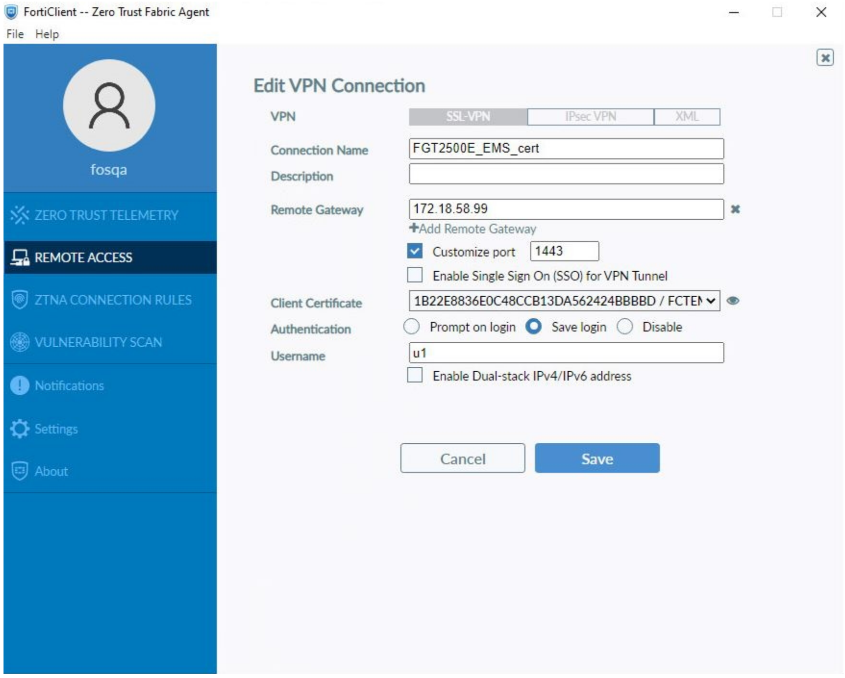
There are two users: one is using PC1 (u1) installed with FortiClient that is registered to EMS 172.18.62.18, and another is using PC2 (u2) installed with FortiClient that is registered to EMS 172.18.62.213. Both users can log in to the SSL VPN tunnel when specifying an EMS signed certificate.



This example assumes that the FortiGate EMS Fabric connectors are already successfully connected, and that the users have successfully registered FortiClient to their corresponding EMS servers.

When FortiClient is registered to EMS, the certificate is automatically installed on the device and is signed by EMS.

- User u1 FortiClient configuration:

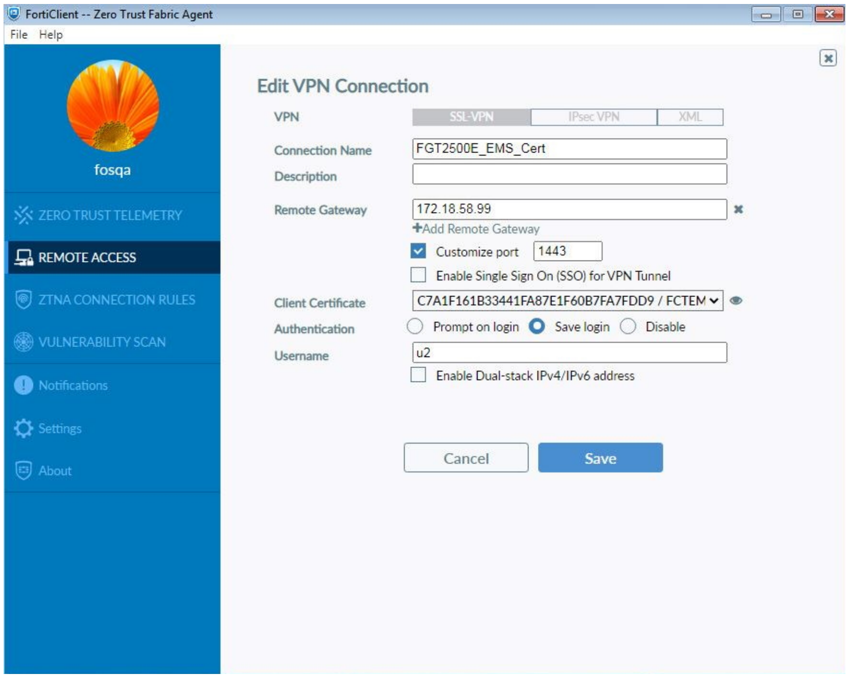


Edit VPN Connection

VPN	SSL-VPN / IPsec VPN / XML
Connection Name	FGT2500E_EMS_cert
Description	
Remote Gateway	172.18.58.99
	+Add Remote Gateway
	☑ Customize port 1443
	□ Enable Single Sign On (SSO) for VPN Tunnel
Client Certificate	1B22E8836E0C48CCB13DA562424BBBBD / FCTEM
Authentication	○ Prompt on login ● Save login ○ Disable
Username	u1
	□ Enable Dual-stack IPv4/IPv6 address

Cancel Save

- User u2 FortiClient configuration:



Edit VPN Connection

VPN: SSL-VPN | IPsec VPN | XML

Connection Name: FGT2500E_EMS_Cert

Description:

Remote Gateway: 172.18.58.99

+Add Remote Gateway

☑ Customize port 1443

□ Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: C7A1F161B33441FA87E1F60B7FA7FDD9 / FCTEM

Authentication: ○ Prompt on login ● Save login ○ Disable

Username: u2

□ Enable Dual-stack IPv4/IPv6 address

Cancel | Save

To configure the SSL VPN connection:

1. Configure the portal settings:

```
config vpn ssl web portal
    edit "testportal1"
        set tunnel-mode enable
        set web-mode enable
        set auto-connect enable
        set keep-alive enable
        set save-password enable
        set ip-pools "ip_pool"
        set split-tunneling disable
        set heading "SSL-VPN Portal 1"
    next
end
```

2. Configure the SSL VPN settings:

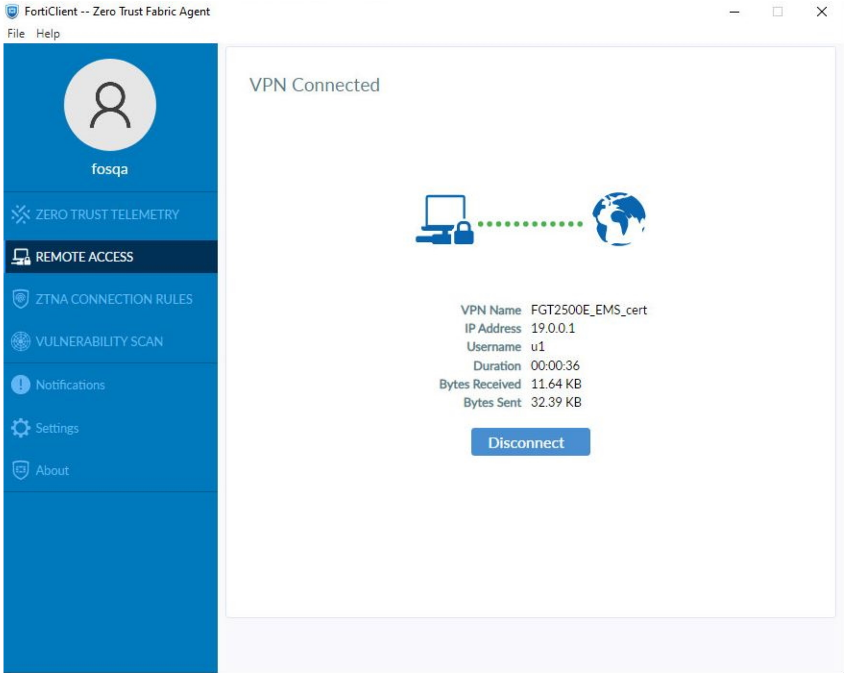
```
config vpn ssl settings
    set servercert "Fortinet_Factory"
    set idle-timeout 0
    set auth-timeout 0
    set login-attempt-limit 0
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 1443
    set source-interface "port2" "port1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "testportal1"
    set encrypt-and-store-password enable
```

```
        set ztna-trusted-client enable
    end
```

Testing the connection to the SSL VPN tunnel

To verify that users u1 and u2 can log in to FortiClient:

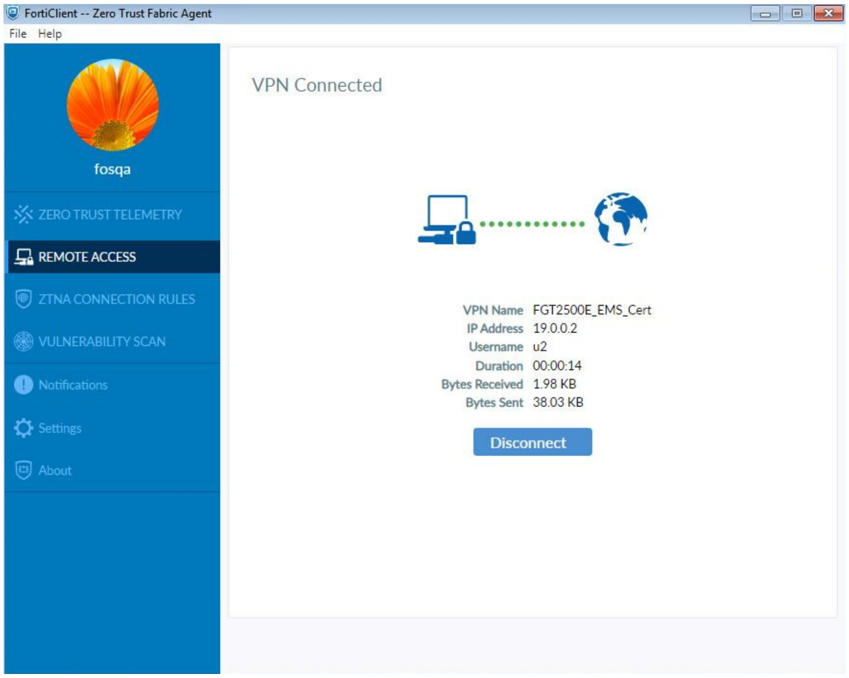
1. Get users u1 and u2 to log in to FortiClient. Both logins should be successful.
   a. User u1:



VPN Connected

```
      VPN Name  FGT2500E_EMS_cert
    IP Address  19.0.0.1
      Username  u1
      Duration  00:00:36
Bytes Received  11.64 KB
    Bytes Sent  32.39 KB
```

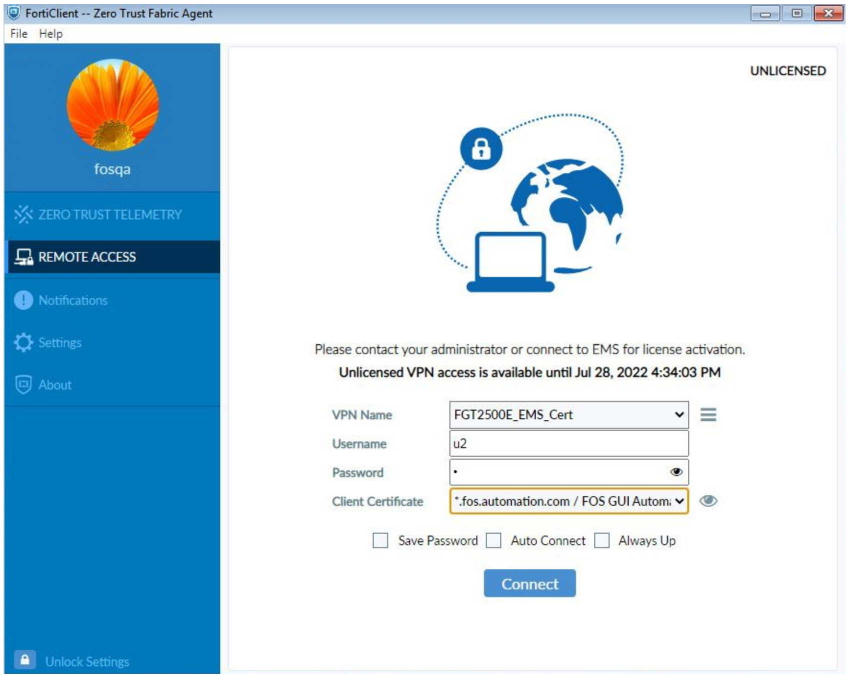
b. User u2:



VPN Connected

VPN Name FGT2500E_EMS_Cert
IP Address 19.0.0.2
Username u2
Duration 00:00:14
Bytes Received 1.98 KB
Bytes Sent 38.03 KB

2. Deregister the u2 FortiClient from EMS 172.18.62.213.
3. When u2 tries to log in to the SSL VPN again with an incorrect certificate, the SSL VPN connection is rejected.
    a. In the *Remote Access* tab, *UNLICENSED* appears in the top-right corner of the window, and a message appears to contact the administrator to activate the license.



UNLICENSED

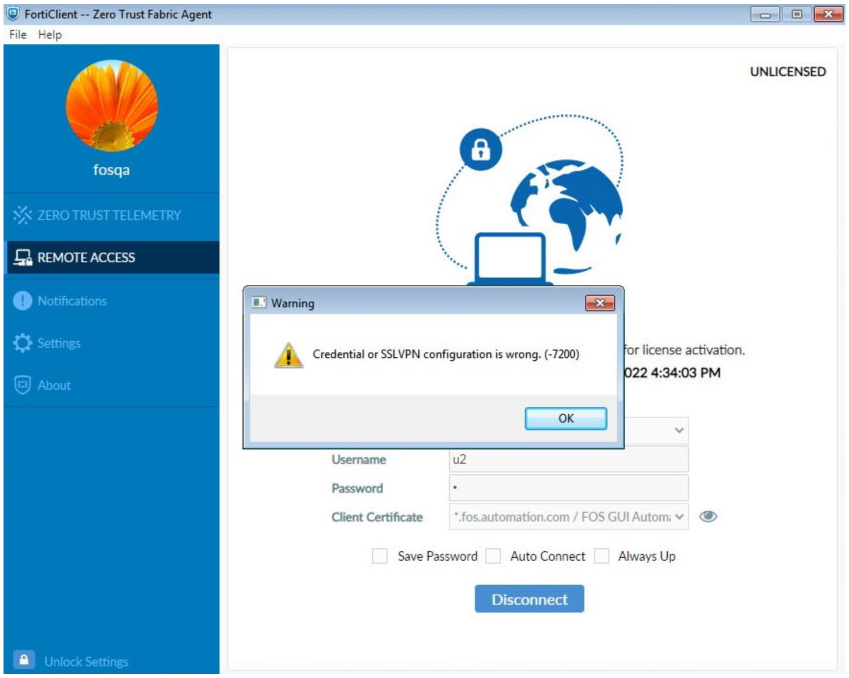
Please contact your administrator or connect to EMS for license activation.

Unlicensed VPN access is available until Jul 28, 2022 4:34:03 PM

VPN Name FGT2500E_EMS_Cert
Username u2
Password •
Client Certificate *.fos.automation.com / FOS GUI Autom

□ Save Password □ Auto Connect □ Always Up

b. After clicking *Connect*, an error message appears that the *Credential or SSLVPN configuration is wrong*.



Credential or SSLVPN configuration is wrong. (-7200)

Username: u2

Password: •

Client Certificate: *.fos.automation.com / FOS GUI Autom:

□ Save Password □ Auto Connect □ Always Up

Once users u1 and u2 log in with FortiClient and use the correct certificate signed by the corresponding EMS (172.18.62.18 and 172.18.62.213 respectively), check the SSL VPN monitor to see that the tunnel connection was established.

To verify that u1 established an SSL VPN connection:

```
# get vpn ssl monitor
SSL-VPN Login Users:
 Index    User    Group    Auth Type      Timeout         Auth-Timeout    From     HTTP in/out
   HTTPS in/out    Two-factor Auth
 0        u1              1(1)             N/A     172.16.200.254 0/0     0/0     0
SSL-VPN sessions:
 Index    User    Group    Source IP      Duration        I/O Bytes       Tunnel/Dest IP
 0        u1              172.16.200.254   537     168693/150495  19.0.0.1
```

To verify that u2 established an SSL VPN connection:

```
# get vpn ssl monitor
SSL-VPN Login Users:
 Index    User    Group    Auth Type      Timeout         Auth-Timeout    From     HTTP in/out
   HTTPS in/out    Two-factor Auth
 1        u2              1(1)             N/A     172.16.200.254 0/0     0/0     0

SSL-VPN sessions:
 Index    User    Group    Source IP      Duration        I/O Bytes       Tunnel/Dest IP
 1        u2              172.16.200.254   300     88805/85301    19.0.0.2
```

Mapping ZTNA virtual host and TCP forwarding domains to the DNS database - 7.2.1

When ZTNA is deployed on a FortiGate in the network and a ZTNA virtual host or TCP forwarding domain is used, the corresponding virtual host or TCP forwarding domain should be mapped to the access proxy's virtual IP. To facilitate this, when FortiClients retrieve the list of published services from the FortiGate, virtual hosts and domains are added to the FortiGate's local DNS database. There is also a constraint to restrict the mapping of a virtual host to one access proxy entry only.

```
config firewall access-proxy
    edit <name>
        set add-vhost-domain-to-dnsdb {enable | disable}
    next
end
```

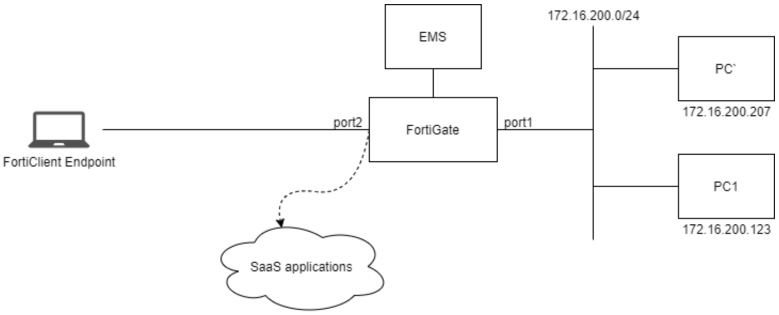
`add-vhost-domain-to-dnsdb {enable | disable}`	When enabled, all virtual hosts and TCP forwarding domains in the access proxy will be added under `config system dns-database`.

```
config system dns-database
    edit <name>
        set view {shadow | public | shadow-ztna}
    next
end
```

`view {shadow | public | shadow-ztna}`	Set the zone view: • `shadow`: shadow DNS zone to serve internal clients. • `public`: public DNS zone to serve public clients. • `shadow-ztna`: resolve to the ZTNA VIP. This implicit DNS zone is only visible to clients connecting to the ZTNA DoT/DoH tunnel.

Example

In this example, the FortiGate has several ZTNA access proxies configured with different VIPs attached to each one.



Different virtual hosts and TCP forwarding domains are configured on each access proxy:

Access proxy	VIP address	Virtual host	TCP forwarding domain
ztna	172.18.82.66	vh1: test1.test.com vh2: test2.test.com	

Access proxy	VIP address	Virtual host	TCP forwarding domain
ztna_2	172.18.82.67	vh3: test3.test.com	
ztna_3	172.18.82.68		test4.test.com

Consequently, DNS entries with shadow ZTNA view are added to the local DNS database.

To configure the FortiGate:

1. Configure three access proxy VIPs:

```
config firewall vip
    edit "ztna"
        set type access-proxy
        set extip 172.18.82.66
        set extintf "any"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
    edit "ztna_2"
        set type access-proxy
        set extip 172.18.82.67
        set extintf "any"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
    edit "ztna_3"
        set type access-proxy
        set extip 172.18.82.68
        set extintf "any"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure three virtual hosts to be used in the ZTNA access proxies:

```
config firewall access-proxy-virtual-host
    edit "vh1"
        set ssl-certificate "*.test.com"
        set host "test1.test.com"
    next
    edit "vh2"
        set ssl-certificate "*.test.com"
        set host "test2.test.com"
    next
    edit "vh3"
        set ssl-certificate "*.test.com"
        set host "test3.test.com"
    next
end
```

3. Configure the first access proxy, and map virtual hosts vh1 and vh2 to different services:

```
config firewall access-proxy
    edit "ztna"
        set vip "ztna"
        set add-vhost-domain-to-dnsdb enable
        config api-gateway
            edit 1
                set virtual-host "vh1"
                config realservers
                    edit 1
                        set addr-type fqdn
                        set address "fqdn4"
                    next
                    edit 2
                        set ip 172.16.200.207
                    next
                end
            next
            edit 2
                set service http
                set virtual-host "vh2"
                config realservers
                    edit 1
                        set ip 172.16.200.123
                    next
                end
            next
        end
    next
end
```

4. Configure the second access proxy, and map one service to virtual host vh3.

```
config firewall access-proxy
    edit "ztna_2"
        set vip "ztna_2"
        set add-vhost-domain-to-dnsdb enable
        config api-gateway
            edit 1
                set virtual-host "vh3"
                config realservers
                    edit 1
                        set ip 172.16.200.207
                    next
                end
            next
        end
    next
end
```

   Since `add-vhost-domain-to-dnsdb` is enabled, a virtual host used in the other access proxy cannot be mapped to this access proxy.

5. Configure the third access proxy for TCP forwarding:

```
config firewall access-proxy
    edit "ztna_3"
        set vip "ztna_3"
        set add-vhost-domain-to-dnsdb enable
        config api-gateway
            edit 2
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set domain "test4.test.com"
                    next
                end
            next
        end
    next
end
```

The virtual host and TCP forwarding domains are mapped to their corresponding access proxy VIP under the local DNS database. Each will appear as a shadow ZTNA entry:

```
show full-configuration system dns-database
config system dns-database
    edit "test1.test.com"
        set domain "test1.test.com"
        set view shadow-ztna
        config dns-entry
            edit 1
                set ttl 86400
                set hostname "test1.test.com"
                set ip 172.18.82.66
            next
        end
        set primary-name "test1.test.com"
        set contact "fgt-ztna"
    next
    edit "test2.test.com"
        set domain "test2.test.com"
        set view shadow-ztna
        config dns-entry
            edit 1
                set ttl 86400
                set hostname "test2.test.com"
                set ip 172.18.82.66
            next
        end
        set primary-name "test2.test.com"
        set contact "fgt-ztna"
    next
    edit "test3.test.com"
        set domain "test3.test.com"
        set view shadow-ztna
        config dns-entry
            edit 1
                set ttl 86400
                set hostname "test3.test.com"
                set ip 172.18.82.67
            next
        end
        set primary-name "test3.test.com"
        set contact "fgt-ztna"
    next
    edit "test4.test.com"
        set domain "test4.test.com"
        set view shadow-ztna
        config dns-entry
            edit 1
                set ttl 86400
                set hostname "test4.test.com"
                set ip 172.18.82.68
            next
        end
        set primary-name "test4.test.com"
        set contact "fgt-ztna"
    next
end
```

Publishing ZTNA services through the ZTNA portal - 7.2.1

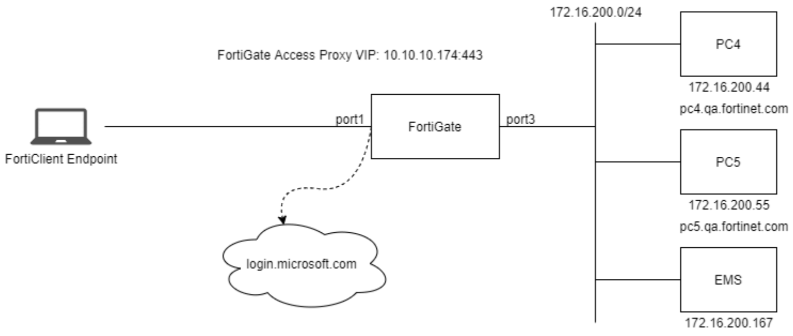
When ZTNA is deployed on a FortiGate in the network, it is important for endpoint clients to know what ZTNA services are available from the FortiGate access proxy. FortiClients are able to learn the available ZTNA services from the FortiGate ZTNA portal. The services that can be learned include HTTP/HTTPS web services, TCP forwarding services, and web portals. The FortiClient must connect to the FortiGate using a DoT/DoH tunnel so it can retrieve the service mapping in JSON format.

This feature is not supported in FortiOS versions 7.2.6 or 7.4.1, and later.

Example 1

In this example, the FortiGate is configured as a ZTNA access proxy with a VIP of 10.10.10.174. It hosts several services, including:

- HTTP service with real server mapping to 172.16.200.44
- HTTP service with real server mapping to PC4, pc4.qa.fortinet.com
- TCP forwarding with real server mapping to login.microsoft.com:443
- SSL VPN web portal mapping to the local ztna_web_portal with a bookmark to PC5, pc5.qa.fortinet.com



The hosted services are published through the ZTNA portal, which is accessible by the FortiClient through `https://vip/fct-api-xxyyzz?command=service[&user=]`. The client must establish a DoT/DoH tunnel with the FortiGate ZTNA portal before the hosted services can be retrieved.

To configure the FortiGate:

1. Configure the EMS connector:

```
config endpoint-control fctems
    edit 1
        set status enable
        set name "1"
        set server "172.16.200.167"
        set serial-number <FortiClient_EMS_serial_number>
        set capabilities fabric-auth silent-approval websocket websocket-malware push-
ca-certs common-tags-api
    next
end
```

2. Configure the SSL VPN portal for publishing the web portal mapping:

```
config vpn ssl web portal
    edit "ztna_web_portal"
        set web-mode enable
        config bookmark-group
            edit "gui-bookmarks"
                config bookmarks
                    edit "pc05"
                        set url "http://172.16.200.55"
                    next
                end
            next
        end
    next
end
```

3. Configure the access proxy VIP for ZTNA:

```
config firewall vip
    edit "test_https"
        set type access-proxy
        set extip 10.10.10.174
        set extintf "port1"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

4. Configure the FQDN firewall address for PC4:

```
config firewall address
    edit "pc4"
        set type fqdn
        set fqdn "pc4.qa.fortinet.com"
    next
end
```

5. Configure the access proxy virtual hosts:

```
config firewall access-proxy-virtual-host
    edit "auto-test_ztna_portal-1"
        set ssl-certificate "Fortinet_SSL"
        set host "qa.fortinet.com"
    next
    edit "auto-test_ztna_portal-0"
        set ssl-certificate "Fortinet_SSL"
        set host "test.fortinet.com"
    next
end
```

When `add-vhost-domain-to-dnsdb` is enabled in the firewall access proxy settings, the virtual hosts are added automatically under `config system dns-database`.

6. Configure the firewall access proxy and map each service:

```
config firewall access-proxy
    edit "test_ztna_portal"
        set vip "test_https"
        set add-vhost-domain-to-dnsdb enable
        config api-gateway
            edit 2
                set virtual-host "auto-test_ztna_portal-0"
                config realservers
                    edit 1
                        set ip 172.16.200.44
                        set port 80
                    next
                end
            next
            edit 3
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "login.microsoft.com"
                        set mappedport 443
                    next
                end
            next
            edit 4
                set service http
                set virtual-host "auto-test_ztna_portal-1"
                config realservers
                    edit 1
                        set addr-type fqdn
                        set address "pc4"
                        set port 80
                    next
                end
            next
            edit 1
                set service web-portal
                set ssl-vpn-web-portal "ztna_web_portal"
            next
        end
    next
end
```

Since `add-vhost-domain-to-dnsdb` is enabled, the `shadow-ztna` DNS entries are added under the `config system dns-database` table. FortiClient endpoints connecting to the ZTNA portal will be able to resolve the virtual hosts to the ZTNA access proxy VIP address.

```
show full-configuration system dns-database
config system dns-database
    edit "test.fortinet.com"
        set domain "test.fortinet.com"
        set view shadow-ztna
        config dns-entry
            edit 1
                set ttl 86400
                set hostname "test.fortinet.com"
                set ip 10.10.10.174
            next
        end
        set primary-name "test.fortinet.com"
        set contact "fgt-ztna"
    next
    edit "qa.fortinet.com"
        set domain "qa.fortinet.com"
        set view shadow-ztna
        config dns-entry
            edit 1
                set ttl 86400
                set hostname "qa.fortinet.com"
                set ip 10.10.10.174
            next
        end
        set primary-name "qa.fortinet.com"
        set contact "fgt-ztna"
    next
end
```

7. Configure the ZTNA policy:

```
config firewall proxy-policy
    edit 1
        set name "test_rule"
        set proxy access-proxy
        set access-proxy "test_ztna_portal"
        set srcintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set ssl-ssh-profile "ssl"
    next
end
```

Testing and results

When ZTNA is configured, a FortiClient can establish a tunnel to the FortiGate using the ZTNA web portal. Once connected, it can retrieve the list of hosted services using `https://10.10.10.174/fct-api-`

`xxyyzz?command=service`.

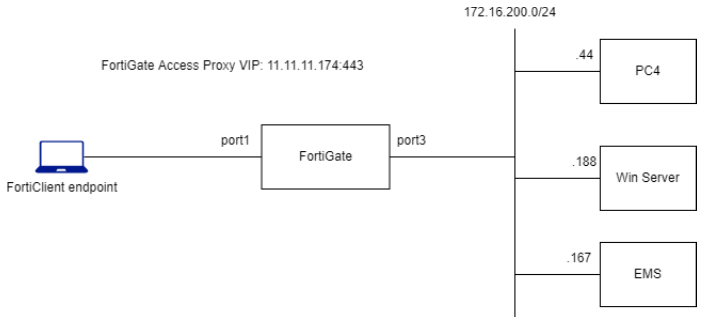
The following JSON is returned:

```
{
    "vips":[
        {
            "vip":"10.10.10.174:443",
            "gateways":[
                {
                    "type":"http",
                    "virtual-host":"qa.fortinet.com",
                    "path":"/",
                    "path-pattern":"sub-string",
                    "servers":[
                        {
                            "address":
                                {
                                    "type":"fqdn",
                                    "value":[
                                        {
                                            "fqdn":"pc4.qa.fortinet.com"
                                        }
                                    ]
                                },
                            "port":"80"
                        }
                    ]
                },
                {
                    "type":"bookmark-http",
                    "virtual-host":"172.16.200.55",
                    "path":"/",
                    "path-pattern":"sub-string"
                },
                {
                    "type":"https",
                    "virtual-host":"",
                    "path":"/",
                    "path-pattern":"sub-string",
                    "servers":[
                        {
                            "address":
                                {
                                    "type":"ip",
                                    "value":[
                                        {
                                            "ip":"172.16.200.44",
                                            "mask":"255.255.255.255"
                                        }
                                    ]
                                },
                            "port":"80"
                        }
                    ]
                },
                {
                    "type":"tcp-fwd",
                    "virtual-host":"",
                    "path":"/tcp",
                    "path-pattern":"sub-string",
                    "servers":[
                        {
                            "address":
                                {
                                    "type":"fqdn",
                                    "value":[
                                        {
                                            "fqdn":"login.microsoft.com"
                                        }
                                    ]
                                },
                            "mappedport":[
                                {
                                    "start":"443",
                                    "end":"443"
                                }
                            ]
                        }
                    ]
                },
                {
                    "type":"web-portal",
                    "virtual-host":"",
                    "path":"/",
                    "path-pattern":"sub-string"
                }
            ]
        }
    ]
}
```

Example 2

In this example, the FortiGate publishes two TCP forwarding rules to its ZTNA service portal. FortiClient EMS is configured to push the FortiGate ZTNA service portal address to its managed endpoints. The FortiClient endpoint queries the FortiGate for the list of ZTNA services and loads them in memory. Users can then access the ZTNA destinations without manually defining the rules or retrieving them from EMS.

The configurations used in this example require FortiClient and FortiClient EMS 7.2.0. See FortiGate ZTNA service portal support and Inline CASB solution for SaaS applications in the FortiClient New Features Guide for more information.



To configure the FortiGate:

1. Configure the EMS connector:

```
config endpoint-control fctems
    edit 1
        set status enable
        set name "1"
        set server "172.16.200.167"
        set serial-number <FortiClient_EMS_serial_number>
        set capabilities fabric-auth silent-approval websocket websocket-malware push-
ca-certs common-tags-api
    next
end
```

2. Configure the access proxy VIP for ZTNA:

```
config firewall vip
    edit "ztna_tcp_fwd"
        set type access-proxy
        set extip 11.11.11.174
        set extintf "port1"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

3. Configure the firewall addresses for PC4 and Win Server:

```
config firewall address
    edit "pc4"
        set ip "172.16.200.44/32”
    next
    edit "win2016_server"
        set ip "172.16.200.188/32”
    next
end
```

4. Configure the firewall access proxy and map it to each service:

```
config firewall access-proxy
    edit "ztna_tcp_fwd"
        set vip "ztna_tcp_fwd"
        set add-vhost-domain-to-dnsdb enable
        config api-gateway
```

```
            edit 1
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "pc4_addr"
                        set mappedport 22
                    next
                    edit 2
                        set address "win2016_server"
                        set mappedport 3389
                    next
                end
            next
        end
    next
end
```

5. Configure the ZTNA policy:

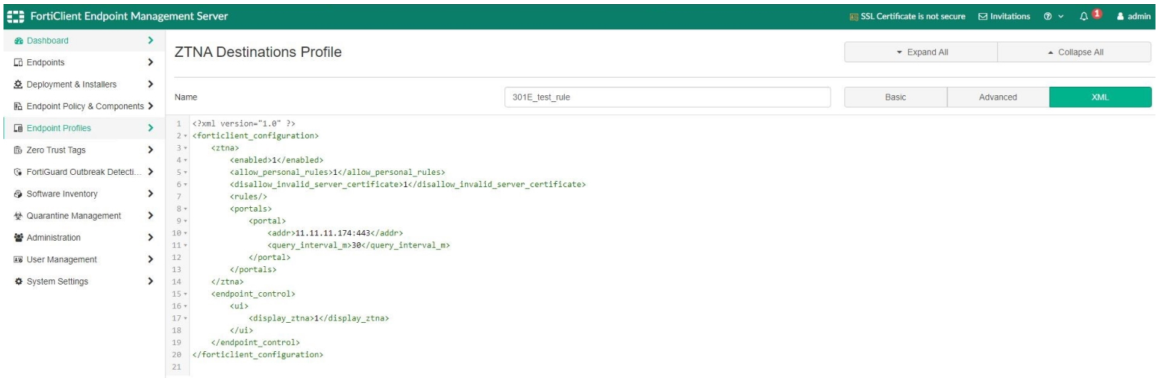
```
config firewall proxy-policy
    edit 1
        set name "ztna_test_rule"
        set proxy access-proxy
        set access-proxy "ztna_tcp_fwd"
        set srcintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
    next
end
```

To configure FortiClient EMS to push the ZTNA access portal gateway to managed endpoints:

1. Log in to the FortiClient EMS and go to *Endpoint Profiles* > *ZTNA Destinations*.
2. Select an existing profile and click *Edit*, or add a new profile.
3. Click *XML* to switch the view from basic to XML.
4. Click *Edit* to edit the XML content, and enter the ZTNA access portal gateway settings:

```
<?xml version="1.0" ?>
<forticlient_configuration>
    <ztna>
        <enabled>1</enabled>
    <allow_personal_rules>1</allow_personal_rules>
    <disallow_invalid_server_certificate>1</ disallow_invalid_server_certificate>

        <rules/>
        <portals>
            <portal>
                <addr>11.11.11.174:443</addr>
                <query_interval_m>30</query_interval_m>
            </portal>
        </portals>
    </ztna>
    <endpoint_control>
```

```
            <ui>
                <display_ztna>1</display_ztna>
            </ui>
        </endpoint_control>
    </forticlient_configuration>
```



Name: 301E_test_rule

```
<?xml version="1.0" ?>
<forticlient_configuration>
    <ztna>
        <enabled>1</enabled>
        <allow_personal_rules>1</allow_personal_rules>
        <disallow_invalid_server_certificate>1</disallow_invalid_server_certificate>
        <rules/>
        <portals>
            <portal>
                <addr>11.11.11.174:443</addr>
                <query_interval_m>30</query_interval_m>
            </portal>
        </portals>
    </ztna>
    <endpoint_control>
        <ui>
            <display_ztna>1</display_ztna>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```

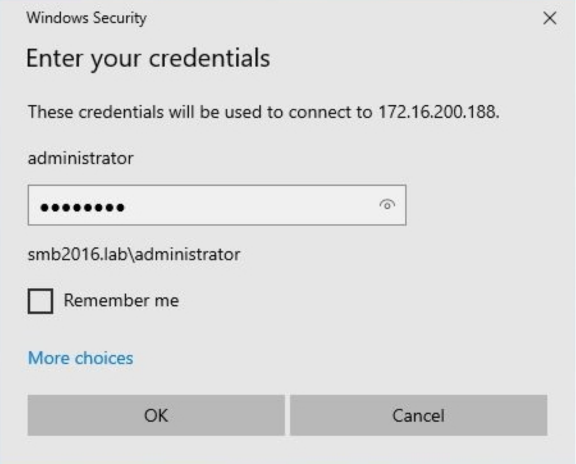
5. Click *Save*. The service portal addresses will be automatically pushed to managed FortiClient endpoints.

To verify that a registered FortiClient endpoint can access the protected services:

1. On a remote PC that has FortiClient installed, ensure that it is registered to FortiClient EMS.
2. Follow the verification steps in FortiGate ZTNA service portal support.
3. On an SSH client, start a connection to the protected SSH server on 172.16.200.44:

   ```
   ssh root@172.16.200.44
   root@172.16.200.44's password:
   ```

   FortiClient will match this traffic to the ZTNA rule learned from the FortiGate service portal and redirect the traffic to it.
4. On an RDP client, start a connection to the protected RDP server on 172.16.200.188.

   Enter your credentials

   These credentials will be used to connect to 172.16.200.188.

   administrator

   ••••••••

   smb2016.lab\administrator

   □ Remember me

   FortiClient will match this traffic to the ZTNA rule learned from the FortiGate service portal and redirect the traffic to it.

ZTNA inline CASB for SaaS application access control - 7.2.1

The FortiGate ZTNA access proxy can be configured to act as an inline cloud access security broker (CASB) by providing access control to software-as-a-service (SaaS) traffic using ZTNA access control rules. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources.

The following components are required to use the ZTNA inline CASB feature:

- The FortiGuard Inline CASB Database (ICDB) used by the FortiGate and FortiClient EMS, which is included with the FortiClient ZTNA license. No separate license is needed for inline CASB.
- A FortiGate ZTNA TCP forwarding access proxy configuration that specifies SaaS application destinations using application names defined in the ICDB
- ZTNA connection rules for SaaS traffic that are provisioned using FortiClient EMS
- FortiClient installed on the user's machine to receive the ZTNA connection rules for SaaS traffic from FortiClient EMS

Support for this feature will be available in a future version of FortiClient and FortiClient EMS.

Previously, ZTNA SaaS access control was possible using the TCP forwarding access proxy configuration on FortiGate and FortiClient:

- On the FortiGate, users would need to search all hostnames used by a SaaS application, configure these hostnames as FQDN addresses, and configure these addresses as part of the ZTNA TCP forwarding settings.
- In FortiClient, users would need to manually add all the hostnames as destinations for ZTNA connection rules or use FortiClient EMS to push those rules to FortiClient.

ZTNA inline CASB for SaaS application access control includes the following functionalities:

- The FortiGuard Inline CASB Database (ICDB) that includes all FQDNs related to specific SaaS applications and corresponding FortiGuard packages for FortiOS and FortiClient. The inline CASB feature is included with the FortiClient ZTNA license. No separate license is needed for inline CASB.
- With the CASB Security Service, users can configure the ZTNA access proxy with a new SaaS proxy access type and conveniently specify SaaS application destinations by application name or by application group name without needing to manually search for and enter FQDNs specific to each SaaS application. This can only be configured in the CLI.
- Users can configure the SaaS application destination in `config firewall proxy-address`, which can be used in `config firewall proxy-policy`.
- The FortiGate traffic log includes a `saasname` field when traffic is controlled by inline CASB for logging SaaS traffic on the FortiGate and FortiAnalyzer.

Supported SaaS applications and SaaS application groups

The inline CASB database, as of version 1.00025, supports the following SaaS applications:

ZTNA access proxy application name	SaaS application
adobe	Adobe services domains

ZTNA access proxy application name	SaaS application
adp	ADP
atlassian	Atlassian
aws_s3	AWS S3
azure	Azure
box	Box
citrix	Citrix
confluence	Confluence
docusign	DocuSign
dropbox	Dropbox
egnyte	Egnyte
github	GitHub
gmail	Gmail
google_cloud	Google Cloud
google_drive	Google Drive
google_office	Google Office
google-web	Google Web Search domains
jira	Jira
ms_excel	Microsoft Excel
ms_exchange	Microsoft Exchange
ms_onedrive	Microsoft OneDrive
ms_outlook	Microsoft Outlook
ms_powerpoint	Microsoft PowerPoint
ms_teams	Microsoft Teams
ms_word	Microsoft Word
salesforce	Salesforce
sap	SAP
sharepoint	SharePoint
webex	Webex
workplace	Workplace
youtube	YouTube

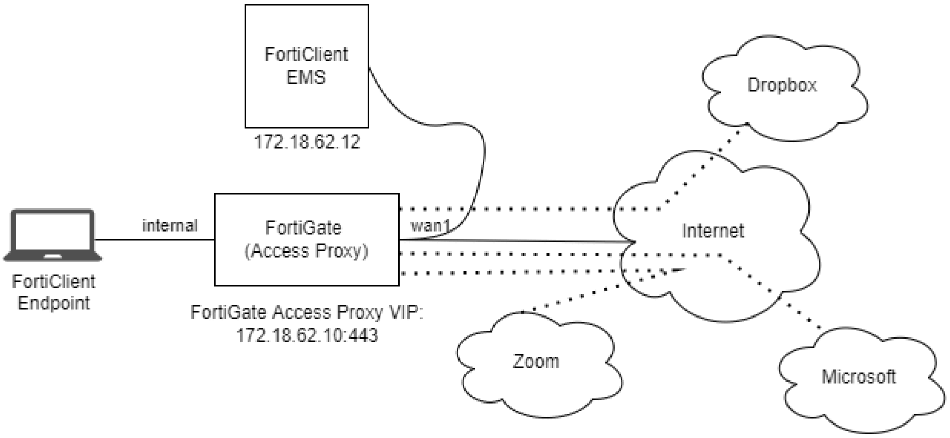
ZTNA access proxy application name	SaaS application
zendesk	Zendesk
zoom	Zoom

The inline CASB database, as of version 1.00025, supports the following SaaS application groups:

ZTNA access proxy application name	SaaS application group
Google	Google SaaS
MS	Microsoft SaaS

Example

In this example, the FortiGate is configured as a ZTNA access proxy with a VIP of 172.18.62.10 and uses the SaaS access proxy type. Dropbox and Zoom SaaS applications are allowed, and the Microsoft SaaS application group is allowed.



Although this topology shows an on-net FortiClient endpoint with respect to the FortiGate, this configuration is also supported with an off-net FortiClient endpoint when the ZTNA access proxy VIP is configured for an external IP address.

The FortiClient EMS in this example uses an external IP address, and it can also be configured to use an internal IP address within the LAN of the FortiGate.

The topology in this example is used for demonstrative purposes only and is not a recommended network topology.

To verify that the ICDB is installed on the FortiGate:

```
# diagnose autoupdate versions
…
Inline CASB Database
---------
Version: 1.00025
Contract Expiry Date: Fri Dec 13 2030
Last Updated using scheduled update on Fri Jul  8 12:19:36 2022
Last Update Attempt: Wed Jul 13 22:42:03 2022
Result: No Updates
```

To configure the FortiGate:

1. Configure the access proxy VIP for ZTNA:

```
config firewall vip
    edit "ZTNA_SaaS"
        set type access-proxy
        set extip 172.18.62.10
        set extintf "internal"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the firewall access proxy using the SaaS proxy access type and specify the SaaS application destinations:

```
config firewall access-proxy
    edit "ZTNA_SaaS"
        set vip "ZTNA_SaaS"
        set log-blocked-traffic enable
        config api-gateway
            edit 1
                set url-map "/saas"
                set service saas
                set application "dropbox" "zoom" "MS"
            next
        end
    next
end
```

3. Optionally, configure the SaaS proxy address, which can be applied in a ZTNA proxy policy:

```
config firewall proxy-address
    edit "ztna_saas_dropbox"
        set type saas
        set application "dropbox"
    next
end
```

4. Configure the ZTNA rule (proxy policy) using the SaaS proxy address as the destination:

```
config firewall proxy-policy
    edit 2
        set name "ZTNA_Rule_SaaS"
        set proxy access-proxy
        set access-proxy "ZTNA_SaaS"
        set srcintf "internal"
        set srcaddr "all"
        set dstaddr "ztna_saas_dropbox"
        set action accept
        set schedule "always"
        set logtraffic all
        set users "ztnauser"
```

```
            set ssl-ssh-profile "custom-deep-inspection"
        next
    end
```

5. Optionally, if user authentication is configured the ZTNA rule (`set users` or `set groups`), configure the authentication scheme and rule (see Configuring the authentication scheme and rule in the ZTNA Deployment guide). The authentication scheme and rule in this example correspond to the local user, `ztnauser`.
   a. Configure the authentication scheme:

```
config authentication scheme
    edit "ZTNA-Auth-scheme"
        set method basic
        set require-tfa disable
        set fsso-guest disable
        set user-database "local-user-db"
    next
end
```

   b. Configure the authentication rule:

```
config authentication rule
    edit "ZTNA-Auth-scheme"
        set status enable
        set protocol http
        set srcintf "internal"
        set srcaddr "all"
        set ip-based enable
        set active-auth-method "ZTNA-Auth-scheme"
        set sso-auth-method ''
        set web-portal enable
        set comments ''
    next
end
```

Testing and results

Before connecting, the users must have corresponding ZTNA connection rules in FortiClient.

Once ZTNA is configured on the FortiGate, ZTNA connection rules in FortiClient are provisioned using FortiClient EMS in one of the following ways:

- In FortiClient EMS, configure SaaS applications in *Endpoint Profiles* > *ZTNA Destinations* and push application destinations to FortiClient. Currently, SaaS application rules are only supported using XML.
- Use the Publishing ZTNA services through the ZTNA portal 7.2.1 on page 336 feature on the FortiGate. FortiClient establishes a tunnel to the FortiGate using the ZTNA web portal and creates ZTNA connection rules based on the SaaS application destinations.

Once connected, the FortiClient retrieves the list of hosted ZTNA services, including the SaaS service, and adds corresponding ZTNA connection rules for the configured SaaS applications.

To view the traffic logs on the FortiGate:

```
# execute log filter category 0
# execute log filter field subtype ztna
# execute log filter field accessproxy ZTNA_SaaS
# execute log display
```

```
1: date=2022-07-21 time=10:37:54 eventtime=1658425074787641779 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=192.168.1.113 srcname="ubuntu-
vm" srcport=58362 srcintf="internal" srcintfrole="lan" dstcountry="United States"
srccountry="Reserved" dstip=162.125.248.18 dstport=443 dstintf="wan1" dstintfrole="wan"
sessionid=3417 service="HTTPS" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="07370508-086d-51ed-3c08-86ba8f10f75e" policyname="ZTNA_Rule_SaaS" duration=76
user="ztnauser" gatewayid=1 vip="ZTNA_SaaS" accessproxy="ZTNA_SaaS" saasname="dropbox"
wanin=3964 rcvdbyte=3964 wanout=1406 lanin=3329 sentbyte=3329 lanout=6228 unauthuser="user1"
unauthusersource="forticlient" appcat="unscanned"

2: date=2022-07-21 time=10:36:53 eventtime=1658425014191265858 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=192.168.1.113 srcname="ubuntu-
vm" srcport=58582 srcintf="internal" srcintfrole="lan" dstcountry="United States"
srccountry="Reserved" dstip=162.125.35.138 dstport=443 dstintf="wan1" dstintfrole="wan"
sessionid=3591 service="HTTPS" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="07370508-086d-51ed-3c08-86ba8f10f75e" policyname="ZTNA_Rule_SaaS" duration=0
user="ztnauser" gatewayid=1 vip="ZTNA_SaaS" accessproxy="ZTNA_SaaS" saasname="dropbox"
wanin=3408 rcvdbyte=3408 wanout=453 lanin=2464 sentbyte=2464 lanout=5234 unauthuser="user1"
unauthusersource="forticlient" appcat="unscanned"
```

ZTNA policy access control of unmanaged devices - 7.2.1

The ZTNA access proxy can determine whether a client device that does not have FortiClient installed is a mobile device that is considered unmanageable, or is not a mobile device that is considered unknown. The ZTNA access proxy tags the device as either `ems-tag-unmanageable` or `ems-tag-unknown` respectively. The FortiGate WAD process achieves this by either matching device TLS fingerprints against a library or learning information from the HTTP User-Agent header if the `set user-agent-detect` setting is enabled.

The `ems-tag-unmanageable` and `ems-tag-unknown` tags allow for ZTNA access control of unmanaged devices using a proxy policy. The `accept-unmanageable` option for the `empty-cert-action` setting allows unmanageable clients to continue ZTNA proxy rule processing.

```
config firewall access-proxy
    edit <name>
        set client-cert enable
        set user-agent-detect {enable | disable}
        set empty-cert-action {accept | block | accept-unmanageable}
     next
end
```

`user-agent-detect {enable	disable}`	Enable/disable detecting the device type by HTTP User-Agent if no client certificate is provided (default = enable).
`empty-cert-action {accept	block	accept-unmanageable}`	Set the action for an empty client certificate: • `accept`: accept the SSL handshake if the client certificate is empty. • `block`: block the SSL handshake if the client certificate is empty. • `accept-unmanageable`: accept the SSL handshake only if the end point is unmanageable.

```
config firewall proxy-policy
    edit <id>
        set ztna-ems-tag {ems-tag-unmanageable | ems-tag-unknown}
    next
end
```

`ztna-ems-tag {ems-tag-unmanageable | ems-tag-unknown}`	Set the EMS tag names: • `ems-tag-unmanageable`: match any device that is unmanageable. • `ems-tag-unknown`: match any device that is not recognized.

Consider the following use cases.

- Case 1: if a client device sends a TLS client hello in a mobile pattern, then WAD will try to match its TLS fingerprint with a WAD original library and mark it with an `ems-tag-unmanageable` tag.
- Case 2: if WAD cannot match the TLS fingerprint with an original library but `user-agent-detect` is enabled (under `config firewall access-proxy`), WAD will try to learn the device type from client request's User-Agent header. If it matches a mobile device, then it is still marked with an `ems-tag-unmanageable` tag.
- Case 3: if WAD cannot match the TLS fingerprint with an existing original or temporary library, or cannot learn it from User-Agent header, or `user-agent-detect` is disabled, then it will mark the device as `ems-tag-unknown`.

In the access proxy settings, if `empty-cert-action` is set to `accept-unmanageable`, then only case 1 and 2 would go through the proxy policy. Case 3 would be denied, and a replacement message page would appear.

Example

To configure ZTNA policy access control of unmanaged devices:

1. Configure the client certificate actions:

```
config firewall access-proxy
    edit "zt1"
        set vip "zt1"
        set client-cert enable
        set user-agent-detect enable
        set auth-portal disable
        set empty-cert-action accept
        set log-blocked-traffic disable
        set add-vhost-domain-to-dnsdb disable
        set decrypted-traffic-mirror ''
    next
end
```

2. Configure the proxy policy with the `ems-tag-unmanageable` tag:

```
config firewall proxy-policy
    edit 1
        set proxy access-proxy
        set access-proxy "zt1"
        set srcintf "port2" "ag2"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "ems-tag-unmanageable"
    next
end
```

HTTP2 connection coalescing and concurrent multiplexing for ZTNA, virtual server load balancing, and explicit proxy - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- HTTP2 connection coalescing and concurrent multiplexing for ZTNA
- HTTP2 connection coalescing and concurrent multiplexing for virtual server load balancing
- HTTP connection coalescing and concurrent multiplexing for explicit proxy

HTTP2 connection coalescing and concurrent multiplexing allows multiple HTTP2 requests to share the same TLS connection when the destination IP is the same, and the host names are compatible in the certificate. This is supported for ZTNA, virtual server load balancing, and explicit proxy.

Basic settings

To configure the ZTNA access proxy:

```
config firewall access-proxy
    edit <name>
        set http-supported-max-version {http1 | http2}
        set svr-pool-multiplex {enable | disable}
        set svr-pool-ttl <integer>
        set svr-pool-server-max-request <integer>
    next
end
```

`http-supported-max-version {http1 | http2}`	Set the maximum supported HTTP version: • http1: support HTTP 1.1 and HTTP1. • http2: support HTTP2, HTTP 1.1, and HTTP1 (default).
`svr-pool-multiplex {enable | disable}`	Enable/disable server pool multiplexing. When enabled, share the connected server in HTTP, HTTPS, and web portal API gateway.
`svr-pool-ttl <integer>`	Set the time-to-live in the server pool for idle connections to servers (in seconds, 0 - 2147483647, default = 15).
`svr-pool-server-max-request <integer>`	Set the maximum number of requests that servers in server pool handle before disconnecting (0 - 2147483647, default = 0).

To configure the load balanced virtual server:

```
config firewall vip
    edit <name>
        set type server-load-balance
        set server-type {http | https}
        set http-multiplex {enable | disable}
        set http-multiplex-ttl <integer>
        set http-multiplex-max-request <integer>
        set http-supported-max-version {http1 | http2}
    next
end
```

`http-multiplex {enable | disable}`	Enable/disable HTTP multiplexing.
`http-multiplex-ttl <integer>`	Set the time-to-live for idle connections to servers (in seconds, 0 - 2147483647, default = 15).
`http-multiplex-max-request <integer>`	Set the maximum number of requests that the multiplex server can handle before disconnecting (0 - 2147483647, default = 0).
`http-supported-max-version {http1 | http2}`	Set the maximum supported HTTP version: • http1: support HTTP 1.1 and HTTP1. • http2: support HTTP2, HTTP 1.1, and HTTP1 (default).

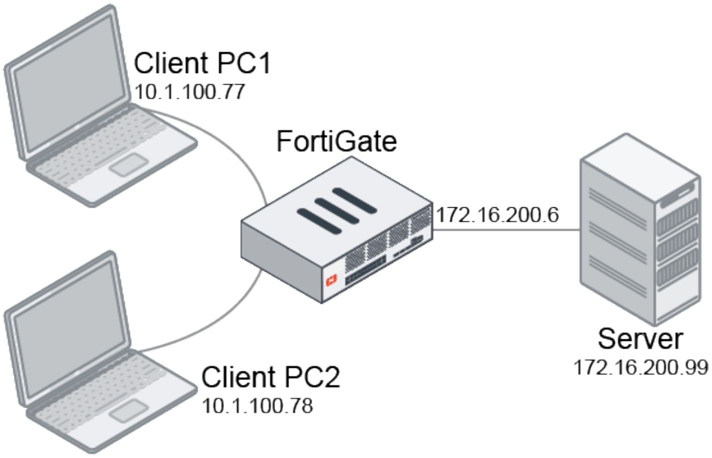
To configure the explicit web proxy:

```
config web-proxy explicit
    set http-connection-mode {static | multiplex | serverpool}
end
```

`http-connection-mode {static | multiplex | serverpool}`	Set the HTTP connection mode: • static: only one server connection exists during the proxy session (default). • multiplex: hold established connections until the proxy session ends. • serverpool: share established connections with other proxy sessions.

Examples

In the following examples, multiple clients submit requests in HTTP2. The requests hit the VIP address, and then FortiGate opens a session between itself (172.16.200.6) and the server (172.16.200.99). The coalescing occurs in this session as the multiple streams share the same TLS session to connect to the same destination server.



ZTNA

In ZTNA scenarios, the FortiGate application gateway may accept multiple HTTP2 requests to the same ZTNA server destined to different virtual hosts on the same real server. These HTTP2 requests can share the same TLS connection between the FortiGate and the real server so that the handshake does not need to be performed multiple times for multiple connections.

In order for the FortiGate to match the SNI (Server Name Indication), this SNI value must appear under the SAN extension on the server certificate. Configuring the SNI value under the CN alone will not work.

To configure connection coalescing and concurrent multiplexing with ZTNA:

1. Configure the VIP:

```
config firewall vip
    edit "vip-ztna"
        set type access-proxy
        set extip 10.1.100.223
        set extintf "port2"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the ZTNA server and path mapping:

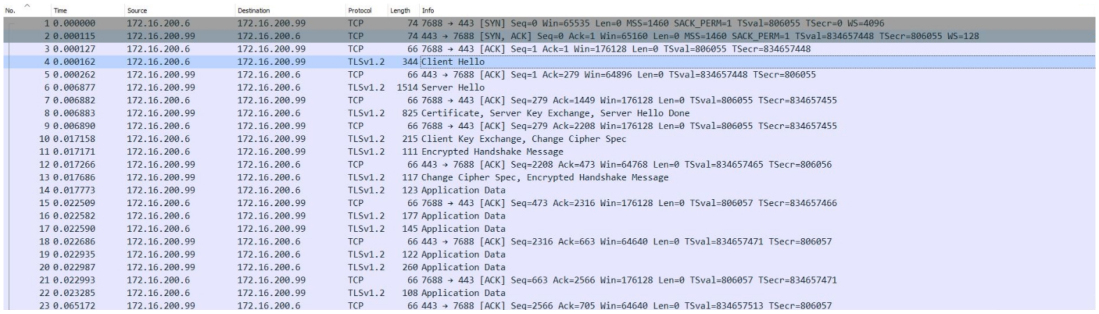
```
config firewall access-proxy
    edit "ztna"
        set vip "vip-ztna"
        set client-cert disable
        set svr-pool-multiplex enable
        set http-supported-max-version http2
        config api-gateway
            edit 1
                set url-map "/a"
                set virtual-host "a.ftnt.com"
                config realservers
                    edit 1
                        set ip 172.16.200.99
                    next
                end
            next
            edit 2
                set url-map "/b"
                set virtual-host "b.ftnt.com"
                config realservers
                    edit 1
                        set ip 172.16.200.99
                    next
                end
            next
        end
    next
end
```

3. Configure the ZTNA policy:

```
config firewall proxy-policy
    edit 3
        set proxy access-proxy
        set access-proxy "ztna"
```

```
            set srcintf "port2"
            set srcaddr "all"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set logtraffic all
            set utm-status enable
            set ssl-ssh-profile "deep-inspection-clone"
            set av-profile "av"
        next
    end
```

4. Get the clients to access a.ftnt.com and b.ftnt.com. The clients share access with the same real server and certificate (CN=*.ftnt.com). The FortiGate shares the first TLS connection with second TLS connection.
5. Verify the sniffer packet capture on the FortiGate server side. There is one client hello.

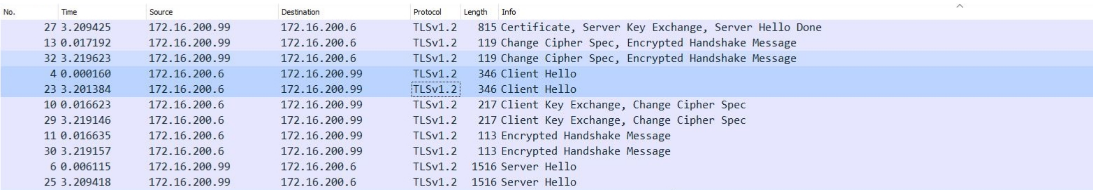


```
No.  Time      Source         Destination    Protocol Length Info
   1 0.000000  172.16.200.6   172.16.200.99  TCP        74 7688 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=806055 TSecr=0 WS=4096
   2 0.000115  172.16.200.99  172.16.200.6   TCP        74 443 → 7688 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=834657448 TSecr=806055 WS=128
   3 0.000127  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=806055 TSecr=834657448
   4 0.000162  172.16.200.6   172.16.200.99  TLSv1.2   344 Client Hello
   5 0.000262  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=1 Ack=279 Win=64896 Len=0 TSval=834657448 TSecr=806055
   6 0.006877  172.16.200.99  172.16.200.6   TLSv1.2  1514 Server Hello
   7 0.006882  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=279 Ack=1449 Win=176128 Len=0 TSval=806055 TSecr=834657455
   8 0.006883  172.16.200.99  172.16.200.6   TLSv1.2   825 Certificate, Server Key Exchange, Server Hello Done
   9 0.006890  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=279 Ack=2208 Win=176128 Len=0 TSval=806055 TSecr=834657455
  10 0.017158  172.16.200.6   172.16.200.99  TLSv1.2   215 Client Key Exchange, Change Cipher Spec
  11 0.017171  172.16.200.6   172.16.200.99  TLSv1.2   111 Encrypted Handshake Message
  12 0.017266  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=2208 Ack=473 Win=64768 Len=0 TSval=834657465 TSecr=806056
  13 0.017686  172.16.200.99  172.16.200.6   TLSv1.2   117 Change Cipher Spec, Encrypted Handshake Message
  14 0.017773  172.16.200.99  172.16.200.6   TLSv1.2   123 Application Data
  15 0.022509  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=473 Ack=2316 Win=176128 Len=0 TSval=806057 TSecr=834657466
  16 0.022582  172.16.200.6   172.16.200.99  TLSv1.2   177 Application Data
  17 0.022590  172.16.200.6   172.16.200.99  TLSv1.2   145 Application Data
  18 0.022686  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=2316 Ack=663 Win=64640 Len=0 TSval=834657471 TSecr=806057
  19 0.022935  172.16.200.99  172.16.200.6   TLSv1.2   122 Application Data
  20 0.022987  172.16.200.99  172.16.200.6   TLSv1.2   260 Application Data
  21 0.022993  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=663 Ack=2566 Win=176128 Len=0 TSval=806057 TSecr=834657471
  22 0.023285  172.16.200.6   172.16.200.99  TLSv1.2   108 Application Data
  23 0.065172  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=2566 Ack=705 Win=64640 Len=0 TSval=834657513 TSecr=806057
```

6. Disable server pool multiplexing:

```
config firewall access-proxy
    edit "ztna"
        set vip "vip-ztna"
        set svr-pool-multiplex disable
    next
end
```

7. Verify the sniffer packet capture. This time, the FortiGate does not coalesce the TLS connection, so there are two client hellos.



```
No.  Time      Source         Destination    Protocol Length Info
  27 3.209425  172.16.200.99  172.16.200.6   TLSv1.2   815 Certificate, Server Key Exchange, Server Hello Done
  13 0.017192  172.16.200.99  172.16.200.6   TLSv1.2   119 Change Cipher Spec, Encrypted Handshake Message
  32 3.219623  172.16.200.99  172.16.200.6   TLSv1.2   119 Change Cipher Spec, Encrypted Handshake Message
   4 0.000160  172.16.200.6   172.16.200.99  TLSv1.2   346 Client Hello
  23 3.201384  172.16.200.6   172.16.200.99  TLSv1.2   346 Client Hello
  10 0.016623  172.16.200.6   172.16.200.99  TLSv1.2   217 Client Key Exchange, Change Cipher Spec
  29 3.219146  172.16.200.6   172.16.200.99  TLSv1.2   217 Client Key Exchange, Change Cipher Spec
  11 0.016635  172.16.200.6   172.16.200.99  TLSv1.2   113 Encrypted Handshake Message
  30 3.219157  172.16.200.6   172.16.200.99  TLSv1.2   113 Encrypted Handshake Message
   6 0.006115  172.16.200.99  172.16.200.6   TLSv1.2  1516 Server Hello
  25 3.209418  172.16.200.99  172.16.200.6   TLSv1.2  1516 Server Hello
```

Virtual server load balancing

To configure connection coalescing and concurrent multiplexing with virtual server load balancing:

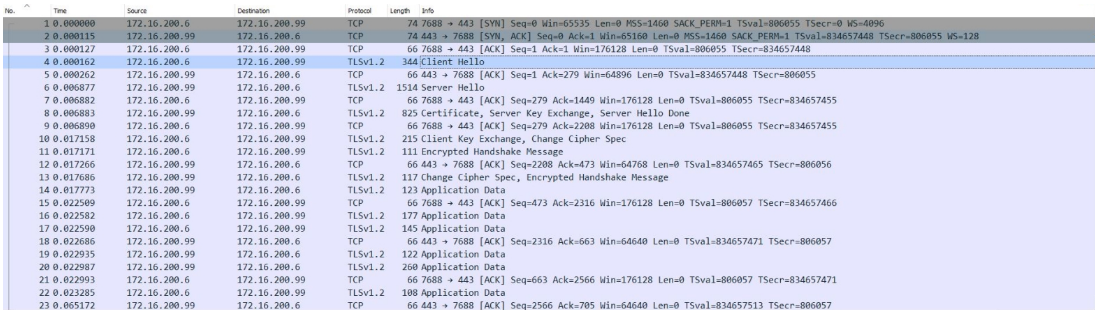
1. Configure the virtual server:

```
config firewall vip
    edit "vip-test"
        set type server-load-balance
        set extip 10.1.100.222
        set extintf "port2"
        set server-type https
        set extport 443
        config realservers
            edit 1
                set ip 172.16.200.99
                set port 443
            next
        end
        set http-multiplex enable
        set ssl-mode full
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "vip-test"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "deep-inspection-clone"
        set av-profile "av"
        set logtraffic all
        set nat enable
    next
end
```

3. Get the clients to access the VIP address (10.1.100.222). The FortiGate shares the first TLS connection with second TLS connection.
4. Verify the sniffer packet capture on the FortiGate server side. There is one client hello.

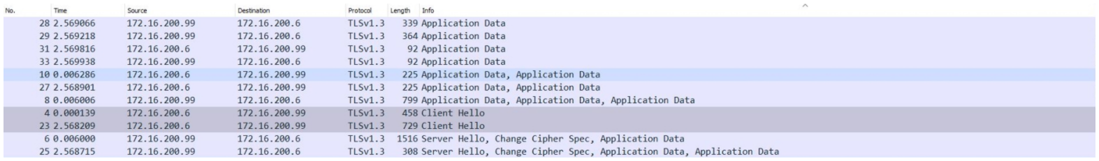


```
No.  Time      Source         Destination    Protocol Length Info
   1 0.000000  172.16.200.6   172.16.200.99  TCP        74 7688 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=806055 TSecr=0 WS=4096
   2 0.000115  172.16.200.99  172.16.200.6   TCP        74 443 → 7688 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=834657448 TSecr=806055 WS=128
   3 0.000127  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=806055 TSecr=834657448
   4 0.000162  172.16.200.6   172.16.200.99  TLSv1.2   344 Client Hello
   5 0.000262  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=1 Ack=279 Win=64896 Len=0 TSval=834657448 TSecr=806055
   6 0.006877  172.16.200.99  172.16.200.6   TLSv1.2  1514 Server Hello
   7 0.006882  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=279 Ack=1449 Win=176128 Len=0 TSval=806055 TSecr=834657455
   8 0.006883  172.16.200.99  172.16.200.6   TLSv1.2   825 Certificate, Server Key Exchange, Server Hello Done
   9 0.006890  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=279 Ack=2208 Win=176128 Len=0 TSval=806055 TSecr=834657455
  10 0.017158  172.16.200.6   172.16.200.99  TLSv1.2   215 Client Key Exchange, Change Cipher Spec
  11 0.017171  172.16.200.6   172.16.200.99  TLSv1.2   111 Encrypted Handshake Message
  12 0.017266  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=2208 Ack=473 Win=64768 Len=0 TSval=834657465 TSecr=806056
  13 0.017686  172.16.200.99  172.16.200.6   TLSv1.2   117 Change Cipher Spec, Encrypted Handshake Message
  14 0.017773  172.16.200.99  172.16.200.6   TLSv1.2   123 Application Data
  15 0.022509  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=473 Ack=2316 Win=176128 Len=0 TSval=806057 TSecr=834657466
  16 0.022582  172.16.200.6   172.16.200.99  TLSv1.2   177 Application Data
  17 0.022590  172.16.200.6   172.16.200.99  TLSv1.2   145 Application Data
  18 0.022686  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=2316 Ack=663 Win=64640 Len=0 TSval=834657471 TSecr=806057
  19 0.022935  172.16.200.99  172.16.200.6   TLSv1.2   122 Application Data
  20 0.022987  172.16.200.99  172.16.200.6   TLSv1.2   260 Application Data
  21 0.022993  172.16.200.6   172.16.200.99  TCP        66 7688 → 443 [ACK] Seq=663 Ack=2566 Win=176128 Len=0 TSval=806057 TSecr=834657471
  22 0.023285  172.16.200.6   172.16.200.99  TLSv1.2   108 Application Data
  23 0.065172  172.16.200.99  172.16.200.6   TCP        66 443 → 7688 [ACK] Seq=2566 Ack=705 Win=64640 Len=0 TSval=834657513 TSecr=806057
```

5. Disable HTTP multiplexing:

```
config firewall vip
    edit "vip-test"
        config realservers
            edit 1
                set type ip
                set ip 172.16.200.99
                set port 443
            next
        end
        set http-multiplex disable
    next
end
```

6. Verify the sniffer packet capture. This time, the FortiGate does reuse the TLS connection, so there are two client hellos sent to the real server.



```
No.  Time      Source          Destination     Protocol  Length  Info
  28 2.569066  172.16.200.99   172.16.200.6    TLSv1.3    339 Application Data
  29 2.569218  172.16.200.99   172.16.200.6    TLSv1.3    364 Application Data
  31 2.569816  172.16.200.6    172.16.200.99   TLSv1.3     92 Application Data
  33 2.569938  172.16.200.99   172.16.200.6    TLSv1.3     92 Application Data
  10 0.006286  172.16.200.6    172.16.200.99   TLSv1.3    225 Application Data, Application Data
  27 2.568901  172.16.200.6    172.16.200.99   TLSv1.3    225 Application Data, Application Data
   8 0.006006  172.16.200.99   172.16.200.6    TLSv1.3    799 Application Data, Application Data, Application Data
   4 0.000139  172.16.200.6    172.16.200.99   TLSv1.3    458 Client Hello
  23 2.568209  172.16.200.6    172.16.200.99   TLSv1.3    729 Client Hello
   6 0.006000  172.16.200.99   172.16.200.6    TLSv1.3   1516 Server Hello, Change Cipher Spec, Application Data
  25 2.568715  172.16.200.99   172.16.200.6    TLSv1.3    308 Server Hello, Change Cipher Spec, Application Data, Application Data
```

Explicit proxy

To configure connection coalescing and concurrent multiplexing with an explicit proxy:

1. Configure the explicit web proxy:

```
config web-proxy explicit
    set status enable
    set http-incoming-port 8080
    set http-connection-mode serverpool
end
```

Connection coalescing and concurrent multiplexing with an explicit proxy only supports HTTP.

2. Enable explicit web proxy on port2:

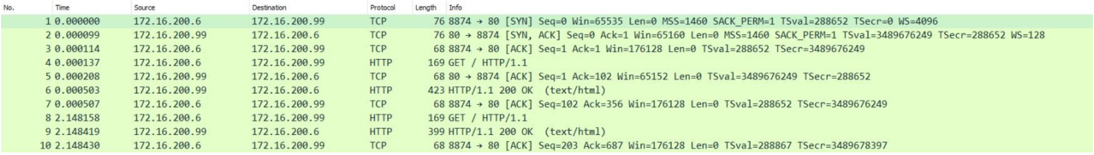
```
config system interface
    edit "port2"
        set ip 10.1.100.6 255.255.255.0
        set explicit-web-proxy enable
    next
end
```

3. Configure the proxy policy:

```
config firewall proxy-policy
    edit 1
        set proxy explicit-web
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set service "web"
        set action accept
        set schedule "always"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set utm-status enable
```

```
            set profile-protocol-options "default-clone"
            set ssl-ssh-profile "deep-inspection-clone"
        next
    end
```

4. Get the clients to access the server through the explicit web proxy (10.1.100.6:8080). The FortiGate shares the first connection TCP three-way handshake with later connections that connect to same destination address.
5. Verify the sniffer packet capture on the FortiGate server side. There is one TCP three-way handshake, but there are two HTTP connections.

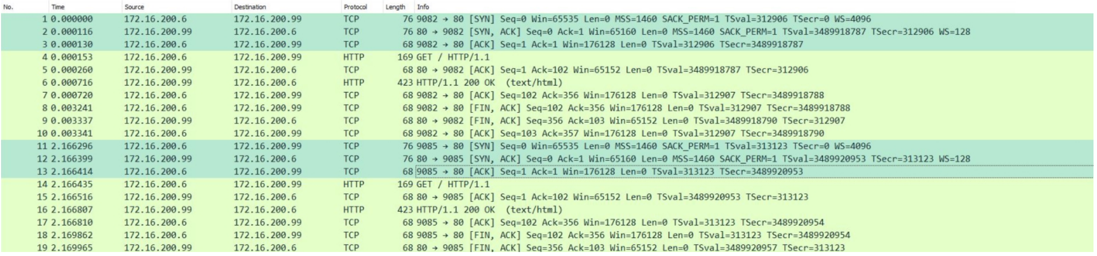


```
No.   Time       Source          Destination     Protocol  Length  Info
    1 0.000000   172.16.200.6    172.16.200.99   TCP        76 8874 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=288652 TSecr=0 WS=4096
    2 0.000099   172.16.200.99   172.16.200.6    TCP        76 80 → 8874 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3489676249 TSecr=288652 WS=128
    3 0.000114   172.16.200.6    172.16.200.99   TCP        68 8874 → 80 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=288652 TSecr=3489676249
    4 0.000137   172.16.200.6    172.16.200.99   HTTP      169 GET / HTTP/1.1
    5 0.000208   172.16.200.99   172.16.200.6    TCP        68 80 → 8874 [ACK] Seq=1 Ack=102 Win=65152 Len=0 TSval=3489676249 TSecr=288652
    6 0.000503   172.16.200.99   172.16.200.6    HTTP      423 HTTP/1.1 200 OK  (text/html)
    7 0.000507   172.16.200.6    172.16.200.99   TCP        68 8874 → 80 [ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=288652 TSecr=3489676249
    8 2.148158   172.16.200.6    172.16.200.99   HTTP      169 GET / HTTP/1.1
    9 2.148419   172.16.200.99   172.16.200.6    HTTP      399 HTTP/1.1 200 OK  (text/html)
   10 2.148430   172.16.200.6    172.16.200.99   TCP        68 8874 → 80 [ACK] Seq=203 Ack=687 Win=176128 Len=0 TSval=288867 TSecr=3489678397
```

6. Change the HTTP connection mode to static:

```
config web-proxy explicit
    set status enable
    set http-incoming-port 8080
    set http-connection-mode static
end
```

7. Verify the sniffer packet capture. This time, the FortiGate establishes a TCP connection for each client.



```
No.   Time       Source          Destination     Protocol  Length  Info
    1 0.000000   172.16.200.6    172.16.200.99   TCP        76 9082 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=312906 TSecr=0 WS=4096
    2 0.000116   172.16.200.99   172.16.200.6    TCP        76 80 → 9082 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3489918787 TSecr=312906 WS=128
    3 0.000130   172.16.200.6    172.16.200.99   TCP        68 9082 → 80 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=312906 TSecr=3489918787
    4 0.000153   172.16.200.6    172.16.200.99   HTTP      169 GET / HTTP/1.1
    5 0.000260   172.16.200.99   172.16.200.6    TCP        68 80 → 9082 [ACK] Seq=1 Ack=102 Win=65152 Len=0 TSval=3489918787 TSecr=312906
    6 0.000716   172.16.200.99   172.16.200.6    HTTP      423 HTTP/1.1 200 OK  (text/html)
    7 0.000720   172.16.200.6    172.16.200.99   TCP        68 9082 → 80 [ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=312907 TSecr=3489918788
    8 0.003241   172.16.200.6    172.16.200.99   TCP        68 9082 → 80 [FIN, ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=312907 TSecr=3489918788
    9 0.003337   172.16.200.99   172.16.200.6    TCP        68 80 → 9082 [FIN, ACK] Seq=356 Ack=103 Win=65152 Len=0 TSval=3489918790 TSecr=312907
   10 0.003341   172.16.200.6    172.16.200.99   TCP        68 9082 → 80 [ACK] Seq=103 Ack=357 Win=176128 Len=0 TSval=312907 TSecr=3489918790
   11 2.166296   172.16.200.6    172.16.200.99   TCP        76 9085 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=313123 TSecr=0 WS=4096
   12 2.166399   172.16.200.99   172.16.200.6    TCP        76 80 → 9085 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3489920953 TSecr=313123 WS=128
   13 2.166414   172.16.200.6    172.16.200.99   TCP        68 9085 → 80 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=313123 TSecr=3489920953
   14 2.166435   172.16.200.6    172.16.200.99   HTTP      169 GET / HTTP/1.1
   15 2.166516   172.16.200.99   172.16.200.6    TCP        68 80 → 9085 [ACK] Seq=1 Ack=102 Win=65152 Len=0 TSval=3489920953 TSecr=313123
   16 2.166807   172.16.200.99   172.16.200.6    HTTP      423 HTTP/1.1 200 OK  (text/html)
   17 2.166810   172.16.200.6    172.16.200.99   TCP        68 9085 → 80 [ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=313123 TSecr=3489920954
   18 2.169862   172.16.200.6    172.16.200.99   TCP        68 9085 → 80 [FIN, ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=313123 TSecr=3489920954
   19 2.169965   172.16.200.99   172.16.200.6    TCP        68 80 → 9085 [FIN, ACK] Seq=356 Ack=103 Win=65152 Len=0 TSval=3489920957 TSecr=313123
```

ZTNA policy access control of unmanageable and unknown devices with dynamic address local tags - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- ZTNA policy access control of unmanageable and unknown devices with dynamic address local tags

The ZTNA application gateway can determine whether a client device that does not have FortiClient installed is a mobile device that is considered unmanageable, or is not a mobile device that is considered unknown. The ZTNA access proxy tags the device as either `EMS_ALL_UNMANAGEABLE_CLIENTS` or `EMS_ALL_UNKNOWN_CLIENTS` respectively. The FortiGate WAD process achieves this by either matching device TLS fingerprints against a library or learning information from the HTTP User-Agent header if the `set user-agent-detect` setting is enabled.

The `EMS_ALL_UNMANAGEABLE_CLIENTS` and `EMS_ALL_UNKNOWN_CLIENTS` tags are different than the `ems-tag-unmanageable` and `ems-tag-unknown` tags introduced in FortiOS 7.2.1. Upgrading from FortiOS 7.2.1 or later to FortiOS 7.2.4 does not preserve these older tags.

Configuring the ZTNA access proxy and proxy policy

The `EMS_ALL_UNMANAGEABLE_CLIENTS` and `EMS_ALL_UNKNOWN_CLIENTS` tags allow for ZTNA access control of unmanageable and unknown devices using a proxy policy. The `accept-unmanageable` option for the `empty-cert-action` setting allows unmanageable clients to continue ZTNA proxy rule processing.

```
config firewall access-proxy
    edit <name>
        set client-cert enable
        set user-agent-detect {enable | disable}
        set empty-cert-action {accept | block | accept-unmanageable}
     next
end
```

`user-agent-detect {enable	disable}`	Enable/disable detecting the device type by HTTP User-Agent if no client certificate is provided (default = enable).
`empty-cert-action {accept	block	accept-unmanageable}`	Set the action for an empty client certificate: • `accept`: accept the SSL handshake if the client certificate is empty. • `block`: block the SSL handshake if the client certificate is empty. • `accept-unmanageable`: accept the SSL handshake only if the end point is unmanageable.

The `user-agent-detect` and `empty-cert-action` settings can only be configured in the CLI.

```
config firewall proxy-policy
    edit <id>
        set ztna-ems-tag {EMS_ALL_UNMANAGEABLE_CLIENTS | EMS_ALL_UNKNOWN_CLIENTS}
    next
end
```

`ztna-ems-tag {EMS_ALL_UNMANAGEABLE_CLIENTS	EMS_ALL_UNKNOWN_CLIENTS}`	Set the EMS tag names: • `EMS_ALL_UNMANAGEABLE_CLIENTS`: match any device that is unmanageable. • `EMS_ALL_UNKNOWN_CLIENTS`: match any device that is not recognized.

Consider the following use cases.

- Case 1: if a client device sends a TLS client hello in a mobile pattern, then WAD will try to match its TLS fingerprint with a WAD original library and mark it with an `EMS_ALL_UNMANAGEABLE_CLIENTS` tag.
- Case 2: if WAD cannot match the TLS fingerprint with an original library but `user-agent-detect` is enabled (under `config firewall access-proxy`), WAD will try to learn the device type from client request's User-Agent header. If it matches a mobile device, then it is still marked with an `EMS_ALL_UNMANAGEABLE_CLIENTS` tag.
- Case 3: if WAD cannot match the TLS fingerprint with an existing original or temporary library, or cannot learn it from User-Agent header, or `user-agent-detect` is disabled, then it will mark the device as `EMS_ALL_UNKNOWN_CLIENTS`.

In the access proxy settings, if `empty-cert-action` is set to `accept-unmanageable`, then only case 1 and 2 would go through the proxy policy. Case 3 would be denied, and a replacement message page would appear.

To configure ZTNA policy access control of unmanageable devices:

1. Configure the client certificate actions:

```
config firewall access-proxy
    edit "zt1"
        set vip "zt1"
        set client-cert enable
        set user-agent-detect enable
        set auth-portal disable
        set empty-cert-action accept
        set log-blocked-traffic disable
        set add-vhost-domain-to-dnsdb disable
        set decrypted-traffic-mirror ''
    next
end
```

2. Configure the proxy policy with the ZTNA EMS tag to control device access:

```
config firewall proxy-policy
    edit 1
        set proxy access-proxy
        set access-proxy "zt1"
        set srcintf "port2" "ag2"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "EMS_ALL_UNMANAGEABLE_CLIENTS"
    next
end
```

Configuring dynamic address local tags

Like other ZTNA tags,`EMS_ALL_UNMANAGEABLE_CLIENTS` and `EMS_ALL_UNKNOWN_CLIENTS` are dynamic addresses on the FortiGate. The following diagnostic commands can be used to view local tag information:

- `diagnose firewall dynamic address`: a list of unmanageable and unknown clients' IP addresses associated with the `EMS_ALL_MANAGEABLE_CLIENTS` and `EMS_ALL_UNKNOWN_CLIENTS` dynamic addresses, respectively, is displayed.
- `diagnose user-device-store device memory list`: when device detection is enabled on a FortiGate interface that has a layer 2 connection to unmanageable and unknown device clients, then a client's device information is displayed.

To verify the list of dynamic firewall addresses in the CLI:

```
(vdom1) # diagnose firewall dynamic address
List all dynamic addresses:
IP dynamic addresses in VDOM vdom1(vfid: 1):
...
CMDB name: EMS_ALL_UNMANAGEABLE_CLIENTS
EMS_ALL_UNMANAGEABLE_CLIENTS: ID(101)
        ADDR(10.1.100.22)
Total IP dynamic range blocks: 1.
Total IP dynamic addresses: 1.
CMDB name: EMS_ALL_UNKNOWN_CLIENTS
EMS_ALL_UNKNOWN_CLIENTS: ID(154)
```

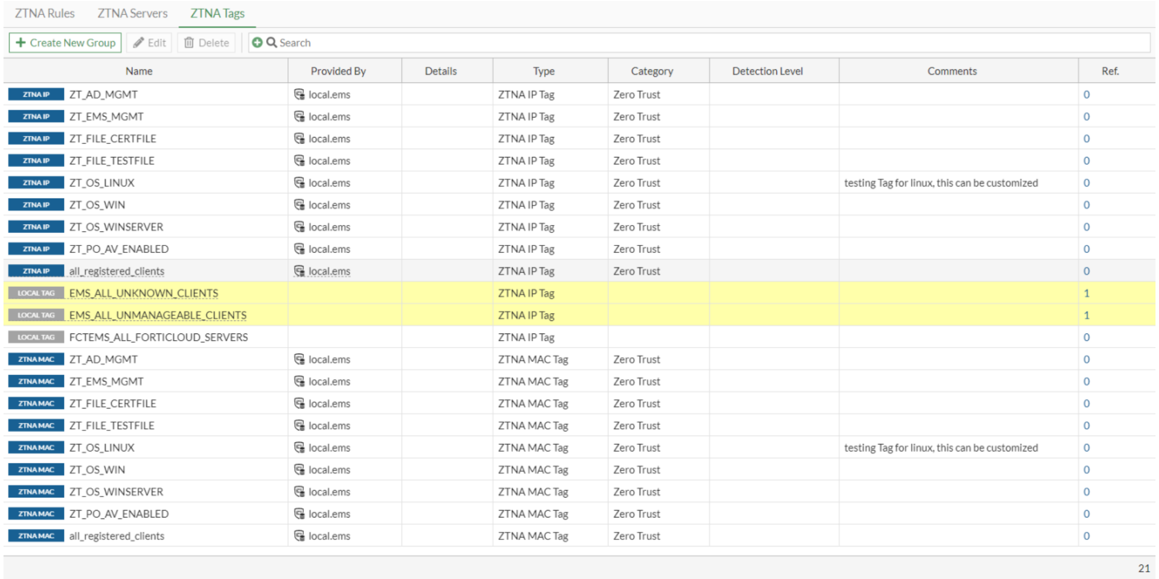
```
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 0.
...
```

To verify the client device information in the CLI:

```
(vdom1) # diagnose user-device-store device memory list
Record #1:
          ...
        device_info
                ...
                'is_online' = 'true'
                'is_ems_registered' = 'false'
                'active_start_time' = '1668811449'
                'is_fortiguard_src' = 'false'
                'tags' = 'EMS_ALL_UNMANAGEABLE_CLIENTS'
                ...
        interface_info
        ...
```

To view the local tag information in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.

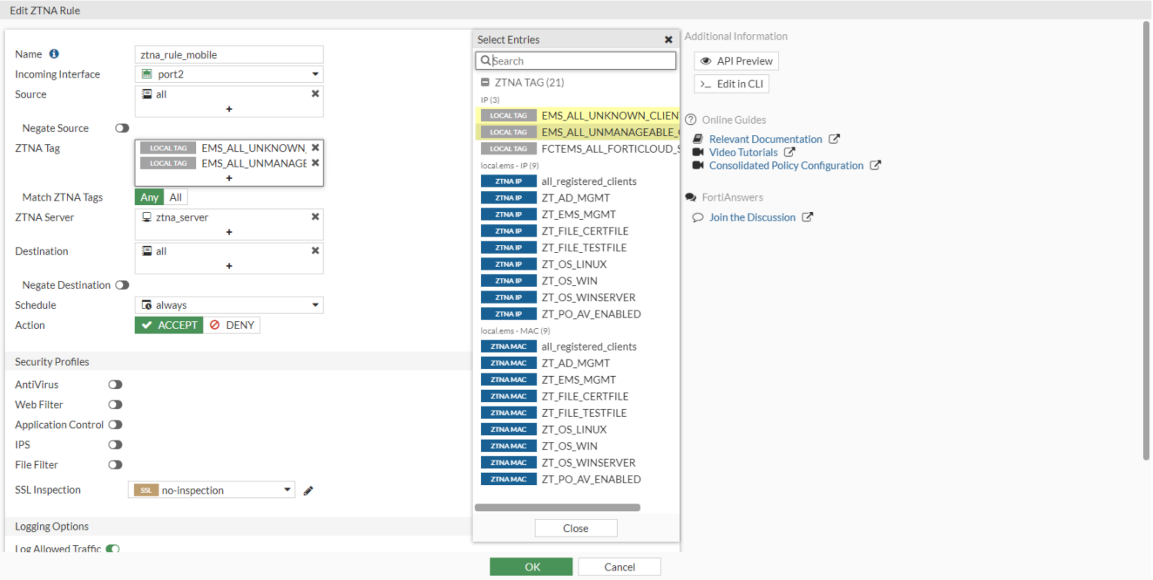


Name	Provided By	Details	Type	Category	Detection Level	Comments	Ref.
ZTNA IP ZT_AD_MGMT	local.ems		ZTNA IP Tag	Zero Trust			0
ZTNA IP ZT_EMS_MGMT	local.ems		ZTNA IP Tag	Zero Trust			0
ZTNA IP ZT_FILE_CERTFILE	local.ems		ZTNA IP Tag	Zero Trust			0
ZTNA IP ZT_FILE_TESTFILE	local.ems		ZTNA IP Tag	Zero Trust			0
ZTNA IP ZT_OS_LINUX	local.ems		ZTNA IP Tag	Zero Trust		testing Tag for linux, this can be customized	0
ZTNA IP ZT_OS_WIN	local.ems		ZTNA IP Tag	Zero Trust			0
ZTNA IP ZT_OS_WINSERVER	local.ems		ZTNA IP Tag	Zero Trust			0
ZTNA IP ZT_PO_AV_ENABLED	local.ems		ZTNA IP Tag	Zero Trust			0
ZTNA IP all_registered_clients	local.ems		ZTNA IP Tag	Zero Trust			0
LOCAL TAG EMS_ALL_UNKNOWN_CLIENTS			ZTNA IP Tag				1
LOCAL TAG EMS_ALL_UNMANAGEABLE_CLIENTS			ZTNA IP Tag				1
LOCAL TAG FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag				0
ZTNA MAC ZT_AD_MGMT	local.ems		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ZT_EMS_MGMT	local.ems		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ZT_FILE_CERTFILE	local.ems		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ZT_FILE_TESTFILE	local.ems		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ZT_OS_LINUX	local.ems		ZTNA MAC Tag	Zero Trust		testing Tag for linux, this can be customized	0
ZTNA MAC ZT_OS_WIN	local.ems		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ZT_OS_WINSERVER	local.ems		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ZT_PO_AV_ENABLED	local.ems		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC all_registered_clients	local.ems		ZTNA MAC Tag	Zero Trust			0

2. Hover over a tag to view the tooltip, which displays matched endpoints and resolved addresses.

To apply a local tag in a ZTNA rule:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Click *Create New*, or select and edit an existing entry.
3. In the *ZTNA Tag* field, click the + to add tags. The local tags appear in the *IP* section.



Edit ZTNA Rule

Name	ztna_rule_mobile
Incoming Interface	port2
Source	all
Negate Source	○
ZTNA Tag	LOCAL TAG EMS_ALL_UNKNOWN_ LOCAL TAG EMS_ALL_UNMANAGE
Match ZTNA Tags	Any All
ZTNA Server	ztna_server
Destination	all
Negate Destination	○
Schedule	always
Action	✓ ACCEPT ⊘ DENY

Security Profiles

AntiVirus	○
Web Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL no-inspection

Logging Options

Log Allowed Traffic ●

Select Entries

Search

ZTNA TAG (21)

IP (3)

- LOCAL TAG EMS_ALL_UNKNOWN_CLIEN
- LOCAL TAG EMS_ALL_UNMANAGEABLE_
- LOCAL TAG FCTEMS_ALL_FORTICLOUD_S

local.ems - IP (9)

- ZTNA IP all_registered_clients
- ZTNA IP ZT_AD_MGMT
- ZTNA IP ZT_EMS_MGMT
- ZTNA IP ZT_FILE_CERTFILE
- ZTNA IP ZT_FILE_TESTFILE
- ZTNA IP ZT_OS_LINUX
- ZTNA IP ZT_OS_WIN
- ZTNA IP ZT_OS_WINSERVER
- ZTNA IP ZT_PO_AV_ENABLED

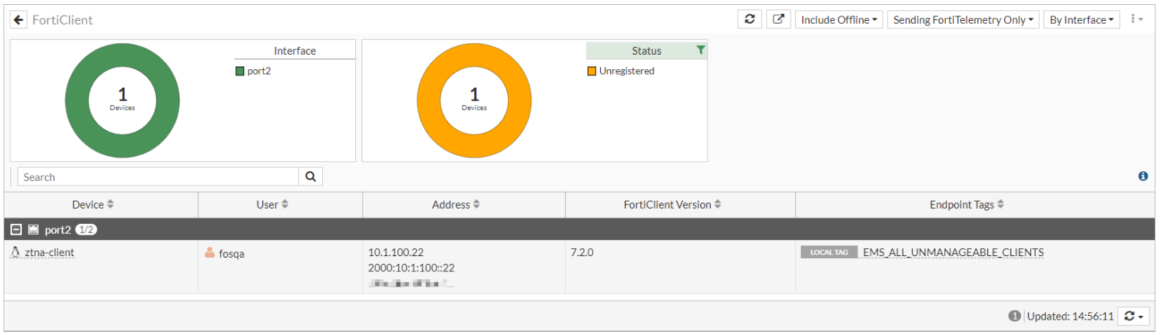
local.ems - MAC (9)

- ZTNA MAC all_registered_clients
- ZTNA MAC ZT_AD_MGMT
- ZTNA MAC ZT_EMS_MGMT
- ZTNA MAC ZT_FILE_CERTFILE
- ZTNA MAC ZT_FILE_TESTFILE
- ZTNA MAC ZT_OS_LINUX
- ZTNA MAC ZT_OS_WIN
- ZTNA MAC ZT_OS_WINSERVER
- ZTNA MAC ZT_PO_AV_ENABLED

4. Configure the other settings as needed.
5. Click *OK*.

Local tag information is also available in the following GUI widgets and pages:

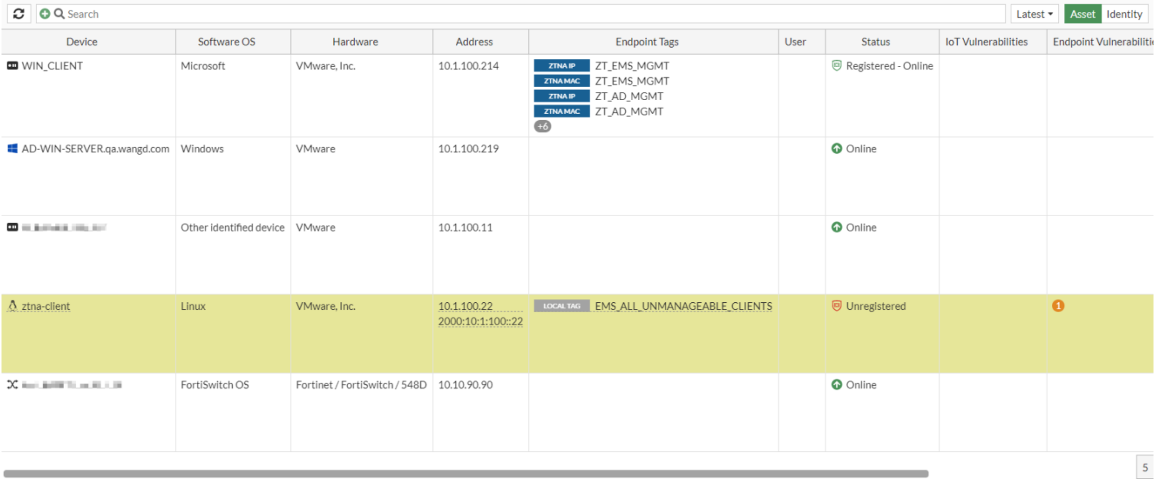
- *Dashboard* > *FortiClient* widget



Device	User	Address	FortiClient Version	Endpoint Tags
port2 1/2				
ztna-client	fosqa	10.1.100.22 2000:10:1:100::22 [redacted]	7.2.0	LOCAL TAG EMS_ALL_UNMANAGEABLE_CLIENTS

Updated: 14:56:11

- *Security Fabric* > *Asset Identity Center* page



Device	Software OS	Hardware	Address	Endpoint Tags	User	Status	IoT Vulnerabilities	Endpoint Vulnerabiliti
WIN_CLIENT	Microsoft	VMware, Inc.	10.1.100.214	ZTNA IP ZT_EMS_MGMT ZTNA MAC ZT_EMS_MGMT ZTNA IP ZT_AD_MGMT ZTNA MAC ZT_AD_MGMT +6		Registered - Online		
AD-WIN-SERVER.qa.wangd.com	Windows	VMware	10.1.100.219			Online		
[redacted]	Other identified device	VMware	10.1.100.11			Online		
ztna-client	Linux	VMware, Inc.	10.1.100.22 2000:10:1:100::22	LOCAL TAG EMS_ALL_UNMANAGEABLE_CLIENTS		Unregistered		1
[redacted]	FortiSwitch OS	Fortinet / FortiSwitch / 548D	10.10.90.90			Online		

Viewing ZTNA traffic logs

ZTNA traffic logs include the following fields related to unmanageable and unknown devices.

- Client connection status with EMS server with possible values of unknown, offline, or online:
  - CLI = `emsconnection`
  - GUI = *EMS Connection*
- Device manageability status with possible values of unknown, manageable, or unmanageable:
  - CLI = `clientdevicemanageable`
  - GUI = *Client Device Manageable*

The device manageability status can have one of the following values:

- Unknown: traffic from a client with an unknown TLS fingerprint and where the user agent information is not available for learning.
- Manageable: traffic from a non-mobile device (platform or operating system), with a known TLS fingerprint, or where the user agent information is available for learning.
- Unmanageable: traffic from a mobile device with a known mobile TLS fingerprint or user agent information is available for learning.

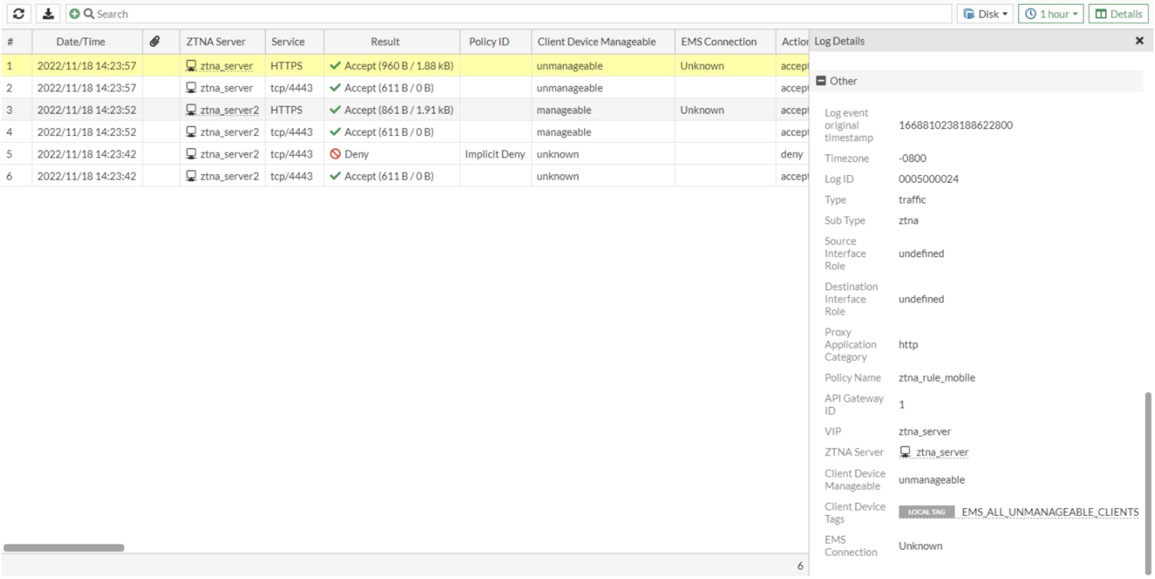
To view the ZTNA traffic logs in the CLI:

```
(vdom1)# execute log filter category 0
(vdom1)# execute log filter field subtype ztna
(vdom1)# execute log display

1: date=2022-11-18 time=14:23:57 eventtime=1668810238188622828 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="vdom1" srcip=10.1.100.22 srcport=41400
srcintf="port2" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.16.200.207 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=12147
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=1 policytype="proxy-
policy" poluuid="03a79dd2-6775-51ed-19a0-444a0314f1a0" policyname="ztna_rule_mobile"
duration=0 gatewayid=1 vip="ztna_server" accessproxy="ztna_server" clientdeviceid="pf-
mobile;os-unknown;app-safari" clientdevicemanageable="unmanageable" clientdevicetags="EMS_
ALL_UNMANAGEABLE_CLIENTS" emsconnection="unknown" wanin=1884 rcvdbyte=1884 wanout=833
lanin=960 sentbyte=960 lanout=3046 fctuid="pf-mobile;os-unknown;app-safari"
appcat="unscanned"

3: date=2022-11-18 time=14:23:52 eventtime=1668810232937847134 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="vdom1" srcip=10.1.100.22 srcport=46392
srcintf="port2" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.16.200.209 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=12144
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=2 policytype="proxy-
policy" poluuid="141b7db8-6785-51ed-32a5-58d696e60e2d" duration=0 gatewayid=1 vip="ztna_
server2" accessproxy="ztna_server2" clientdeviceid="pf-pc;os-unknown;app-curl"
clientdevicemanageable="manageable" clientdevicetags="EMS_ALL_UNKNOWN_CLIENTS"
emsconnection="unknown" wanin=1907 rcvdbyte=1907 wanout=699 lanin=861 sentbyte=861
lanout=3089 fctuid="pf-pc;os-unknown;app-curl" appcat="unscanned"

5: date=2022-11-18 time=14:23:42 eventtime=1668810222897968134 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="vdom1" srcip=10.1.100.22 srcport=46390
srcintf="port2" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.62.68 dstport=4443 dstintf="vdom1" dstintfrole="undefined" sessionid=12134
service="tcp/4443" proxyapptype="http" proto=6 action="deny" policyid=0 policytype="proxy-
```

```
policy" duration=0 vip="ztna_server2" accessproxy="ztna_server2"
clientdevicemanageable="unknown" msg="Denied: failed to match a proxy-policy" wanin=0
rcvdbyte=0 wanout=0 lanin=806 sentbyte=806 lanout=2661 appcat="unscanned" crscore=30
craction=131072 crlevel="high"
```

To view the ZTNA traffic logs in the GUI:

1. Go to *Log & Report > ZTNA Traffic*.
2. Select an entry and click *Details*.
3. Check the *Client Device Manageable* and *EMS Connection* fields.



#	Date/Time		ZTNA Server	Service	Result	Policy ID	Client Device Manageable	EMS Connection	Actio
1	2022/11/18 14:23:57		ztna_server	HTTPS	✓ Accept (960 B / 1.88 kB)		unmanageable	Unknown	accept
2	2022/11/18 14:23:57		ztna_server	tcp/4443	✓ Accept (611 B / 0 B)		unmanageable		accept
3	2022/11/18 14:23:52		ztna_server2	HTTPS	✓ Accept (861 B / 1.91 kB)		manageable	Unknown	accept
4	2022/11/18 14:23:52		ztna_server2	tcp/4443	✓ Accept (611 B / 0 B)		manageable		accept
5	2022/11/18 14:23:42		ztna_server2	tcp/4443	🛇 Deny	Implicit Deny	unknown		deny
6	2022/11/18 14:23:42		ztna_server2	tcp/4443	✓ Accept (611 B / 0 B)		unknown		accept

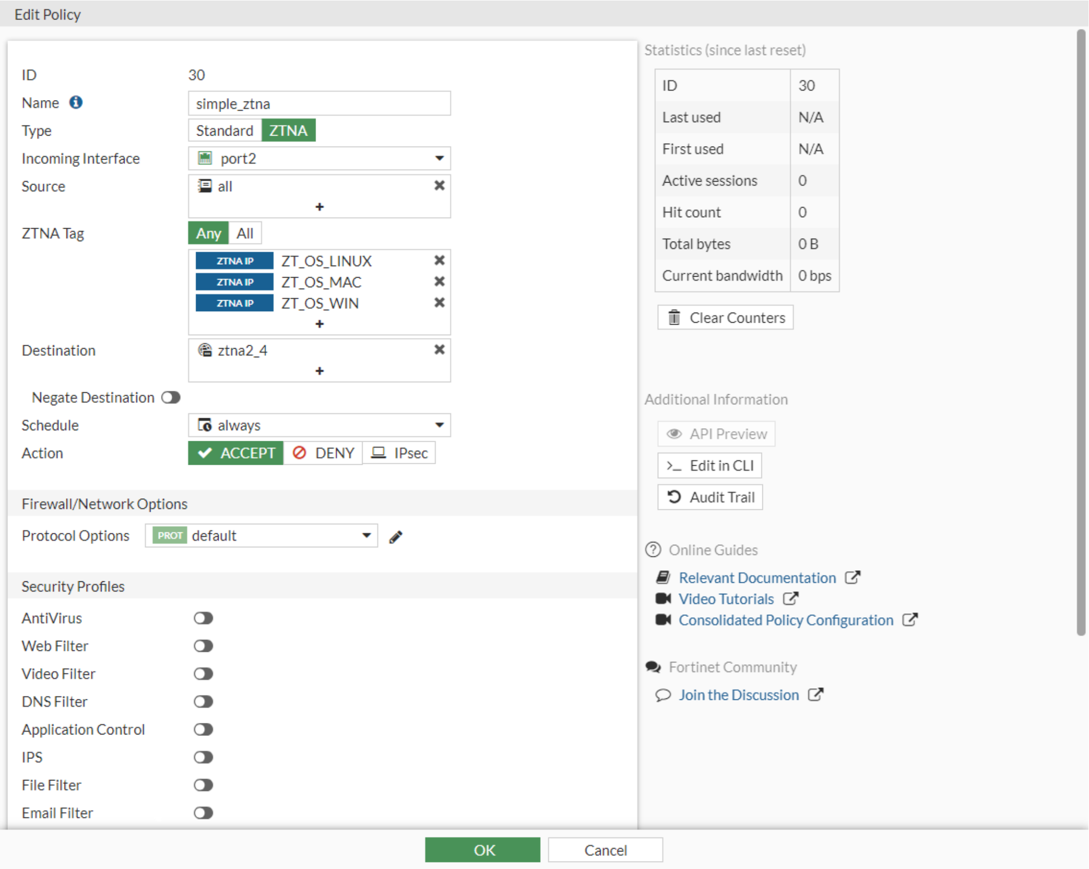
6

Log event original timestamp	1668810238188622800
Timezone	-0800
Log ID	0005000024
Type	traffic
Sub Type	ztna
Source Interface Role	undefined
Destination Interface Role	undefined
Proxy Application Category	http
Policy Name	ztna_rule_mobile
API Gateway ID	1
VIP	ztna_server
ZTNA Server	ztna_server
Client Device Manageable	unmanageable
Client Device Tags	LOCAL TAG EMS_ALL_UNMANAGEABLE_CLIENTS
EMS Connection	Unknown

Add the Any and All options back for ZTNA tags in the GUI - 7.2.6

The *Any* and *All* options in the GUI for the *ZTNA Tag* field are added back to the simple and full ZTNA policy configuration pages. The default setting is *Any*.

Simple ZTNA policy (*Policy & Objects > Firewall Policy* page):


Edit Policy

ID 30
Name simple_ztna
Type Standard [✓ ZTNA]
Incoming Interface port2
Source all
ZTNA Tag [✓ Any] All
ZTNA IP ZT_OS_LINUX
ZTNA IP ZT_OS_MAC
ZTNA IP ZT_OS_WIN
Destination ztna2_4
Negate Destination ○
Schedule always
Action [✓ ACCEPT] DENY IPsec

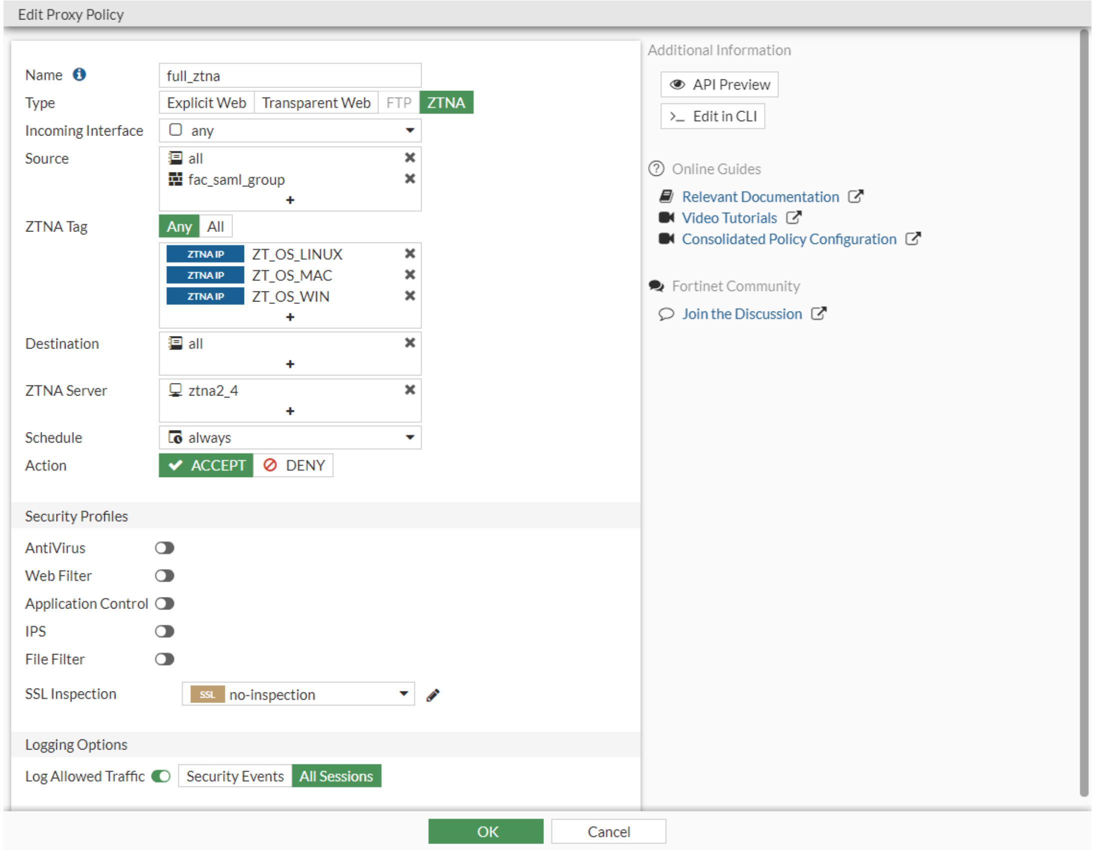
Firewall/Network Options
Protocol Options PROT default

Security Profiles
AntiVirus ○
Web Filter ○
Video Filter ○
DNS Filter ○
Application Control ○
IPS ○
File Filter ○
Email Filter ○

Statistics (since last reset)

ID	30
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 bps

Simple ZTNA policy (*Policy & Objects* > *Proxy Policy* page):



Edit Proxy Policy

Name: full_ztna

Type: Explicit Web | Transparent Web | FTP | [✓ ZTNA]

Incoming Interface: any

Source: all, fac_saml_group

ZTNA Tag: [✓ Any] | All

ZTNA IP ZT_OS_LINUX

ZTNA IP ZT_OS_MAC

ZTNA IP ZT_OS_WIN

Destination: all

ZTNA Server: ztna2_4

Schedule: always

Action: [✓ ACCEPT] | DENY

Security Profiles

AntiVirus ○

Web Filter ○

Application Control ○

IPS ○

File Filter ○

SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic ● Security Events | [✓ All Sessions]

In the CLI, use the `ztna-tags-match-logic {or | and}` setting under `config firewall policy` and `config firewall proxy-policy` to configure the ZTNA tag matching logic.

NGFW

This section includes information about NGFW policy mode related new features:

- Allow web filter category groups to be selected in NGFW policies on page 366
- Add option to set application default port as a service port on page 367
- Introduce learn mode in security policies in NGFW mode on page 370

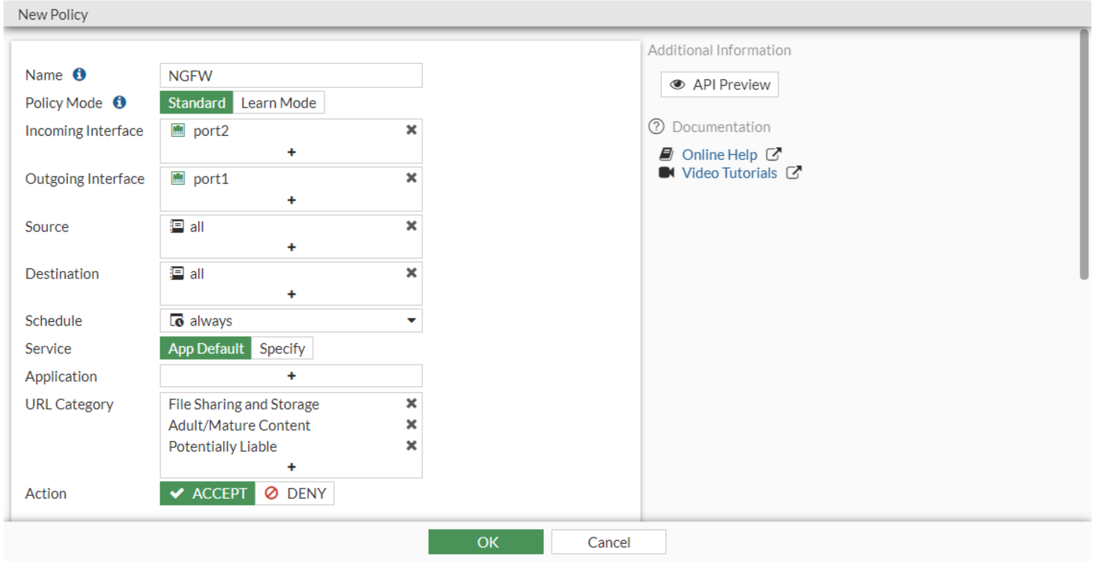
Allow web filter category groups to be selected in NGFW policies

When configuring security policies in NGFW policy-based mode, it is possible to select and apply web filter URL categories and groups.

In this example, the potentially liable group (g01), adult/mature content group (g02), and file sharing and storage category (24) are applied in a security policy.

To configure web filter URL categories and groups in a security policy in the GUI:

1. Go to *Policy & Objects > Security Policy*, and click *Create New* or edit an existing policy.
2. For *URL Category*, click the +.
3. Click the *FortiGuard Web Filter Category Group* section, select *Potentially Liable* and *Adult/Mature Content*.
4. In the *FortiGuard Web Filter Category > Bandwidth Consuming* section, select *File Sharing and Storage*.



New Policy

Name: NGFW

Policy Mode: Standard | Learn Mode

Incoming Interface: port2

Outgoing Interface: port1

Source: all

Destination: all

Schedule: always

Service: App Default | Specify

Application:

URL Category: File Sharing and Storage
Adult/Mature Content
Potentially Liable

Action: ✓ ACCEPT | DENY

5. Configure the other settings as needed.
6. Click *OK*.

To configure web filter URL categories and groups in a security policy in the CLI:

```
config firewall security-policy
    edit 1
        set name "NGFW"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set url-category g01 g02 24
    next
end
```

Add option to set application default port as a service port

The `default-app-port-as-service` option can be used in NGFW mode to set the application default port as a service port. This allows applications to match the policy and be blocked immediately the first time that traffic hits the firewall. When this option is enabled, the NGFW policy aggregates the ports used by the applications in the policy and performs a pre-match on the traffic. This has changed from previous behavior where the traffic must be identified by IPS first, and then policy matching occurs based on the matched port.

```
config system settings
    set default-app-port-as-service {enable | disable}
end
```

This option can be configured on a per-VDOM level.

This setting is enabled by default on new installations. When upgrading, the setting is disabled to retain the previous behavior.

To configure the application default port as service port:

1. Configure the VDOM settings:

   ```
   config system settings
       set vdom-type traffic
       set opmode nat
       set ngfw-mode policy-based
       set block-land-attack disable
       set default-app-port-as-service enable
       set application-bandwidth-tracking disable
   end
   ```

2. Configure the NGFW policy:

   ```
   config firewall security-policy
       edit 1
           set name "test"
           set srcintf "port2"
           set dstintf "port1"
           set srcaddr "all"
           set dstaddr "all"
           set internet-service-src disable
           set enforce-default-app-port enable
           set action accept
       next
   end
   ```

Sample logs

The following logging behavior occurs in NGFW mode with `default-app-port-as-service`:

- When `default-app-port-as-service` and `enforce-default-app-port` are enabled, traffic that does not match the default port is blocked immediately. Only a traffic log is generated.

  Log with SSH and FTP traffic:

  ```
  1: date=2022-02-24 time=11:16:36 eventtime=1645730197145603994 tz="-0800"
  logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vd1"
  srcip=10.1.100.12 srcport=40402 srcintf="port2" srcintfrole="undefined"
  dstip=172.16.200.55 dstport=21 dstintf="port1" dstintfrole="undefined"
  srccountry="Reserved" dstcountry="Reserved" sessionid=6811 proto=6 action="deny"
  policyid=0 policytype="security-policy" poluuid="7ed35582-95a2-51ec-0d21-4093cb91e67b"
  ```

```
policyname="Default" centralnatid=1 service="FTP" trandisp="snat" transip=172.16.200.4
transport=40402 duration=10 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned"
```

Log with SSH and FTP traffic with port 2121:

```
1: date=2022-02-24 time=11:19:20 eventtime=1645730360685614031 tz="-0800"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vd1"
srcip=10.1.100.12 srcport=41362 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.55 dstport=2121 dstintf="port1" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=7213 proto=6 action="deny"
policyid=0 policytype="security-policy" poluuid="7ed35582-95a2-51ec-0d21-4093cb91e67b"
policyname="Default" centralnatid=1 service="tcp/2121" trandisp="snat"
transip=172.16.200.4 transport=41362 duration=9 sentbyte=60 rcvdbyte=0 sentpkt=1
rcvdpkt=0 appcat="unscanned"
```

- When `default-app-port-as-service` is disabled and `enforce-default-app-port` is enabled, traffic that does not match the default port is not blocked immediately. Application and traffic logs are generated.

Traffic log with SSH and FTP traffic:

```
1: date=2022-02-24 time=11:21:51 eventtime=1645730511325606916 tz="-0800"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vd1"
srcip=10.1.100.12 srcport=40408 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.55 dstport=21 dstintf="port1" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=7522 proto=6 action="deny"
policyid=0 policytype="security-policy" poluuid="7ed35582-95a2-51ec-0d21-4093cb91e67b"
policyname="Default" centralnatid=1 service="FTP" trandisp="snat" transip=172.16.200.4
transport=40408 duration=14 sentbyte=164 rcvdbyte=171 sentpkt=3 rcvdpkt=2 appid=15896
app="FTP" appcat="Network.Service" apprisk="elevated" utmaction="block" countapp=1
utmref=65501-0
```

Application log with SSH and FTP traffic:

```
2: date=2022-02-24 time=11:21:39 eventtime=1645730499338228209 tz="-0800"
logid="1059028705" type="utm" subtype="app-ctrl" eventtype="signature" level="warning"
vd="vd1" appid=15896 srcip=10.1.100.12 srccountry="Reserved" dstip=172.16.200.55
dstcountry="Reserved" srcport=40408 dstport=21 srcintf="port2" srcintfrole="undefined"
dstintf="port1" dstintfrole="undefined" proto=6 service="FTP" direction="outgoing"
policyid=0 sessionid=7522 action="block" appcat="Network.Service" app="FTP"
incidentserialno=188744239 msg="Network.Service: FTP" apprisk="elevated"
```

Traffic log with SSH and FTP traffic with port 2121:

```
1: date=2022-02-24 time=11:24:25 eventtime=1645730665235613912 tz="-0800"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vd1"
srcip=10.1.100.12 srcport=41366 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.55 dstport=2121 dstintf="port1" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=7876 proto=6 action="deny"
policyid=0 policytype="security-policy" poluuid="7ed35582-95a2-51ec-0d21-4093cb91e67b"
policyname="Default" centralnatid=1 service="tcp/2121" trandisp="snat"
transip=172.16.200.4 transport=41366 duration=11 sentbyte=112 rcvdbyte=171 sentpkt=2
rcvdpkt=2 appid=15896 app="FTP" appcat="Network.Service" apprisk="elevated"
utmaction="block" countapp=1 utmref=65500-0
```

Application log with SSH and FTP traffic with port 2121:

```
2: date=2022-02-24 time=11:24:16 eventtime=1645730656426052412 tz="-0800"
logid="1060028736" type="utm" subtype="app-ctrl" eventtype="port-violation"
level="warning" vd="vd1" appid=15896 srcip=10.1.100.12 srccountry="Reserved"
dstip=172.16.200.55 dstcountry="Reserved" srcport=41366 dstport=2121 srcintf="port2"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 service="FTP"
direction="outgoing" policyid=0 sessionid=7876 action="block" appcat="Network.Service"
app="FTP" incidentserialno=188744241 msg="Network.Service: FTP, non-default port used:
2121" apprisk="elevated"
```

Introduce learn mode in security policies in NGFW mode

In NGFW mode, administrators can configure a security policy in learn mode to monitor traffic that passes through the source and destination interfaces. All traffic is allowed between the interfaces and logged. The learn mode uses a special prefix in the `policymode` and `profile` fields in traffic and UTM logs for use by FortiAnalyzer and the Policy Analyzer Management Extension Application (MEA) that is available with FortiManager.

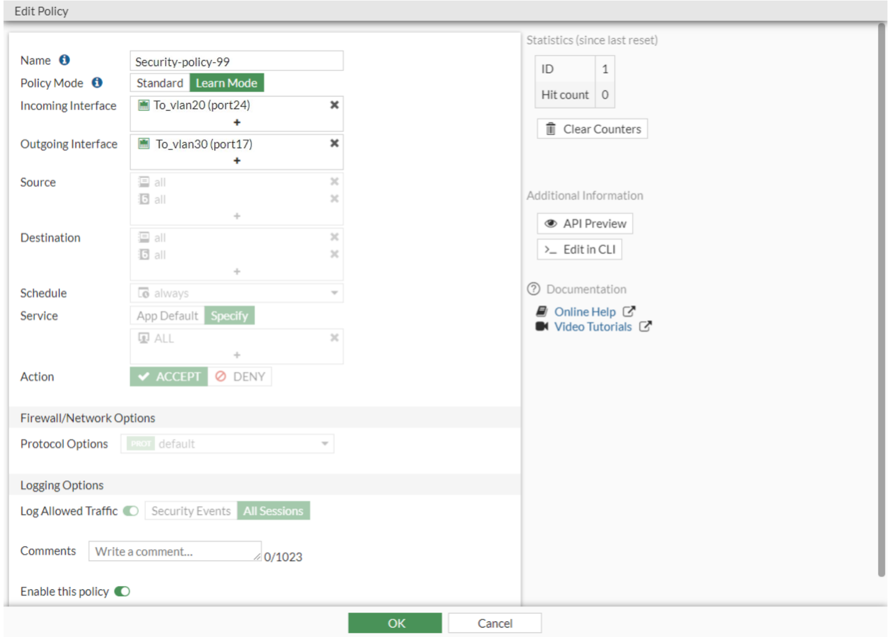
When enabled on FortiManager, Policy Analyzer MEA works with security policies in learning mode to analyze logs sent from a managed FortiGate to FortiAnalyzer. Based on the analyzed traffic, FortiManager administrators can choose to automatically create a policy in FortiManager for the managed FortiGate. For more information about Policy Analyzer MEA, see the Policy Analyzer Administration Guide.

The following limitations apply when learn mode is enabled in a security policy:

- Only interfaces with `device-identification enable` can be used as source interfaces in a security policy with learning mode enabled.
- Incoming and outgoing interfaces do not support `any`.
- Internet service is not supported.
- NAT46 and NAT64 are not supported.
- Users and groups are not supported.
- Some negate options are not supported.

To enable learn mode in the GUI:

1. Enable policy-based NGFW mode:
   a. Go to *System > Settings*.
   b. Set the *NGFW Mode* to *Policy-based* and click *Apply*.
2. Go to *Policy & Objects > Security Policy*, and open a security policy for editing.
3. Set the *Policy Mode* to *Learn Mode*.



Edit Policy

Name: Security-policy-99

Policy Mode: Standard | Learn Mode

Incoming Interface: To_vlan20 (port24)

Outgoing Interface: To_vlan30 (port17)

Source: all, all

Destination: all, all

Schedule: always

Service: App Default | Specify — ALL

Action: ✓ ACCEPT | DENY

Firewall/Network Options

Protocol Options: PROT default

Logging Options

Log Allowed Traffic: Security Events | All Sessions

Comments: Write a comment... 0/1023

Enable this policy

Statistics (since last reset)

ID	1
Hit count	0

4. Select an *Incoming Interface*.
5. Select an *Outgoing Interface*.
6. (Optional) Type a comment in the *Comments* box.
7. Toggle on *Enable this policy*.
8. Click *OK* to save the security policy.

To enable learn mode in the CLI:

1. Enable policy-based NGFW mode:

```
config system settings
    set ngfw-mode policy-based
end
```

2. Enable learn mode in a security policy:

```
config firewall security-policy
    edit <id>
        set learning-mode enable
    next
end
```

To view learn mode fields in logs in the CLI:

1. Filter and view fields in traffic logs:

```
# execute log filter category 0

# execute log display

1 logs found.
```

```
1 logs returned.

1: date=2022-03-21 time=10:21:11 eventtime=1647883271150012188 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.41 srcport=43296 srcintf="port24" srcintfrole="undefined"
dstip=172.16.200.55 dstport=80 dstintf="port17" dstintfrole="wan"
srccountry="Reserved" dstcountry="Reserved" sessionid=33934 proto=6
policymode="learn" action="accept" policyid=99 policytype="security-policy"
poluuid="6e3f7f54-a932-51ec-73ba-8282cfd0b73c" policyname="Security-policy-99"
centralnatid=3 service="HTTP" trandisp="snat" transip=172.16.200.9 transport=43296
duration=1 sentbyte=412 rcvdbyte=529 sentpkt=6 rcvdpkt=4 appid=15893
app="HTTP.BROWSER" appcat="Web.Client" apprisk="medium" utmaction="allow"
countweb=1 countav=1 countips=3 countapp=1 crscore=50 craction=2
srchwvendor="VMware" devtype="Computer" osname="Debian"
mastersrcmac="00:0c:29:b5:92:8d" srcmac="00:0c:29:b5:92:8d" srcserver=0
utmref=65534-0
```

2. Filter and view fields in UTM logs:

```
# execute log filter category 2

# execute log display

1 logs found.

1 logs returned.

1: date=2022-03-21 time=10:21:09 eventtime=1647883270101403283 tz="-0700"
logid="0211008193" type="utm" subtype="virus" eventtype="infected" level="notice"
vd="root" policyid=99 poluuid="6e3f7f54-a932-51ec-73ba-8282cfd0b73c"
policytype="security-policy" policymode="learn" msg="File is infected."
action="monitored" service="HTTP" sessionid=33934 srcip=10.1.100.41
dstip=172.16.200.55 srcport=43296 dstport=80 srccountry="Reserved"
dstcountry="Reserved" srcintf="port24" srcintfrole="undefined" dstintf="port17"
dstintfrole="wan" proto=6 direction="incoming" filename="eicar.com"
quarskip="Quarantine-disabled" virus="EICAR_TEST_FILE" viruscat="Virus" dtype="av-
engine" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172
url="http://172.16.200.55/virus/eicar.com" profile="learn-av" agent="curl/7.35.0"
httpmethod="GET"
analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical" rawdata="Response-
Content-Type=application/x-msdos-program"
```

3. Filter and view fields in UTM-IPS logs:

```
# execute log filter category 4

# execute log display

3 logs found.
```

```
3 logs returned.

1: date=2022-03-21 time=10:21:09 eventtime=1647883270101485354 tz="-0700"
logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert"
vd="root" severity="info" srcip=10.1.100.41 srccountry="Reserved"
dstip=172.16.200.55 dstcountry="Reserved" srcintf="port24" srcintfrole="undefined"
dstintf="port17" dstintfrole="wan" sessionid=33934 action="detected" proto=6
service="HTTP" policyid=99 poluuid="6e3f7f54-a932-51ec-73ba-8282cfd0b73c"
policytype="security-policy" policymode="learn" attack="Eicar.Virus.Test.File"
srcport=43296 dstport=80 agent="curl/7.35.0" httpmethod="GET" direction="incoming"
attackid=29844 profile="learn-ips" ref="http://www.fortinet.com/ids/VID29844"
incidentserialno=158335134 attackcontextid="2/2"
attackcontext="YW0NCg0KWDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFO
VElWSVJVUy1URVNULUZJTEUhJEgrSCo8L1BBQ0tFVD4="

2: date=2022-03-21 time=10:21:09 eventtime=1647883270101484791 tz="-0700"
logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert"
vd="root" severity="info" srcip=10.1.100.41 srccountry="Reserved"
dstip=172.16.200.55 dstcountry="Reserved" srcintf="port24" srcintfrole="undefined"
dstintf="port17" dstintfrole="wan" sessionid=33934 action="detected" proto=6
service="HTTP" policyid=99 poluuid="6e3f7f54-a932-51ec-73ba-8282cfd0b73c"
policytype="security-policy" policymode="learn" attack="Eicar.Virus.Test.File"
srcport=43296 dstport=80 agent="curl/7.35.0" httpmethod="GET" direction="incoming"
attackid=29844 profile="learn-ips" ref="http://www.fortinet.com/ids/VID29844"
incidentserialno=158335134 attackcontextid="1/2"
attackcontext="PFBBVFRFUk5TPiBYNU8hUCVAQVBbNFxQWlg1NChQXik3Q0MpN30kRUlDQVItU1RBTkRB
UkQtQU5USVZJUlVTLVRFU1QtRklMRSEkSCtIKjtYNU8hUCVAQVBbNFxQWlg1NChQXik3Q0MpN30kRUlDQVI
tU1RBTkRBUkQtQU5USVZJUlVTLVRFU1QtRklMRSEkSCtIKjwvUEFUVEVSTlM+CjxVUkk+IDwvVVJJPgo8SE
VBREVSPiBIVFRQLzEuMSAyMDAgT0sNCkRhdGU6IE1vbiwgMjEgTWFyIDIwMjIgMTc6MjE6MTAgR01UDQpTZ
XJ2ZXI6IEFwYWNoZS8yLjQuMTggKFVidW50dSkNCkxhc3QtTW9kaWZpZWQ6IFRodSwgMDEgRGVjIDIwMTYg
MDE6MjY6MzUgR01UDQpFVGFnOiAiNDQtNTQyOGViNjU4MDk3YSINCkFjY2VwdC1SYW5nZXM6IGJ5dGVzDQp
Db250ZW50LUxlbmd0aDogNjgNCkNvbnRlbnQtVHlwZTogYXBwbGljYXRpb24veC1tc2Rvcy1wcm9ncmFtDQ
oNCjwvSEVBREVSPgo8Qk9EWT4gWDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJEL
UFOVElWSVJVUy1URVNULUZJTEUhJEgrSCo8L0JPRFk+CjxQQUNLRVQ+IEhUVFAvMS4xIDIwMCBPSw0KRGF0
ZTogTW9uLCAyMSBNYXIgMjAyMiAxNzoyMToxMCBHTVQNClNlcnZlcjogQXBhY2hlLzIuNC4xOCAoVWJ1bnR
1KQ0KTGFzdC1Nb2RpZmllZDogVGh1LCAwMSBEZWMgMjAxNiAwMToyNjozNSBHTVQNCkVUYWc6ICI0NC01ND
I4ZWI2NTgwOTdhIg0KQWNjZXB0LVJhbmdlczogYnl0ZXMNCkNvbnRlbnQtTGVuZ3RoOiA2OA0KQ29udGVud
C1UeXBlOiBhcHBsaWNhdGlvbi94LW1zZG9zLXByb2dy"

3: date=2022-03-21 time=10:21:09 eventtime=1647883270101483279 tz="-0700"
logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert"
vd="root" severity="info" srcip=10.1.100.41 srccountry="Reserved"
dstip=172.16.200.55 dstcountry="Reserved" srcintf="port24" srcintfrole="undefined"
dstintf="port17" dstintfrole="wan" sessionid=33934 action="detected" proto=6
service="HTTP" policyid=99 poluuid="6e3f7f54-a932-51ec-73ba-8282cfd0b73c"
policytype="security-policy" policymode="learn" attack="Eicar.Virus.Test.File"
srcport=43296 dstport=80 hostname="172.16.200.55" url="/virus/eicar.com"
agent="curl/7.35.0" httpmethod="GET" direction="incoming" attackid=29844
```

```
profile="learn-ips" ref="http://www.fortinet.com/ids/VID29844"
incidentserialno=158335134 msg="file_transfer: Eicar.Virus.Test.File"
attackcontextid="0/2" rawdataid="1/1" rawdata="Response-Content-Type=application/x-
msdos-program"
```

4. Filter and view fields in UTM-webfilter logs:

```
# execute log filter category 3

# execute log display

2 logs found.

2 logs returned.

2: date=2022-03-21 time=10:21:09 eventtime=1647883270100329681 tz="-0700"
logid="0319013317" type="utm" subtype="webfilter" eventtype="urlmonitor"
level="notice" vd="root" policyid=99 poluuid="6e3f7f54-a932-51ec-73ba-8282cfd0b73c"
policytype="security-policy" policymode="learn" sessionid=33934 srcip=10.1.100.41
srcport=43296 srccountry="Reserved" srcintf="port24" srcintfrole="undefined"
dstip=172.16.200.55 dstport=80 dstcountry="Reserved" dstintf="port17"
dstintfrole="wan" proto=6 httpmethod="GET" service="HTTP" hostname="172.16.200.55"
agent="curl/7.35.0" profile="learn-webf" action="passthrough" reqtype="direct"
url="http://172.16.200.55/virus/eicar.com" sentbyte=92 rcvdbyte=0
direction="outgoing" msg="URL has been visited" ratemethod="domain" cat=255
catdesc="Unknown"
```

Policies

This section includes information about policy related new features:

- Adding traffic shapers to multicast policies on page 374
- Add Policy change summary and Policy expiration to Workflow Management on page 376
- Virtual patching on the local-in management interface 7.2.4 on page 379

Adding traffic shapers to multicast policies

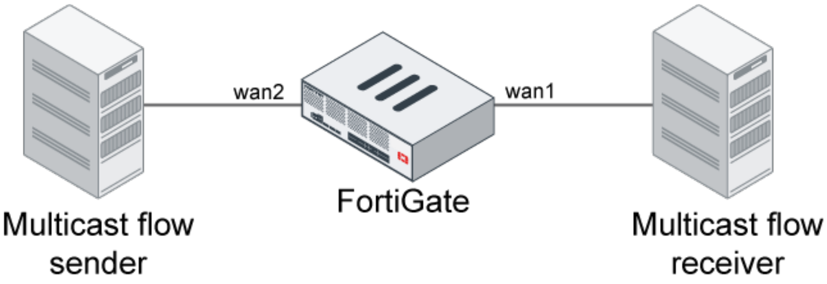
When multicast routing is enabled, a traffic shaper can be added to a multicast policy.

Only a shared traffic shaper with the `per-policy` option disabled can be used. This is the default state of the `per-policy` option. The `auto-asic-offload` option must also be disabled on the multicast policy.

This feature is currently not supported on IPv6 multicast policies or on transparent mode VDOMs.

Example

In this example, a traffic shaper is applied to the multicast policy. A multicast flow sender sends the multicast data stream. The shaper attached to the multicast session is checked, and the shaping of the data stream is confirmed in the multicast session.



To apply traffic shaping to a multicast policy:

1. Enable multicast routing on the VDOM:

```
config router multicast
    set multicast-routing enable
    config pim-sm-global
        config rp-address
            edit 1
                set ip-address 10.1.100.10
            next
        end
    end
    config interface
        edit "wan2"
            set pim-mode sparse-mode
        next
        edit "wan1"
            set pim-mode sparse-mode
        next
    end
end
```

2. Create a traffic shaper:

```
config firewall shaper traffic-shaper
    edit "shaper128kbps-high"
        set guaranteed-bandwidth 128
        set maximum-bandwidth 128
        set per-policy disable
        set diffserv enable
        set diffservcode 010101
    next
end
```

3. Apply the traffic shaper to the multicast policy and disable NPU offloading:

```
config firewall multicast-policy
    edit 1
        set name "test_multicast-policy"
        set logtraffic enable
        set srcintf "wan2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set snat enable
        set auto-asic-offload disable
        set traffic-shaper "shaper128kbps-high"
    next
end
```

4. Check the shaper and DSCP in the multicast session:

```
# diagnose sys mcast-session list
    session info: id=26 vf=0 proto=17 10.1.100.41.35537->230.0.0.1.7878
    used=2 path=1 duration=118 expire=179 indev=18 pkts=119 bytes=64260
    state=00000000:
    session-npu-info: ipid/vlifid=0/0 vlanid/vtag_in=0/0 in_npuid=0 tae_index=0 qid=0
fwd_map=0x00000000
    path: log snat npu-deny nsaddr=172.16.200.10 policy=1, outdev=17, tos=0x15
            origin-shaper=shaper128kbps-high prio=2 tos=0x15 guarantee 16000Bps max
16000Bps traffic 620Bps drops 0pkt/0B
    Total 1 sessions
```

Add Policy change summary and Policy expiration to Workflow Management

Two options, *Policy change summary* and *Policy expiration*, are added to *Workflow Management*. *Policy change summary* enforces an audit trail for changes to firewall policies. *Policy expiration* allows administrators to set a date for the firewall policy to be disabled.

There are three states for the *Policy change summary*:

- *Disable*: users will not be prompted to add a summary when editing a policy.
- *Required*: the *Policy change summary* will be enabled and will require users to add a summary when editing or creating a firewall policy.
- *Optional*: the *Policy change summary* will be enabled but users can leave the summary empty, if preferred, when editing or creating a firewall policy.

There are three states for *Policy expiration*:

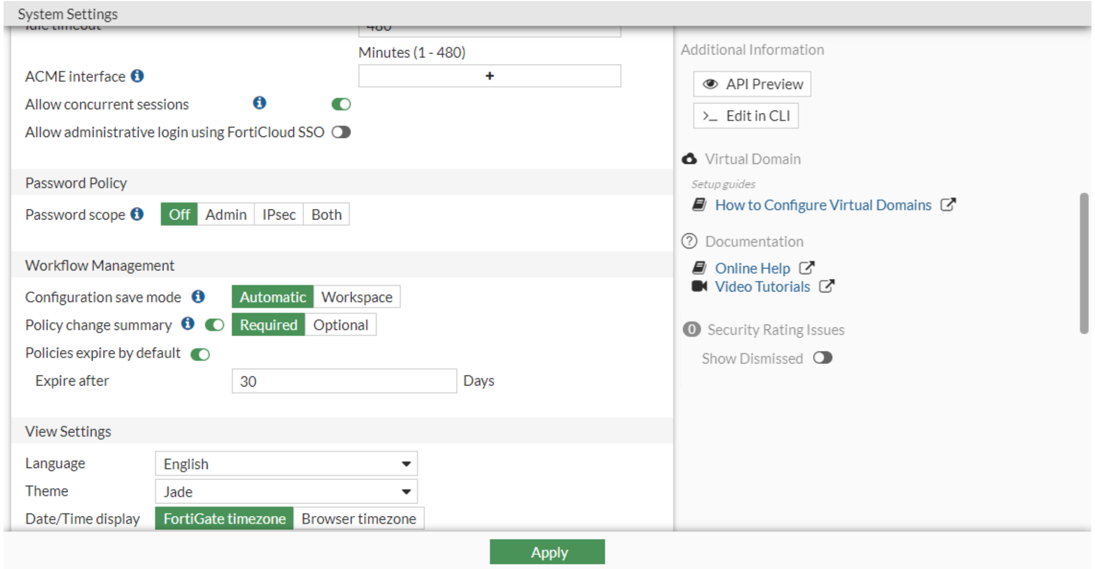
- *Disable*: the firewall policy will not expire. This is the default setting for *Policy expiration*.
- *Default*: the firewall policy will expire after the default number of days.
- *Specify*: the firewall policy will expire at a set date and time.

The default value for *Policy expiration* is 30 days. This number can be changed in the CLI or in *System* > *Settings* in the GUI to any value between zero and 365 days. If the default value is set to zero, the *Default* state will disable the *Policy expiration*.

To configure the firewall policy change summary and default expiration in the GUI:

1. Go to *System* > *Feature Visibility*.
2. Enable *Workflow Management*.

3. Click *Apply*.
4. Go to *System* > *Settings*.
5. In the *Workflow Management* section, set *Policy change summary* to *Required*. *Policies expire by default* is enabled by default with an *Expire after* value of *30*.



System Settings

Idle timeout 480 Minutes (1 - 480)

ACME interface +

Allow concurrent sessions ●

Allow administrative login using FortiCloud SSO ○

Password Policy

Password scope [✓ Off] Admin IPsec Both

Workflow Management

Configuration save mode [✓ Automatic] Workspace

Policy change summary ● [✓ Required] Optional

Policies expire by default ●

Expire after 30 Days

View Settings

Language English

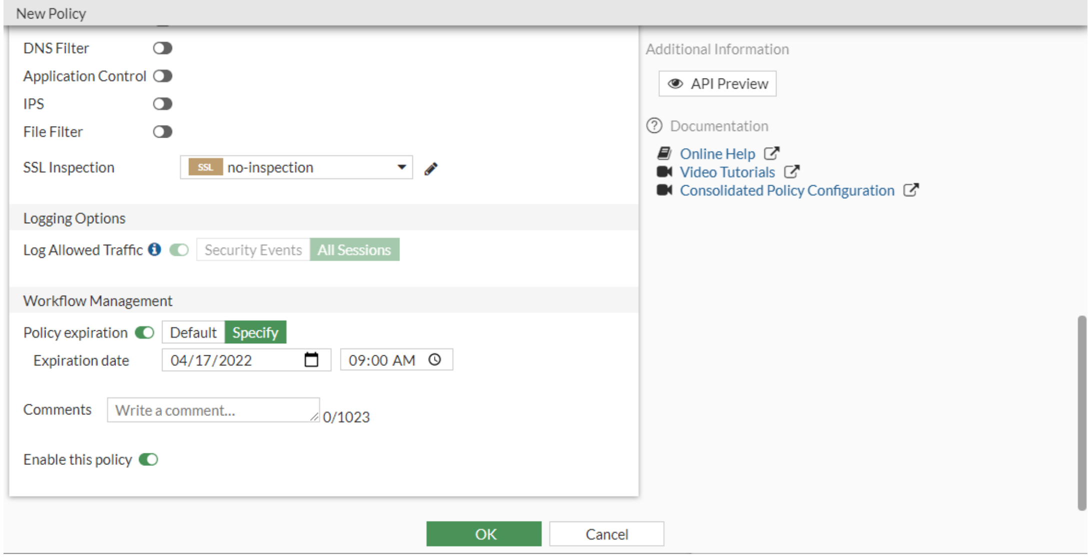
Theme Jade

Date/Time display [✓ FortiGate timezone] Browser timezone

6. Click *Apply*.

To configure firewall policy expiration in the GUI:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Name the policy and configure the necessary parameters.
3. Set *Policy expiration* to *Specify*. The *Expiration date* fields appears with the current date and time.



New Policy

DNS Filter ○

Application Control ○

IPS ○

File Filter ○

SSL Inspection SSL no-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Workflow Management

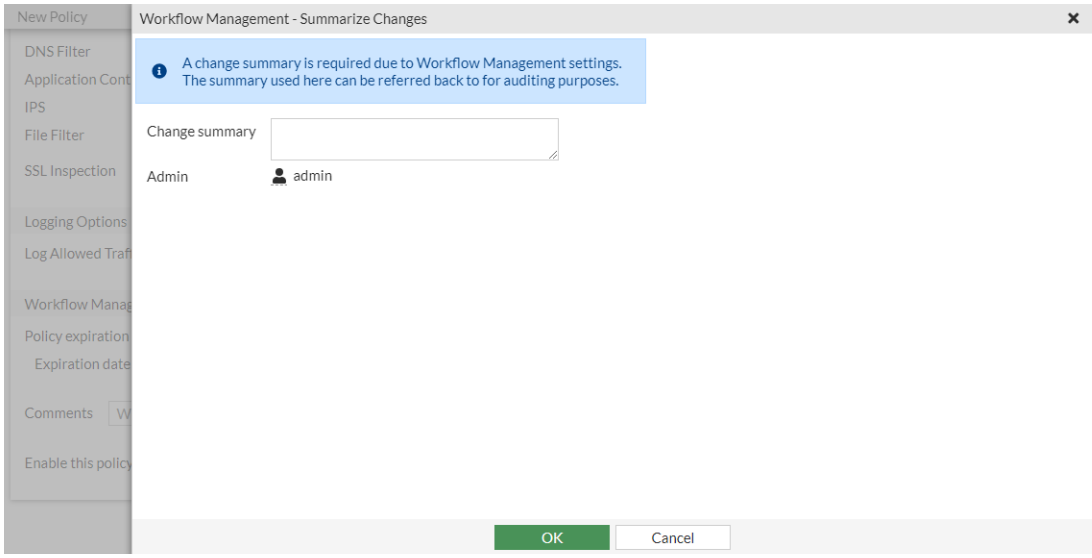
Policy expiration ● Default [✓ Specify]

Expiration date 04/17/2022 09:00 AM

Comments Write a comment... 0/1023

Enable this policy ●

4. Select the date and time for the policy to expire from the *Expiration date* fields.
5. Click *OK*. The *Workflow Management - Summarize Changes* pane opens.



Workflow Management - Summarize Changes

A change summary is required due to Workflow Management settings. The summary used here can be referred back to for auditing purposes.

Change summary

Admin: admin

6. In the *Change summary* field, enter details about the changes made to the policy. These details can be referred to later for auditing purposes.
7. Click *OK*.

To configure the firewall policy change summary in the CLI:

```
config system settings
    set gui-enforce-change-summary {disable | require | optional}
end
```

To configure the policy expiration default value in the CLI:

```
config system settings
    set default-policy-expiry-days <integer>
end
```

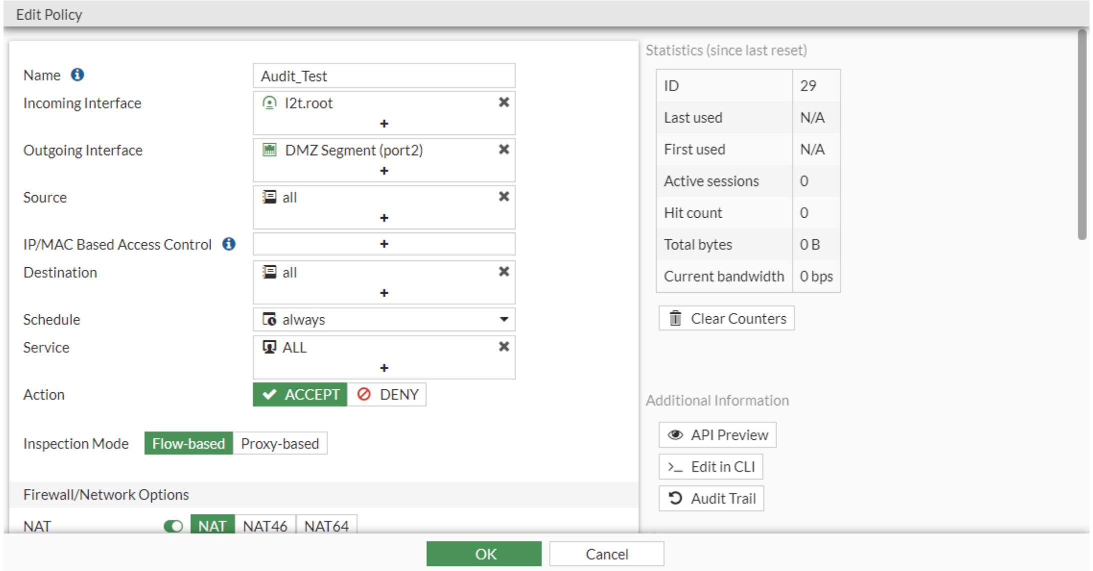
To configure firewall policy expiration in the CLI:

```
config firewall policy
    edit <id>
        set policy-expiry {enable | disable}
        set policy-expiry-date <YYYY-MM-DD HH:MM:SS>
    next
end
```

Policy change summaries are used to track changes made to a firewall policy. The *Audit trail* allow users to review the policy change summaries, including the date and time of the change and which user made the change.

To review the audit trail in the GUI:

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Select the policy you want to review and click *Edit*.



Edit Policy

Name	Audit_Test
Incoming Interface	l2t.root
Outgoing Interface	DMZ Segment (port2)
Source	all
IP/MAC Based Access Control	+
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY
Inspection Mode	Flow-based Proxy-based

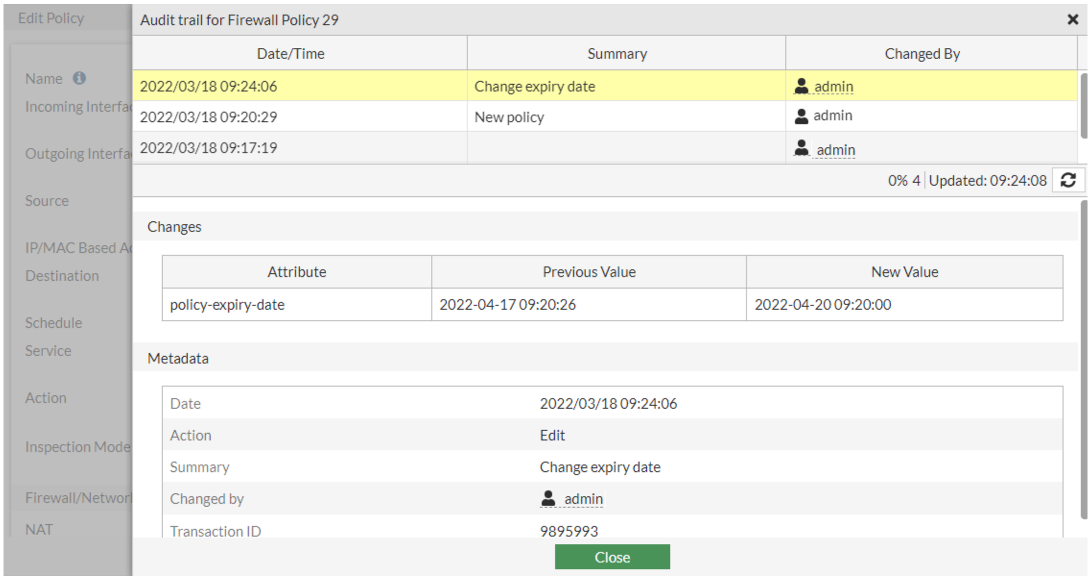
Firewall/Network Options

NAT ● NAT NAT46 NAT64

Statistics (since last reset)

ID	29
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 bps

3. In the right-side banner, click *Audit Trail*. The *Audit trail for Firewall Policy* pane opens and displays the policy change summaries for the selected policy.



Audit trail for Firewall Policy 29

Date/Time	Summary	Changed By
2022/03/18 09:24:06	Change expiry date	admin
2022/03/18 09:20:29	New policy	admin
2022/03/18 09:17:19		admin

0% 4 Updated: 09:24:08

Changes

Attribute	Previous Value	New Value
policy-expiry-date	2022-04-17 09:20:26	2022-04-20 09:20:00

Metadata

Date	2022/03/18 09:24:06
Action	Edit
Summary	Change expiry date
Changed by	admin
Transaction ID	9895993

4. Select an entry to review the details of the change made.
5. When you are done reviewing the *Audit Trail*, click *Close*.
6. Click *Cancel* to exit the *Edit Policy* page.

Virtual patching on the local-in management interface - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Virtual patching on the local-in management interface

Virtual patching is a method of mitigating vulnerability exploits by using the FortiGate’s IPS engine to block known vulnerabilities. Virtual patching can be applied to traffic destined to the FortiGate by applying IPS signatures to the local-in interface using local-in policies. Attacks geared towards GUI and SSH management access, for example, can be mitigated using IPS signatures pushed from FortiGuard, thereby virtually patching these vulnerabilities.

When the `virtual-patch` option is enabled in a local-in policy, the IPS engine queries the FortiGuard API server using the WAD process to obtain a list of vulnerabilities targeting the FortiGate on a particular version. IPS enables vulnerability rules to scan local-in traffic on the specified interface. All matched local-in traffic is dropped accordingly.

To configure virtual patching:

```
config firewall local-in-policy
    edit <id>
        set virtual-patch {enable | disable}
    next
end
```

The FortiGate must have a valid IPS license, and the extended IPS database must be enabled for more vulnerabilities to be covered in order to use the `virtual-patch` option.

To enable the extended database:

```
config ips global
    set database extended
end
```

Once `virtual-patch` is enabled, the WAD process will periodically query vulnerability items from the FortiGuard API server and forward it to IPS.

Sample vulnerability item found on the FortiGuard API server

```
{"vendor":"fortinet","min_version":"6.0.0","severity":"high","vuln_
type":"Permission/Priviledge/Access Control","refs":["CVE-2018-
13382"],"ID":108824,"product":"fortios","patch_sig_id":0,"description":"An Improper
Authorization vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.8 and 5.4.1 to
5.4.10 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN
web portal allows an unauthenticated attacker to modify the password of an SSL VPN web
portal user via specially crafted HTTP requests","max_version":"6.0.4","date_added":"2022-
09-20 18:33:50.517577","date_updated":"2022-09-20 18:33:50.517594"}
```

FortiGuard can be queried from the FortiOS CLI for a list of vulnerability rules while specifying parameters for the vendor, version, product, and model by running the `diagnose wad dev-vuln query` command. For example, to query Fortinet's FortiOS 7.0.3:

```
# diagnose wad dev-vuln query vendor=fortinet&version=7.0.3&product=fortios
FortiGate-201E # Dev-Vuln fetching is in process...
Dev-Vuln Lookup result: success, cache: miss, fgd: found, item: 0x7fbd2f09e138
Vulnerability details:
 info entry (1):
        'vendor' = fortinet
       'product' = fortios
         'model' = N/A
   'version.min' = 7.0.0
   'version.max' = 7.0.3
      'firmware' = N/A
         'build' = N/A
```

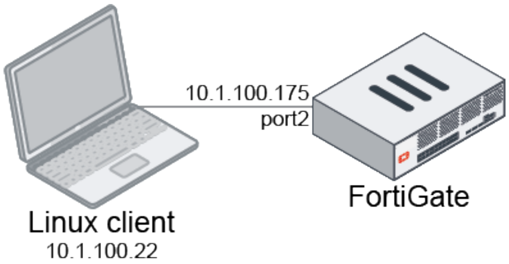
```
     'date_added' = 2022-10-06 17:45:18.208424
   'date_updated' = 2022-10-06 17:45:18.208440
         'sig_id' = 0
        'vuln_id' = 146868
       'severity' = 2
...
```

After receiving the vulnerability rules from the WAD process, the IPS engine marks them as virtual patch rules mapped to each CVE vulnerability signature. For example:

> FortiOS.NodeJS.Proxy.Authentication.Bypass(CVE-2022-40684)
>
> FortiOS.SSL.VPN.Web.Portal.Password.Improper.Authentication(CVE-2018-13382)
>
> FortiOS.SSL.VPN.Web.Protoal.Pathname.Information.Disclosure(CVE-2018-13379)

Example

In this example, the FortiGate's port2 is configured with virtual patching enabled. In the test scenario, the FortiGate is set to debug mode in order to block a harmless attack. IPS will scan local-in traffic and all matched local-in traffic will be dropped accordingly. Intrusion prevention logs will be recorded.



To configure virtual patching on the local-in management interface:

1. Configure the local-in policy:

```
config firewall local-in-policy
    edit 1
        set intf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "ALL"
        set schedule "always"
        set virtual-patch enable
    next
end
```

2. For testing purpose only, enable all signatures for the virtual patch feature:

```
# diagnose ips vpatch enable-all
```

3. From the Linux client, start a cURL download:

```
root@PC02:~# curl -vk -F "file=@eicar" https://10.1.100.175 -m 10
```

The attack is blocked, and a security event log (intrusion prevention) is recorded.

4. Reset the virtual patch enabled signatures back to the default:

```
# diagnose ips vpatch reset
```

Objects

This section includes information about object related new features:

- Allow empty address groups on page 382
- Remove overlap check for VIPs on page 383
- Using IPv6 addresses in the ISDB 7.2.4 on page 384
- Add ISDB on-demand mode to reduce the size stored on the flash drive 7.2.4 on page 386

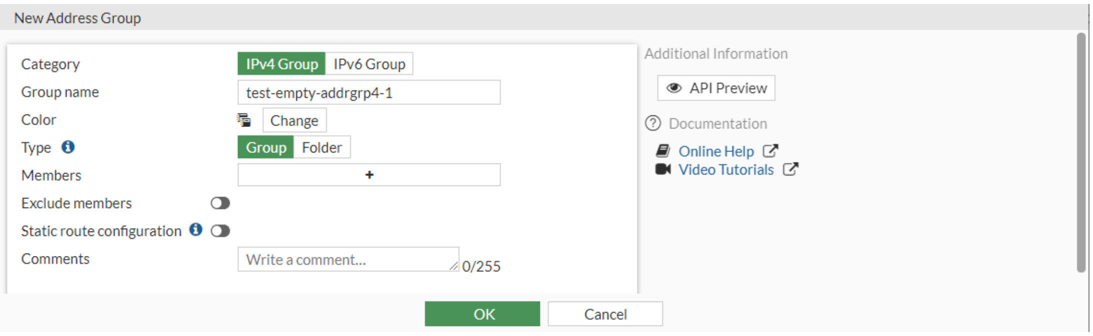
Allow empty address groups

Address groups with no members can be configured in the GUI, CLI, and through the API. In previous versions of FortiOS, error messages appear for empty address groups and they cannot be configured.

When an address group with no members is configured in a firewall policy, the policy will not match any traffic. In this case, policy matching logic will proceed down the list of firewall policies until matching the implicit deny policy.

To create an empty address group in the GUI:

1. Go to *Policy & Objects* > *Addresses* and click *Create New* > *Address Group*.
2. Enter a name.



New Address Group

Category	IPv4 Group
Group name	test-empty-addrgrp4-1
Type	Group
Members	
Exclude members	○
Static route configuration	○
Comments	Write a comment... 0/255

3. Click *OK*. The *This field is required.* error is not displayed under the *Members* field.

To create an empty address group in the CLI:

```
config firewall addrgrp
    edit "test-empty-addrgrp4-1"
    next
end
```

No error message is returned in the console.

Remove overlap check for VIPs

The overlap check for VIPs was removed, so there are no constraints when configuring multiple VIPs with the same external interface and IP. A new security rating report alerts users of any VIP overlaps.

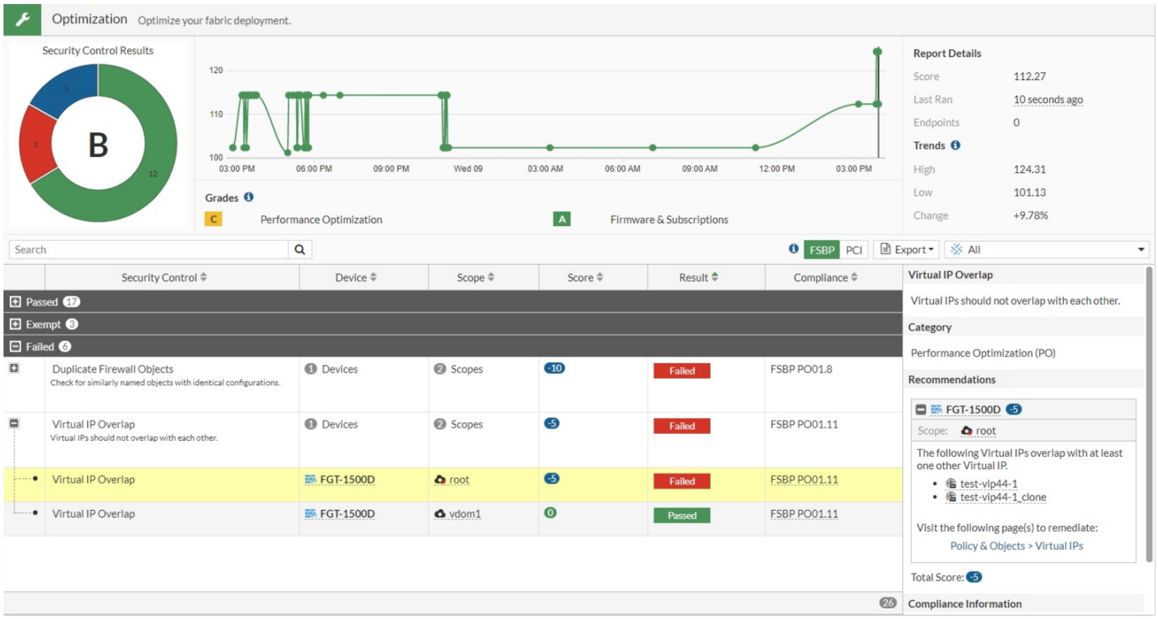
To configure two VIPs with the same external interface and IP:

```
config firewall vip
    edit "test-vip44-1"
        set extip 10.1.100.154
        set mappedip "172.16.200.156"
        set extintf "port24"
    next
    edit "test-vip44-1_clone"
        set extip 10.1.100.154
        set mappedip "172.16.200.156"
        set extintf "port24"
        set src-filter 10.1.100.11
    next
end
```

No error message appears regarding the overlapping VIPs.

To view the security rating report:

1. Go to *Security Fabric* > *Security Rating* and click the *Optimization* scorecard.
2. Expand the *Failed* section. The *Virtual IP Overlap* results show an overlap (*test-vip44-1* and *test-vip44-1_clone*) on the root FortiGate.



Report Details

Score	112.27
Last Ran	10 seconds ago
Endpoints	0
Trends	
High	124.31
Low	101.13
Change	+9.78%

Security Control	Device	Scope	Score	Result	Compliance
Passed 17					
Exempt 3					
Failed 6					
Duplicate Firewall Objects Check for similarly named objects with identical configurations.	1 Devices	2 Scopes	-10	Failed	FSBP PO01.8
Virtual IP Overlap Virtual IPs should not overlap with each other.	1 Devices	2 Scopes	-5	Failed	FSBP PO01.11
Virtual IP Overlap	FGT-1500D	root	-5	Failed	FSBP PO01.11
Virtual IP Overlap	FGT-1500D	vdom1	0	Passed	FSBP PO01.11

26

Virtual IP Overlap

Virtual IPs should not overlap with each other.

Category

Performance Optimization (PO)

Recommendations

FGT-1500D -5

Scope: root

The following Virtual IPs overlap with at least one other Virtual IP.

- test-vip44-1
- test-vip44-1_clone

Visit the following page(s) to remediate:

Policy & Objects > Virtual IPs

Total Score: -5

Compliance Information

Using IPv6 addresses in the ISDB - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

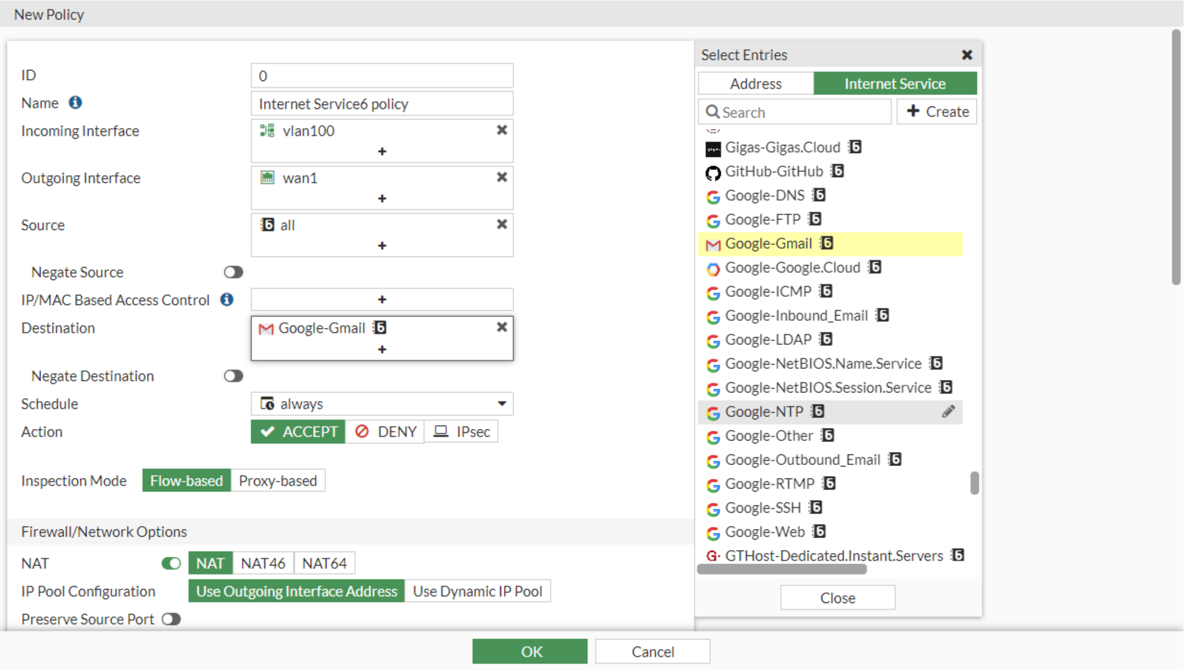
- Sample IPv6 configuration

IPv6 addresses are supported in the Internet Service Database (ISDB), and they can be configured in firewall policies.

In this example, the Google Gmail IPv6 ISDB address is used as a destination in a firewall policy.

To configure a policy with an IPv6 ISDB address in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. In the *Destination* field, click the + and select the *Internet Service* tab.
3. In the *IPV6 INTERNET SERVICE* section, select *Google Gmail*.



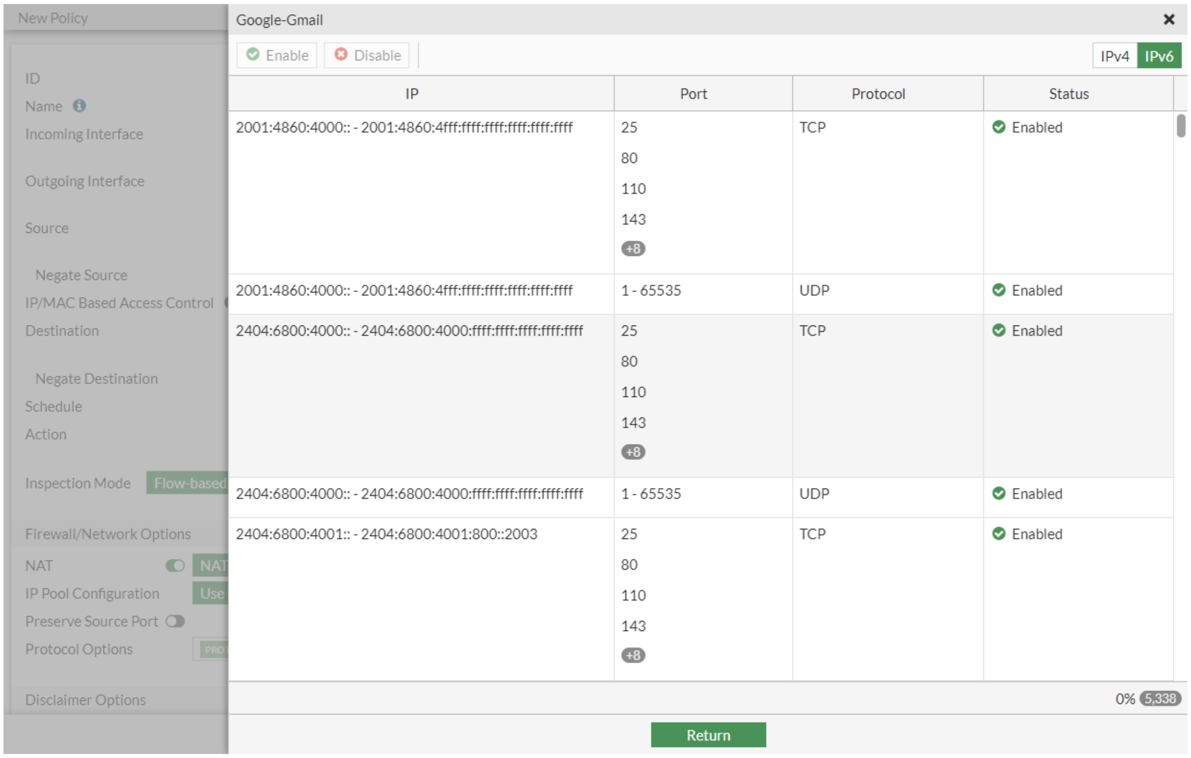
New Policy

ID	0
Name	Internet Service6 policy
Incoming Interface	vlan100
Outgoing Interface	wan1
Source	all
Negate Source	○
IP/MAC Based Access Control	+
Destination	Google-Gmail
Negate Destination	○
Schedule	always
Action	ACCEPT / DENY / IPsec
Inspection Mode	Flow-based / Proxy-based

Firewall/Network Options

NAT	● NAT / NAT46 / NAT64
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic IP Pool
Preserve Source Port	○

4. Optionally, hover over the *Google Gmail* and click *View/Edit Entries*. A pane appears that displays the IPv6 address ranges for this Internet Service.



IP	Port	Protocol	Status
2001:4860:4000:: - 2001:4860:4fff:ffff:ffff:ffff:ffff:ffff	25 80 110 143 +8	TCP	✓ Enabled
2001:4860:4000:: - 2001:4860:4fff:ffff:ffff:ffff:ffff:ffff	1 - 65535	UDP	✓ Enabled
2404:6800:4000:: - 2404:6800:4000:ffff:ffff:ffff:ffff:ffff	25 80 110 143 +8	TCP	✓ Enabled
2404:6800:4000:: - 2404:6800:4000:ffff:ffff:ffff:ffff:ffff	1 - 65535	UDP	✓ Enabled
2404:6800:4001:: - 2404:6800:4001:800::2003	25 80 110 143 +8	TCP	✓ Enabled

5. Click *Return* to close the pane.
6. Configure the other settings as needed.
7. Click *OK*.

To configure a policy with an IPv6 ISDB address in the CLI:

```
config firewall policy
    edit 4
        set name "Internet Service6 policy"
        set srcintf "vlan100"
        set dstintf "wan1"
        set action accept
        set srcaddr6 "all"
        set internet-service6 enable
        set internet-service6-name "Google-Gmail"
        set schedule "always"
        set nat enable
    next
end
```

To view IPv6 ISDB address entries in the kernel:

```
# diagnose firewall internet-service6-prio-id list
List internet service in kernel(prio-id):
65646(Google-Gmail)
```

To view summary details for the Google Gmail IPv6 ISDB address:

```
# diagnose internet-service6 id-summary 65646

Version: 00007.02907
Timestamp: 202212161345
Total number of IP ranges: 36878
Number of Groups: 12
Group(0), Singularity(20), Number of IP ranges(60)
Group(1), Singularity(18), Number of IP ranges(12)
Group(2), Singularity(17), Number of IP ranges(2728)
Group(3), Singularity(16), Number of IP ranges(2812)
Group(4), Singularity(15), Number of IP ranges(4011)
Group(5), Singularity(10), Number of IP ranges(2345)
Group(6), Singularity(9), Number of IP ranges(14)
Group(7), Singularity(8), Number of IP ranges(1555)
Group(8), Singularity(7), Number of IP ranges(2704)
Group(9), Singularity(6), Number of IP ranges(7300)
Group(10), Singularity(5), Number of IP ranges(3154)
Group(11), Singularity(4), Number of IP ranges(10183)
Internet Service: 65646(Google-Gmail)
Number of IP ranges: 482
Singularity: 15
Icon Id: 510
Direction: both
Data source: isdb
Country: 32 36 56 76 124 152 158 203 208 246 250 276 344 348 356 372 376 380 392 404 458 484
        528 616 634 643 682 702 710 724 752 756 784 826 840
Region: 65535
City: 65535
```

Add ISDB on-demand mode to reduce the size stored on the flash drive - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Internet Service Database on-demand mode

Internet Service Database (ISDB) on-demand mode replaces the full-sized ISDB file with a much smaller file that is downloaded onto the flash drive. This file contains only the essential entries for Internet Services. When a service is used in a firewall policy, the FortiGate queries FortiGuard to download the IP addresses and stores them on the flash drive. The FortiGate also queries the local MAC Database (MADB) for corresponding MAC information. The content of the ISDB entries used in firewall policies persists through reboots.

To enable ISDB (FFDB) on-demand mode:

1. Configure the global setting:

   ```
   config system global
       set internet-service-database on-demand
   end
   ```

   All FFDB files are erased.
2. Verify that there are no ISDB (FFDB) files:

```
# diagnose autoupdate versions | grep Internet -A 6
Internet-service On-Demand Database
---------
Version: 0.00000
Contract Expiry Date: n/a
Last Updated using manual update on Mon Jan  1 00:00:00 2001
Last Update Attempt: n/a
Result: Updates Installed
```

Shortly after, the ISDB (FFDB) data structure is downloaded on the FortiGate. The following message appears in the debug messages:

```
do_ffsr_update[1567]-Starting  Update FFDB ondemand:(not final retry)
```

3. Run diagnostics again to verify that the ISDB (FFDB) files are saved on the FortiGate flash drive:

```
# diagnose autoupdate versions | grep Internet -A 6
Internet-service On-Demand Database
---------
Version: 7.02950
Contract Expiry Date: n/a
Last Updated using manual update on Fri Jan  6 06:45:00 2023
Last Update Attempt: n/a
Result: Updates Installed
```

4. Since no services have been applied to a policy, the IP range and IP address values are blank in the the summary details. For example, check the summary details for ID 1245187, Fortinet DNS:

```
# diagnose internet-service id-summary 1245187
Version: 00007.02950
Timestamp: 202301060645
Total number of IP ranges: 3085
Number of Groups: 1
Group(0), Singularity(90), Number of IP ranges(3085)
Internet Service: 1245187(Fortinet-DNS)
Number of IP ranges: 0
Number of IP addresses: 0
Singularity: 0
Icon Id: 19
Direction: dst
Data source: isdb
Country:
Region:
City:
```

5. Apply the Fortinet DNS service in a firewall policy:

```
config firewall policy
    edit 1
        set name "FDNS"
        set srcintf "port1"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set internet-service enable
        set internet-service-name "Fortinet-DNS"
        set schedule "always"
        set nat enable
    next
end
```

6. Verify the summary details again for ID 1245187 (Fortinet DNS). There is now data for the IP range and IP address values:

```
# diagnose internet-service id-summary 1245187
Version: 00007.02951
Timestamp: 202301061144
Total number of IP ranges: 3558
Number of Groups: 2
Group(0), Singularity(90), Number of IP ranges(3078)
Group(1), Singularity(10), Number of IP ranges(480)
Internet Service: 1245187(Fortinet-DNS)
Number of IP ranges: 480
Number of IP addresses: 55242
Singularity: 10
Icon Id: 19
Direction: dst
Data source: isdb
Country: 12 32 36 40 56 124 158 170 203 222 250 276 320 332 344 356 360 372 380 392 458
484
        528 591 600 604 642 643 702 764 784 807 826 840
Region: 55 132 159 169 251 261 283 444 501 509 529 565 596 634 697 709 721 742 744 758
776 860
        1002 1056 1073 1151 1180 1190 1195 1216 1264 1280 1283 1284 1287 1290 1315 1319
1348 1363 1373 1380 1387
        1437 1457 1509 1536 1539 1660 1699 1740 1752 1776 1777 1826 1833 1874 1906 1965
2014 2028 2039 2060 2063
        2147 2206 65535
City: 615 679 818 1001 1106 1117 1180 1207 1330 1668 1986 2139 2812 2868 3380 3438 3485
3670 4276 4588 4622 4904
        5334 5549 5654 5827 6322 6325 6330 6355 6652 7844 9055 10199 10333 11420 12930
13426 13685 13769 14107 14813 15121
        15220 15507 15670 16347 16561 16564 16567 16631 17646 17746 17885 17975 17995
18071 18476 19066 19285 20784 21065 21092 21136
        21146 21266 21337 21779 21993 22292 22414 22912 23352 23367 23487 23574 23635
23871 23963 24076 24203 24298 24611 24955 25050
        25332 26854 27192 27350 28825 28866 65535
```

To verify MAC vendor information:

```
# diagnose vendor-mac id 1
Vendor MAC: 1(ASUS)
Version: 0000100146
Timestamp: 202301031100
Number of MAC ranges: 85
00:04:0f:00:00:00 - 00:04:0f:ff:ff:ff
00:0c:6e:00:00:00 - 00:0c:6e:ff:ff:ff
00:0e:a6:00:00:00 - 00:0e:a6:ff:ff:ff
...
```

Security profiles

This section includes information about security profile related new features:

- Antivirus on page 389
- Web filter on page 400
- IPS on page 403
- Others on page 405

Antivirus

This section includes information about antivirus related new features:

- FortiSandbox inline scanning on page 389
- Inline scanning with FortiGuard AI-Based Sandbox Service 7.2.1 on page 395
- Antivirus exempt list for files based on individual hash 7.2.4 on page 399

FortiSandbox inline scanning

FortiOS supports FortiSandbox inline scanning in proxy inspection mode. When inline scanning is enabled, the client's file is held while it is sent to FortiSandbox for inspection. During this time, the FortiGate may apply client comforting (see Protocol options in the FortiOS Administration Guide). For example, leaking a certain amount of bytes at a certain time interval to the client. Once a verdict is returned, the appropriate action (allow or block) is performed on the held file. If there is an error connecting to the FortiSandbox or a timeout on the FortiSandbox scanning the file within the default 50 seconds, the file can be passed, logged, or blocked based on FortiGate's configuration.

Inline scanning requires a FortiSandbox appliance running version 4.2 or later, and the FortiSandbox must be reachable by port 4443. This feature is not supported on FortiSandbox Cloud or FortiGate Cloud Sandbox. See Understanding Inline Block feature in the FortiSandbox Best Practices for more information.

FortiSandbox inline scanning is disabled by default. FortiSandbox inline scanning is best used in conjunction with AV engine scanning since there is a higher rate of detection by using both at the same time.

To enable FortiSandbox inline scanning:

```
config system fortisandbox
    set status enable
    set inline-scan {enable | disable}
    set server <fortisandbox_server_ip>
end
```

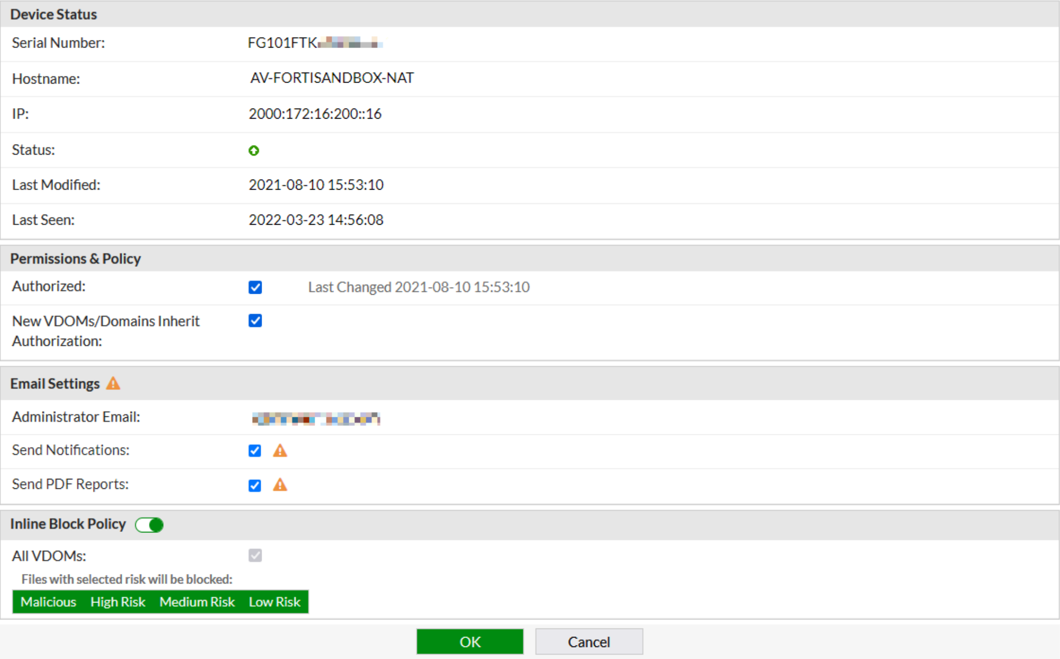
To configure the FortiSandbox scanning options in an antivirus profile:

```
config antivirus profile
    edit <name>
        set fortisandbox-mode {inline | analytics-suspicious | analytics-everything}
        set fortisandbox-error-action {ignore | log-only | block}
        set fortisandbox-timeout-action {ignore | log-only | block}
        set fortisandbox-max-upload <integer>
        config {http | ftp | imap | pop3 | smtp | mapi | cifs | ssh}
            set av-scan {disable | block | monitor}
            set fortisandbox {disable | block | monitor}
        end
    next
end
```

`fortisandbox-mode {inline	analytics-suspicious	analytics-everything}`	Set the FortiSandbox scan mode: • `inline`: FortiSandbox inline scanning • `analytics-suspicious`: FortiSandbox post-transfer scanning; submit supported files if heuristics or other methods determine they are suspicious • `analytics-everything`: FortiSandbox post-transfer scanning; submit supported files and known infected files (default)
`fortisandbox-error-action {ignore	log-only	block}`	Set the action to take if FortiSandbox inline scanning encounters an error reaching the FortiSandbox: • `ignore`: take no action • `log-only`: log the FortiSandbox inline scan error, but allow the file (default) • `block`: block the file upon FortiSandbox inline scan error
`fortisandbox-timeout-action {ignore	log-only	block}`	Set the action to take if FortiSandbox inline scanning encounters a scan timeout: • `ignore`: take no action • `log-only`: log the FortiSandbox inline scan timeout, but allow the file (default) • `block`: block the file upon FortiSandbox inline scan timeout
`fortisandbox-max-upload <integer>`	Set the maximum size of files that can be uploaded to FortiSandbox (1 - 396, default = 10).
`av-scan {disable	block	monitor}`	Enable the antivirus scan service. Set to `block` or `monitor` to work with FortiSandbox (default = `disable`).
`fortisandbox {disable	block	monitor}`	Set the protocol level parameter for FortiSandbox file scanning: • `disable` (default), `block`, and `monitor` are available for inline scanning • `disable` (default) and `monitor` are available for post-transfer scanning

Basic configuration

This example assumes that *Inline Block Policy* is already enabled in FortiSandbox for the FortiGate with selected risk levels (see FortiGate devices in the FortiSandbox Administration Guide for more information). The inline block policy in this example blocks all risk levels: malicious, high risk, medium risk, and low risk.



Device Status

Serial Number:	FG101FTK[redacted]
Hostname:	AV-FORTISANDBOX-NAT
IP:	2000:172:16:200::16
Status:	●
Last Modified:	2021-08-10 15:53:10
Last Seen:	2022-03-23 14:56:08

Permissions & Policy

Authorized:	☑ Last Changed 2021-08-10 15:53:10
New VDOMs/Domains Inherit Authorization:	☑

Email Settings ⚠

Administrator Email:	[redacted]
Send Notifications:	☑ ⚠
Send PDF Reports:	☑ ⚠

Inline Block Policy ●

All VDOMs: ☑

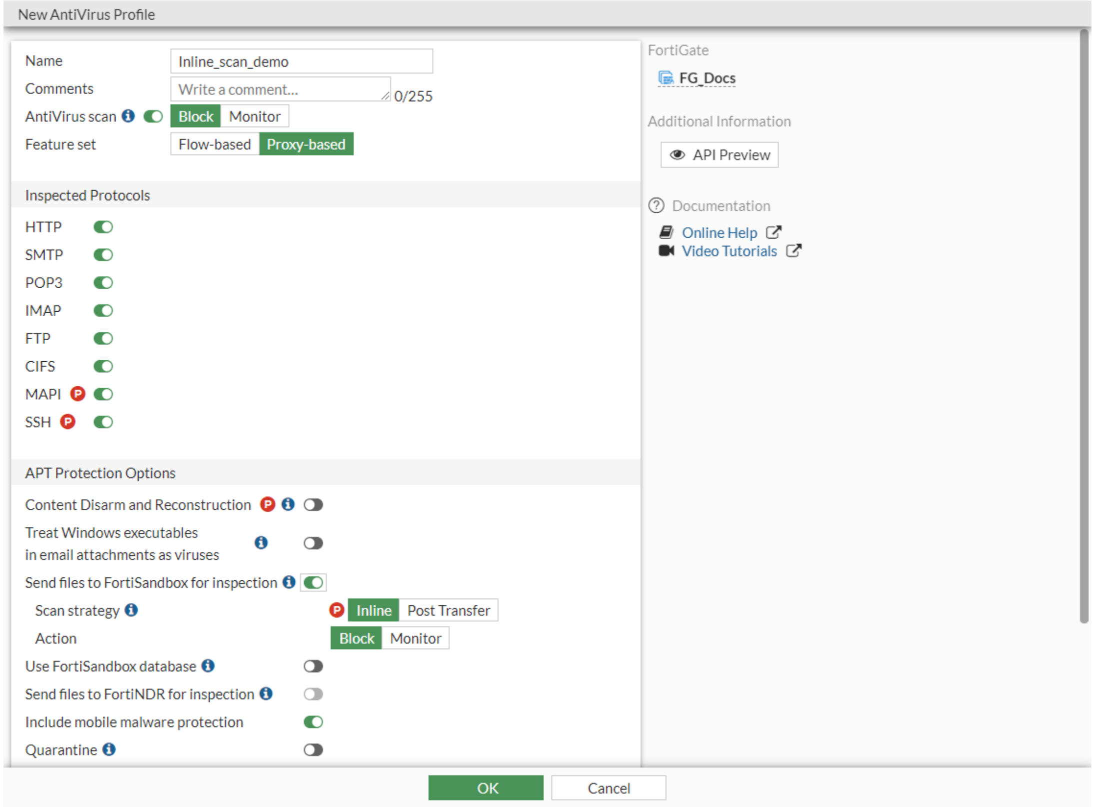
Files with selected risk will be blocked:

To configure FortiSandbox inline scanning in the GUI:

1. Enable FortiSandbox inline scanning globally:

```
config system fortisandbox
    set status enable
    set inline-scan enable
    set server "172.18.70.76"
end
```

2. Configure the antivirus profile:
   a. Go *to Security Profiles* > *AntiVirus* and click *Create New*.
   b. Set the *Feature set* to *Proxy-based*.
   c. Enable the protocols to inspect.
   d. Enable *AntiVirus scan* and set it to *Block*.
   e. Enable *Send files to FortiSandbox* for inspection and set the *Action* to *Block*. The *Scan strategy* appears as *Inline* because it was configured in the CLI.



New AntiVirus Profile

Name: Inline_scan_demo

Comments: Write a comment... 0/255

AntiVirus scan: enabled — Block | Monitor (Block selected)

Feature set: Flow-based | Proxy-based (Proxy-based selected)

Inspected Protocols

- HTTP: enabled
- SMTP: enabled
- POP3: enabled
- IMAP: enabled
- FTP: enabled
- CIFS: enabled
- MAPI: enabled
- SSH: enabled

APT Protection Options

- Content Disarm and Reconstruction: disabled
- Treat Windows executables in email attachments as viruses: disabled
- Send files to FortiSandbox for inspection: enabled
  - Scan strategy: Inline | Post Transfer (Inline selected)
  - Action: Block | Monitor (Block selected)
- Use FortiSandbox database: disabled
- Send files to FortiNDR for inspection: disabled
- Include mobile malware protection: enabled
- Quarantine: disabled

f. Click *OK*.

To configure FortiSandbox inline scanning in the CLI:

1. Enable FortiSandbox inline scanning globally:

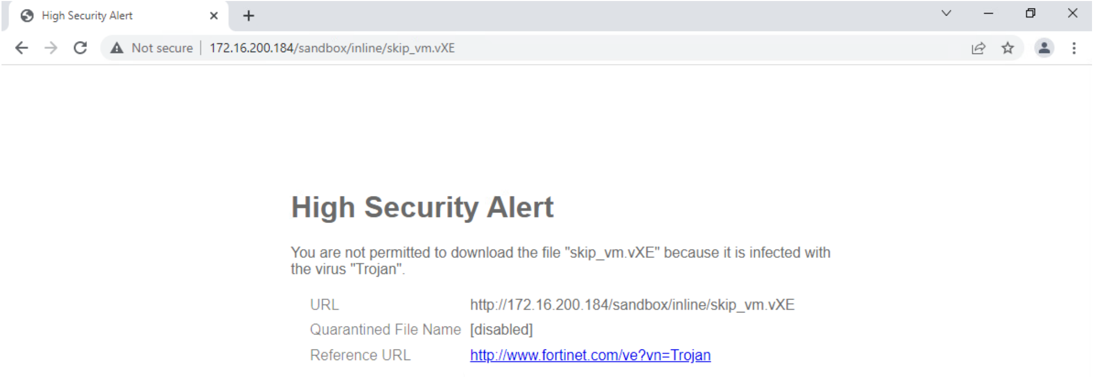
```
config system fortisandbox
    set status enable
    set inline-scan enable
    set server "172.18.70.76"
end
```

2. Configure the antivirus profile:

```
config antivirus profile
    edit "Inline_scan_demo"
        set feature-set proxy
        set fortisandbox-mode inline
        config http
            set av-scan block
            set fortisandbox block
        end
        config ftp
            set av-scan block
            set fortisandbox block
        end
        config imap
            set av-scan block
            set fortisandbox block
        end
        config pop3
            set av-scan block
            set fortisandbox block
        end
        config smtp
            set av-scan block
            set fortisandbox block
        end
        config mapi
            set av-scan block
            set fortisandbox block
        end
        config cifs
            set av-scan block
            set fortisandbox block
        end
        config ssh
            set av-scan block
            set fortisandbox block
        end
    next
end
```

To verify that infected files are blocked inline:

1. On a client, open a web browser and download an infected file.
2. The file is held while being scanned by FortiSandbox. Once FortiSandbox determines that file's risk level is not tolerated by the inline block policy, the FortiGate drops the connection and displays a replacement message that the file cannot be downloaded.



High Security Alert

You are not permitted to download the file "skip_vm.vXE" because it is infected with the virus "Trojan".

URL	http://172.16.200.184/sandbox/inline/skip_vm.vXE
Quarantined File Name	[disabled]
Reference URL	http://www.fortinet.com/ve?vn=Trojan

3. In FortiOS, view the antivirus log.
   - In the GUI, go to *Log & Report* > *Security Events* and click the *AntiVirus* card.
   - In the CLI:

```
# execute log filter category 2
# execute log display
1 logs found.
1 logs returned.

1: date=2022-03-23 time=16:19:37 eventtime=1648077577156255080 tz="-0700"
```

```
logid="0210008232" type="utm" subtype="virus" eventtype="fortisandbox"
level="warning" vd="vdom1" policyid=1 poluuid="9170ca3e-aade-51ec-772b-1d31f135fe26"
policytype="policy" msg="Blocked by FortiSandbox." action="blocked" service="HTTP"
sessionid=10545 srcip=10.1.100.181 dstip=172.16.200.184 srcport=37046 dstport=80
srccountry="Reserved" dstcountry="Reserved" srcintf="port1" srcintfrole="undefined"
dstintf="port9" dstintfrole="undefined" srcuuid="5b426c60-aade-51ec-f020-
b3d334ba18d3" dstuuid="5b426c60-aade-51ec-f020-b3d334ba18d3" proto=6
direction="incoming" filename="skip_vm.vXE" quarskip="File-was-not-quarantined"
virus="Trojan" viruscat="Unknown" dtype="fortisandbox"
ref="http://www.fortinet.com/ve?vn=Trojan" virusid=0
url="http://172.16.200.184/sandbox/inline/skip_vm.vXE" profile="Inline_scan_demo"
agent="curl/7.68.0" httpmethod="GET" analyticssubmit="false" fsaaction="deny"
fsaseverity="high-risk" fsaverdict="block" fsafileid=0 fsafiletype="exe" crscore=50
craction=2 crlevel="critical
```

Configuration with FortiSandbox scanning error and timeout actions

In this example, the HTTP protocol settings for `av-scan` and `fortisandbox` in the AV profile are both set to `block`. All files traversing HTTP in this configuration are scanned by the AV engine first, and then by FortiSandbox inline scanning for further file analysis. Based on the FortiSandbox results, FortiOS will take the appropriate action.

Files can be blocked if they contain a scan error or timeout. The scan timeout is configured in FortiSandbox and set to 50 seconds. If the file scan takes longer than 50 seconds, FortiSandbox returns a timeout to the FortiGate, and file is dropped with the current configuration. If a user tries to download the same file again, the cached result is provided by FortiSandbox to the FortiGate based on the previous file scan.

This example assumes FortiSandbox inline scanning has been configured globally. The FortiGate will block the file if there is an inline scanning error or timeout.

To configure the antivirus profile to block files if there is an inline scanning error or timeout:

```
config antivirus profile
    edit "av"
        set feature-set proxy
        set fortisandbox-mode inline
        config http
            set av-scan block
            set fortisandbox block
        end
        set fortisandbox-error-action block
        set fortisandbox-timeout-action block
    next
end
```

If the administrator decides to take more risk and scan all files traversing HTTP, but log or ignore an inline scanning error or timeout, the profile is modified as follows:

```
config antivirus profile
    edit "av"
        set fortisandbox-error-action {log-only | ignore}
        set fortisandbox-timeout-action {log-only | ignore}
    next
end
```

The AV engine is still used first, followed by FortiSandbox inline scanning. The FortiGate will log or ignore the file if there is an inline scanning error or timeout, and the file is allowed to pass through.

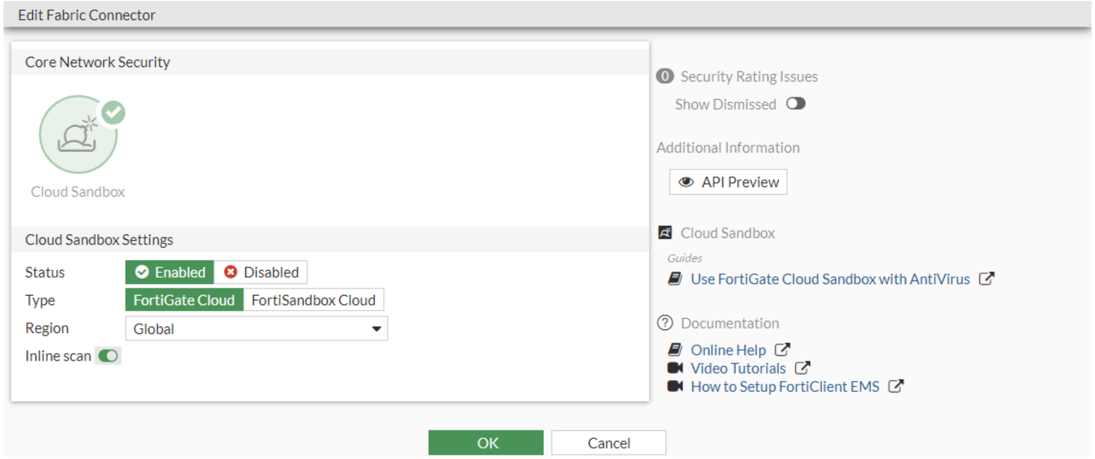
Inline scanning with FortiGuard AI-Based Sandbox Service - 7.2.1

Inline scanning is now supported when the FortiGate is licensed with the FortiGuard AI-Based Sandbox Service (FAIS). It works similar to inline scanning for the FortiSandbox appliance by holding a file up to 50 seconds for the verdict to be returned. Timed out scans can be set to block, log, or ignore (see Configuration with FortiSandbox scanning error and timeout actions for use case examples). Inline scanning can be enabled from the GUI on the *Cloud Sandbox* configuration page.

Inline scanning is supported for FortiSandbox appliance, FortiNDR, and FAIS. On a FortiGate, only a single inline scanning type can be configured at a time.

To configure FAIS inline scanning in the GUI:

1. Enable the FortiGate Cloud feature visibility:
   a. Go to *System* > *Feature Visibility*.
   b. In the *Additional Features* section, enable *FortiGate Cloud Sandbox*.
   c. Click *Apply*.
2. Configure the *Cloud Sandbox* Fabric connector:
   a. Go to *Security Fabric* > *Fabric Connectors* and double-click the *Cloud Sandbox* card.
   b. Set the *Type* to *FortiGate Cloud*.
   c. Select a *Region*.
   d. Enable *Inline scan*.

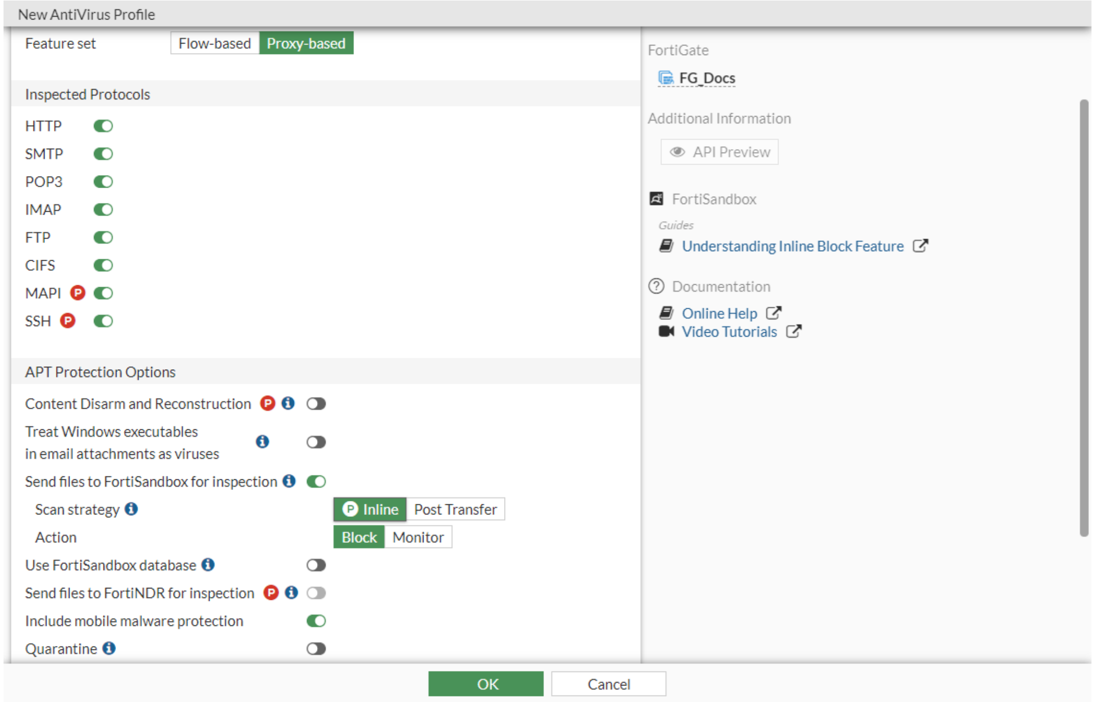


Status: [✓ Enabled] Disabled
Type: [✓ FortiGate Cloud] FortiSandbox Cloud
Region: Global
Inline scan: ●

   e. Click *OK*.
3. Configure the antivirus profile:
   a. Go *to Security Profiles* > *AntiVirus* and click *Create New*.
   b. Set the *Feature set* to *Proxy-based*.
   c. Enable the protocols to inspect.

d. Enable *Send files to FortiSandbox* for inspection.

e. Set the *Scan strategy* to *Inline*, and set the *Action* to *Block*.



New AntiVirus Profile

Feature set: Flow-based [✓ Proxy-based]

Inspected Protocols

HTTP ●
SMTP ●
POP3 ●
IMAP ●
FTP ●
CIFS ●
MAPI ●
SSH ●

APT Protection Options

Content Disarm and Reconstruction ○
Treat Windows executables in email attachments as viruses ○
Send files to FortiSandbox for inspection ●
Scan strategy: [✓ Inline] Post Transfer
Action: [✓ Block] Monitor
Use FortiSandbox database ○
Send files to FortiNDR for inspection ○
Include mobile malware protection ●
Quarantine ○

f. Click *OK*.

To configure FAIS inline scanning in the CLI:

1. Disable FortiSandbox appliance and FortiSandbox Cloud:

```
config system fortisandbox
    set status disable
end
```

2. Configure FortiGate Cloud Sandbox:

```
# execute forticloud-sandbox region
0  Global
1  Europe
2  Japan
3  US
Please select cloud sandbox region[0-3]:0
Cloud sandbox region is selected: Global
```

3. Enable inline scanning for FortiGate Cloud:

```
config system fortiguard
    set sandbox-region "Global"
    set sandbox-inline-scan enable
end
```

4. Configure the antivirus profile:

```
config antivirus profile
    edit "av"
```

```
        set feature-set proxy
        set fortisandbox-mode inline
        config http
            set fortisandbox block
        end
        config ftp
            set fortisandbox block
        end
        config imap
            set fortisandbox block
        end
        config pop3
            set fortisandbox block
        end
        config smtp
            set fortisandbox block
        end
        config mapi
            set fortisandbox block
        end
        config cifs
            set fortisandbox block
        end
        config ssh
            set fortisandbox block
        end
        set scan-mode default
    next
end
```

To verify that infected files are blocked inline:

1. On a client, open a web browser and download an infected file using HTTP.
2. The file is held while being scanned by FortiGate Cloud Sandbox. Once FortiGate Cloud Sandbox determines that file's risk level is not tolerated, the FortiGate drops the connection and displays a replacement message that the file cannot be downloaded.
3. Verify the antivirus log:

```
# execute log display
1 logs found.
1 logs returned.

1: date=2022-07-12 time=16:31:26 eventtime=1657668686245018328 tz="-0700"
logid="0210008232" type="utm" subtype="virus" eventtype="fortisandbox" level="warning"
vd="vdom1" policyid=1 poluuid="54c06312-01fd-51ed-0db5-10c9586a0c2e" policytype="policy"
msg="Blocked by FortiSandbox." action="blocked" service="HTTP" sessionid=19934
srcip=10.1.100.191 dstip=172.16.200.194 srcport=51688 dstport=80 srccountry="Reserved"
dstcountry="Reserved" srcintf="port1" srcintfrole="undefined" dstintf="port9"
dstintfrole="undefined" srcuuid="1cb467b6-01fd-51ed-8abf-72abd959c0d0"
dstuuid="1cb467b6-01fd-51ed-8abf-72abd959c0d0" proto=6 direction="incoming"
filename="skip_vm.vXE" quarskip="Quarantine-disabled" virus="Unknown" viruscat="Trojan"
dtype="fortisandbox" ref="http://www.fortinet.com/ve?vn=Unknown" virusid=0
url="http://172.16.200.194/sandbox/inline/skip_vm.vXE" profile="av" agent="curl/7.68.0"
httpmethod="GET" analyticssubmit="false" fsaaction="deny" fsaverdict="block"
```

```
fsaseverity="high-risk" fsafileid=0 fsafiletype="exe" crscore=50 craction=2
crlevel="critical"
```

To verify that infected files are monitored:

1. Edit the antivirus profile to monitor files over HTTP:

```
config antivirus profile
    edit "av"
        set feature-set proxy
        set fortisandbox-mode inline
        config http
            set fortisandbox monitor
        end
    next
end
```

2. On a client, open a web browser and download an infected file using HTTP.
3. Verify the antivirus log:

```
# execute log display
1 logs found.
1 logs returned.

1: date=2022-07-12 time=16:34:25 eventtime=1657668865371976563 tz="-0700"
logid="0210008233" type="utm" subtype="virus" eventtype="fortisandbox" level="notice"
vd="vdom1" policyid=1 poluuid="54c06312-01fd-51ed-0db5-10c9586a0c2e" policytype="policy"
msg="Detected by FortiSandbox." action="monitored" service="HTTP" sessionid=20002
srcip=10.1.100.191 dstip=172.16.200.194 srcport=51724 dstport=80 srccountry="Reserved"
dstcountry="Reserved" srcintf="port1" srcintfrole="undefined" dstintf="port9"
dstintfrole="undefined" srcuuid="1cb467b6-01fd-51ed-8abf-72abd959c0d0"
dstuuid="1cb467b6-01fd-51ed-8abf-72abd959c0d0" proto=6 direction="incoming"
filename="skip_vm.vXE" quarskip="Quarantine-disabled" virus="Unknown" viruscat="Trojan"
dtype="fortisandbox" ref="http://www.fortinet.com/ve?vn=Unknown" virusid=0
url="http://172.16.200.194/sandbox/inline/skip_vm.vXE" profile="av" agent="curl/7.68.0"
httpmethod="GET" analyticssubmit="false" fsaaction="deny" fsaverdict="block"
fsaseverity="high-risk" fsafileid=0 fsafiletype="exe" crscore=50 craction=2
crlevel="critical"
```

To verify that infected files are blocked inline if a scan timeout occurs:

1. Edit the antivirus profile to block files over HTTP and when there is a scan timeout:

```
config antivirus profile
    edit "av"
        set feature-set proxy
        set fortisandbox-mode inline
        config http
            set fortisandbox block
        end
        set fortisandbox-timeout-action block
    next
end
```

2. On a client, open a web browser and download a large ZIP file (clean file).
3. When the scan timeout occurs, a replacement message appears that *The file "zipfile.zip" is still being scanned and will be released once complete. Please try the transfer again in a few minutes.*

4. Verify the antivirus log:

```
# execute log display
1 logs found.
1 logs returned.

1: date=2022-07-12 time=16:44:51 eventtime=1657669491697816069 tz="-0700"
logid="0210008236" type="utm" subtype="virus" eventtype="fortisandbox" level="warning"
vd="vdom1" policyid=1 poluuid="54c06312-01fd-51ed-0db5-10c9586a0c2e" policytype="policy"
msg="FortiSandbox scan timeout." action="blocked" service="HTTP" sessionid=20258
srcip=10.1.100.191 dstip=172.16.200.194 srcport=51830 dstport=80 srccountry="Reserved"
dstcountry="Reserved" srcintf="port1" srcintfrole="undefined" dstintf="port9"
dstintfrole="undefined" srcuuid="1cb467b6-01fd-51ed-8abf-72abd959c0d0"
dstuuid="1cb467b6-01fd-51ed-8abf-72abd959c0d0" proto=6 direction="incoming"
filename="zipfile.zip" quarskip="Quarantine-disabled"
url="http://172.16.200.194/sandbox/zipfile.zip" profile="av" agent="curl/7.68.0"
httpmethod="GET" analyticssubmit="false" fsaaction="timeout" fsafileid=0 crscore=50
craction=2 crlevel="critical"
```

5. After a few minutes, download the ZIP file again.
6. When the scan is complete on the FortiSandbox side, the file is downloaded and no log is generated because the scan deemed that the file is clean.

Antivirus exempt list for files based on individual hash - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Exempt list for files based on individual hash

The antivirus exempt list allows users to exempt known safe files that happen to be incorrectly classified as malicious by the AV signature and AV engine scan. Users can specify file hashes in MD5, SHA1, or SHA256 for matching, which are applied at a per-VDOM level. When matched, the FortiGate ignores the AV scan verdict so that the corresponding UTM behavior defined in the AV profile is not performed.

```
config antivirus exempt-list
    edit <name>
        set hash-type {md5 | sha1 | sha256}
        set hash <string>
        set status {enable | disable}
    next
end
```

The exempt list does not apply to results from outbreak prevention, machine learning, FortiNDR, or FortiSandbox inline scans.

In this example, an antivirus exempt list is configured for the EICAR anti-malware test file. Although the antivirus profile is configured to block HTTP, the client is able to download the file.

To configure an antivirus exempt list:

1. Configure the antivirus profile:

```
config antivirus profile
    edit "av"
        set feature-set proxy
        config http
            set av-scan block
        end
    next
end
```

2. Configure the antivirus exempt list:

```
config antivirus exempt-list
    edit "test-hash"
        set comment "eicar.com"
        set hash-type md5
        set hash "44d88612fea8a8f36de82e1278abb02f"
        set status enable
    next
end
```

3. Get a client to access https://www.eicar.com/ and download the anti-malware test file.

   The FortiGate exempts the AV scan verdict and bypasses the file. The client can download the file and no replacement message is displayed.

Web filter

This section includes information about web filter related new features:

- Using the Websense Integrated Services Protocol in flow mode on page 400
- Inspecting HTTP3 traffic on page 401

Using the Websense Integrated Services Protocol in flow mode

Websense Integrated Services Protocol (WISP) servers can be used server in flow mode, which allows the FortiGate to send traffic to the third-party web filtering service for rating. This feature was previously only supported in proxy-based security profiles.

When a WISP server is used in a web filter profile, in flow or proxy mode, the following web filter scanning priority sequence is used:

1. Local URL filter
2. Websense web filtering service
3. FortiGuard web filtering service

To use a WISP server in flow mode:

1. Configure the WISP servers:

```
config web-proxy wisp
    edit "wisp1"
        set server-ip 10.2.3.4
    next
    edit "wisp2"
        set server-ip 10.2.3.5
    next
    edit "wisp3"
        set server-ip 192.168.1.2
    next
    edit "wisp4"
        set server-ip 192.168.3.4
    next
end
```

2. Configure the web filter profile:

```
config webfilter profile
    edit "webfilter_flowbase"
        set feature-set flow
        config ftgd-wf
            unset options
            config filters
                edit 64
                    set category 64
                    set action block
                next
            end
        end
        set wisp enable
        set wisp-servers "wisp1" "wisp2"
        set wisp-algorithm {primary-secondary | round-robin | auto-learning}
        set log-all-url enable
    next
end
```

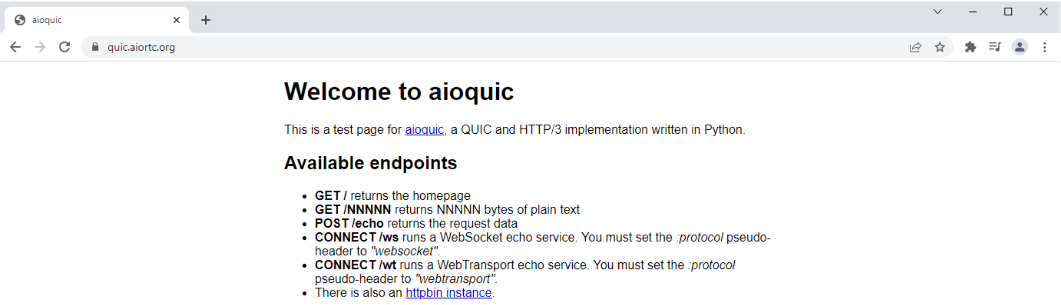
Inspecting HTTP3 traffic

HTTP/3 traffic can be inspected on the FortiGate in flow mode inspection.

When using Chrome, the browser may switch the HTTP/3 connection to HTTP/2 when deep inspection is applied, due to its sensitivity to delays caused by deep inspection.

Example

In this example, a web filter profile is created to block the words *Welcome to aioquic*, which appear in a website that uses HTTP/3.



Welcome to aioquic

This is a test page for aioquic, a QUIC and HTTP/3 implementation written in Python.

Available endpoints

- **GET /** returns the homepage
- **GET /NNNNN** returns NNNNN bytes of plain text
- **POST /echo** returns the request data
- **CONNECT /ws** runs a WebSocket echo service. You must set the *:protocol* pseudo-header to *"websocket"*.
- **CONNECT /wt** runs a WebTransport echo service. You must set the *:protocol* pseudo-header to *"webtransport"*.
- There is also an httpbin instance.

To block content in HTTP/3 traffic:

1. Configure the web filter banned word table:

```
config webfilter content
    edit 1
        set name "aioquic"
        config entries
            edit "Welcome to aioquic"
                set status enable
            next
        end
    next
end
```

2. Apply the banned word table in the web filter profile:

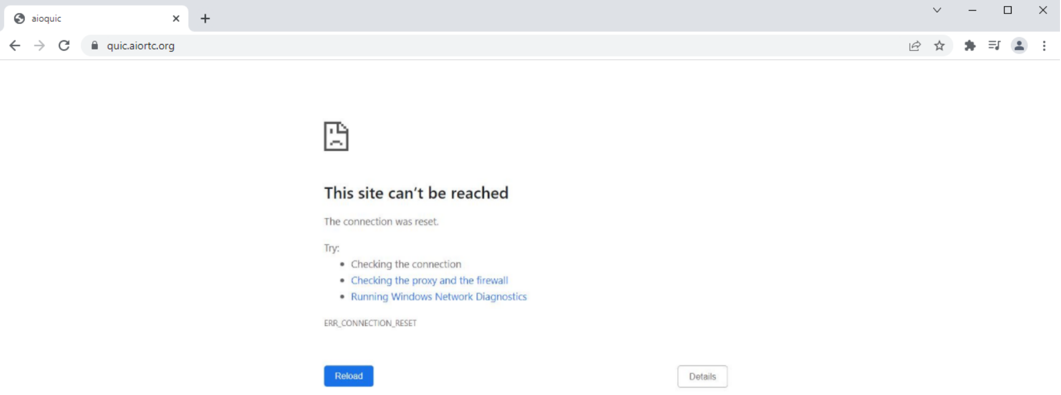
```
config webfilter profile
    edit "flow-webfilter"
        config web
            set bword-table 1
        end
        config ftgd-wf
            unset options
        end
    next
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set webfilter-profile "flow-webfilter"
        set logtraffic all
        set nat enable
    next
end
```

4. Access the website using a supported HTTP/3 client, such as Chrome or Firefox. The website is blocked by the

FortiGate.



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

IPS

This section includes information about IPS related new features:

- IPS sensor entry filters on page 403
- Support full extended IPS database for CP9 models and slim extended database for other physical models on page 404
- Support full extended IPS database for FortiGate VMs with eight cores or more 7.2.5 on page 405

IPS sensor entry filters

When configuring IPS sensor profiles, IPS signatures can be filtered based on the attributes: default status, default action, vulnerability type, and the last update date. When monitoring the specific, filtered signatures, logs are not generated for other, irrelevant signatures.

This avoids generating a lot of false positives due to many signatures having the pass action, which is never logged.

To use the filters in an IPS sensor profile:

```
config ips sensor
    edit "test_default"
        config entries
            edit 1
                set default-action pass
                set default-status enable
                set vuln-type 12
                set last-modified before 2020/02/02
            next
        end
    next
end
```

default-action {pass | block | all}	Filter by signatures' default actions (default = all).

default-status {enable | disable | all}	Filter by signatures' default statuses (default = all).
vuln-type <integer> ... <integer>	Filter by signatures' vulnerability types.
last-modified {before | after | between} <date> [end-date]	Filter by signatures' last modified date (default = before 00/00/00). The date format is `yyyy/mm/dd`. The year range is 2001 - 2050.

When the IPS profile is used in a firewall profile and then the EICAR virus test file signature is triggered, the signature matches the values set in the filter and logs are generated:

```
1:date=2022-02-15 time=14:07:03 eventtime=1644962823303491048 tz="-0800" logid="0419016384"
type="utm" subtype="ips" eventtype="signature" level="alert" vd="vd1" severity="info"
srcip=10.1.100.11 srccountry="Reserved" dstip=172.16.200.55 dstcountry="Reserved"
srcintf="port38" srcintfrole="undefined" dstintf="port37" dstintfrole="undefined"
sessionid=1171 action="detected" proto=6 service="HTTP" policyid=1 poluuid="623d2d28-8ea7-
51ec-00ef-7549685a77c2" policytype="policy" attack="Eicar.Virus.Test.File" srcport=47230
dstport=80 hostname="172.16.200.55" url="/virus/eicar" direction="incoming" attackid=29844
profile="test_default" ref="http://www.fortinet.com/ids/VID29844" incidentserialno=103809025
msg="file_transfer: Eicar.Virus.Test.File"
```

```
# get ips rule status | grep Eicar.Virus.Test.File -A 18
rule-name: "Eicar.Virus.Test.File"
rule-id: 29844
rev: 10.111
date: 1491926400
action: pass
status: enable
log: disable
log-packet: disable
severity: 0.info
service: TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP
location: server, client
os: All
application: Other
rate-count: 0
rate-duration: 0
rate-track: none
rate-mode: continuous
vuln_type: Anomaly
```

Support full extended IPS database for CP9 models and slim extended database for other physical models

FortiGate models with the CP9 SPU receive the IPS full extended database (DB), and the other physical FortiGate models receive a slim version of the extended DB. The slim-extended DB is a smaller version of the full extended DB that contains top active IPS signatures. It is designed for customers who prefer performance.

Customers with non-CP9 SPU models need to upgrade to a CP9 SPU model (physical FortiGate) in order to get full IPS signature coverage. All FortiGate models 200 (E and F) and higher have a CP9 SPU.

See Determining the content processor in your FortiGate unit in the FortiOS Hardware Acceleration Guide to check if your device has a CP9 SPU.

Support full extended IPS database for FortiGate VMs with eight cores or more - 7.2.5

FortiGate VMs with eight or more vCPUs can be configured to have a minimum of eight cores to be eligible to run the full extended database (DB). Any FortiGate VM with less than eight cores will receive a slim version of the extended DB. The slim-extended DB is a smaller version of the full extended DB that contains top active IPS signatures. It is designed for customers who prefer performance.

Others

This section includes information about other security profile related new features:

- Add email filters for block allow lists on page 405
- Enhance the DLP backend and configurations on page 409
- Add option to disable the FortiGuard IP address rating on page 416
- ICAP scanning with SCP and FTP on page 416
- Add persistency for banned IP list 7.2.1 on page 419
- Reduce memory usage on FortiGate models with 2 GB RAM or less by not running WAD processes for unused proxy features 7.2.1 on page 421
- Allow the YouTube channel override action to take precedence 7.2.1 on page 421
- Add REST API for IPS session monitoring 7.2.4 on page 421
- Hide proxy features in the GUI by default for models with 2 GB RAM or less 7.2.4 on page 423
- Re-introduce DLP profiles in the GUI 7.2.4 on page 425
- Remove option to block QUIC by default in application control 7.2.4 on page 431
- Improve replacement message displayed in blocked videos 7.2.5 on page 433
- Introduce SIP IPS profile as a complement to SIP ALG 7.2.5 on page 433

Add email filters for block allow lists

Two new email block/allow list filters have been added to match the recipient address (email-to) and subject (subject). The email address type (email) in previous FortiOS versions has been changed to email sender (email-from).

When upgrading, any email entries are converted to email-from.

```
config emailfilter block-allow-list
    edit <id>
        set name <string>
        config entries
            edit <id>
                set type {ip | email-to | email-from | subject}
            next
        end
    next
end
```

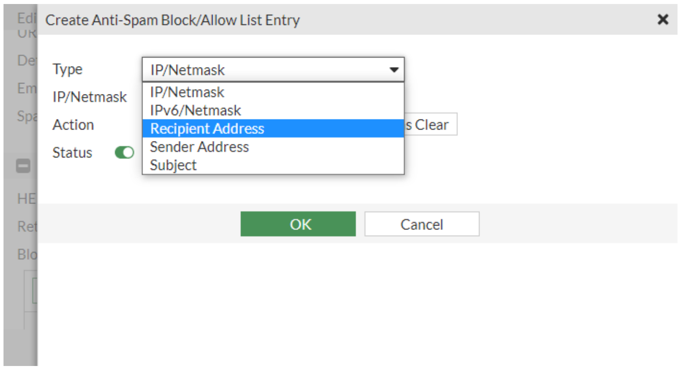
The new filter types are currently not supported in flow inspection mode.

When downgrading from 7.2 to earlier versions, `email-from`, `email-to`, and `subject` entries could be lost.

In this example, an email filter is configured with three block/allow list entries that use the new email-related entry types.

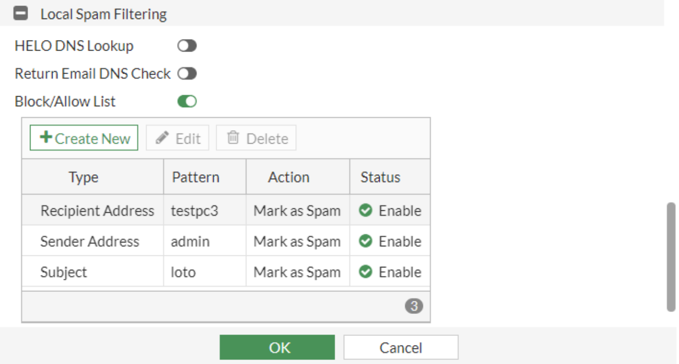
To configure block/allow list filters in the GUI:

1. Go to *Security Profiles* > *Email Filter* and click *Create New*.
2. Enter a *Name*, set the *Feature set* to *Proxy-based*.
3. Enable *Enable spam detection and filtering*.
4. In the *Local Spam Filtering* section, enable *Block/Allow List*.
5. Create the recipient address filter:
   a. Click *Create New*. The *Create Anti-Spam Block/Allow List Entry* pane opens.
   b. Select the *Recipient Address* filter *Type*, enter a *Pattern*, and select *Mark as Spam*.



   c. Click *OK*. The *Recipient Address* filter type has been added to the Block/Allow List.
6. Create the sender address filter:
   a. Click *Create New*.
   b. Select the *Sender Address* filter *Type*, enter a *Pattern*, and select *Mark as Spam*.
   c. Click *OK*. The *Sender Address* filter type has been added to the Block/Allow List.
7. Create the subject filter:
   a. Click *Create New*.
   b. Select the *Subject* filter *Type*, enter a *Pattern*, and select *Mark as Spam*.

c. Click *OK*. The *Subject* filter type has been added to the Block/Allow List.



Local Spam Filtering

HELO DNS Lookup

Return Email DNS Check

Block/Allow List

Type	Pattern	Action	Status
Recipient Address	testpc3	Mark as Spam	✓ Enable
Sender Address	admin	Mark as Spam	✓ Enable
Subject	loto	Mark as Spam	✓ Enable

8. Click *OK*.
9. Configure the firewall policy:
   a. Go to *Policy & Objects > Firewall Policy* and click *Create New*, or edit an existing policy.
   b. Configure the other settings as needed.
   c. Enable the *Email Filter* option and select the previously created profile.
   d. Configure the other settings as needed.
   e. Click *OK*.

To configure block/allow list filters in the CLI:

1. Configure the block/allow list entries:

```
config emailfilter block-allow-list
    edit 3
        set name "newBALtypes"
        config entries
            edit 1
                set type email-to
                set pattern "testpc3"
            next
            edit 2
                set type email-from
                set pattern "admin"
            next
            edit 3
                set type subject
                set pattern "loto"
            next
        end
    next
end
```

2. Configure the email filter profile:

```
config emailfilter profile
    edit "newBALtypes"
        set feature-set proxy
        set spam-filtering enable
        set options spambal
        config imap
            set action tag
        end
        config pop3
            set action tag
        end
        config smtp
            set action discard
        end
        set spam-bal-table 3
    next
end
```

3. Use the email filter profile in a firewall policy:

```
    config firewall policy
        edit 1
            set utm-status enable
            set inspection-mode proxy
            set emailfilter-profile "newBALtypes"
            set nat enable
        next
    end
```

When an email is detected as spam for one of the defined filter types, the FortiGate will reply to the SMTP message with a 554 5.7.1 code and insert the following replacement messages:

Filter type	Message
Blocked for `email-to`	This message has been blocked because mail to this email address is not allowed.
Blocked for `email-from`	This message has been blocked because mail from this email address is not allowed.
Blocked for `subject`	This message has been blocked because the subject contains a banned phrase.

To view the generated UTM logs in the GUI, go to *Log & Report* > *Security Events* and click the *Anti-Spam* card.

To view and filter the UTM logs in the CLI:

```
# execute log filter category 5
```

```
# execute log display
```

```
1: date=2022-02-17 time=19:38:13 eventtime=1645155493096591226 tz="-0800" logid="0513020480"
type="utm" subtype="emailfilter" eventtype="spam" level="notice" vd="vdom1" policyid=1
poluuid="ed18d1fe-8f60-51ec-c782-68322b3bfbe1" policytype="policy" sessionid=26031
srcip=10.1.100.22 srcport=32952 srccountry="Reserved" srcintf="port21"
srcintfrole="undefined" srcuuid="cc019bd6-8f60-51ec-323a-03b14a3c17bf" dstip=172.16.200.55
dstport=25 dstcountry="Reserved" dstintf="port17" dstintfrole="undefined" dstuuid="cc019bd6-
8f60-51ec-323a-03b14a3c17bf" proto=6 service="SMTP" profile="newBALtypes" action="blocked"
from="testpc3@qa.fortinet.com" to="testpc3@qa.fortinet.com" sender="testpc3@qa.fortinet.com"
recipient="testpc3@qa.fortinet.com" direction="outgoing" msg="subject is in email blocklist.
(no.3 pattern matched)" subject="loto" size="230" attachment="no"
```

```
2: date=2022-02-17 time=19:37:10 eventtime=1645155430137897870 tz="-0800" logid="0513020480"
type="utm" subtype="emailfilter" eventtype="spam" level="notice" vd="vdom1" policyid=1
poluuid="ed18d1fe-8f60-51ec-c782-68322b3bfbe1" policytype="policy" sessionid=25908
srcip=10.1.100.22 srcport=32948 srccountry="Reserved" srcintf="port21"
```

```
srcintfrole="undefined" srcuuid="cc019bd6-8f60-51ec-323a-03b14a3c17bf" dstip=172.16.200.55
dstport=25 dstcountry="Reserved" dstintf="port17" dstintfrole="undefined" dstuuid="cc019bd6-
8f60-51ec-323a-03b14a3c17bf" proto=6 service="SMTP" profile="newBALtypes" action="blocked"
from="testpc3@qa.fortinet.com" direction="outgoing" msg="from email address is in email
blocklist.(no.2 pattern matched)" size="0"

3: date=2022-02-17 time=19:28:20 eventtime=1645154899989684584 tz="-0800" logid="0513020480"
type="utm" subtype="emailfilter" eventtype="spam" level="notice" vd="vdom1" policyid=1
poluuid="ed18d1fe-8f60-51ec-c782-68322b3bfbe1" policytype="policy" sessionid=25008
srcip=10.1.100.22 srcport=32940 srccountry="Reserved" srcintf="port21"
srcintfrole="undefined" srcuuid="cc019bd6-8f60-51ec-323a-03b14a3c17bf" dstip=172.16.200.55
dstport=25 dstcountry="Reserved" dstintf="port17" dstintfrole="undefined" dstuuid="cc019bd6-
8f60-51ec-323a-03b14a3c17bf" proto=6 service="SMTP" profile="newBALtypes" action="blocked"
from="testpc3@qa.fortinet.com" to="testpc3@qa.fortinet.com" direction="outgoing" msg="to
email address is in email blocklist.(no.1 pattern matched)" size="0"
```

Enhance the DLP backend and configurations

The DLP backend has been enhanced to use Hyperscan to perform a one-parse algorithm for scanning multiple patterns. This allows DLP to scale up without any performance downgrade.

DLP configurations have been improved and changed in the following ways:

- Separate DLP settings into data type, dictionary, sensor, and profile configurations.
- Add DLP data type that includes five pre-defined data types to match for keyword, regex, hex, credit card, and social security number (SSN). Custom data types can be added.

```
config dlp data-type
    edit "keyword"
        set pattern "built-in"
    next
    edit "regex"
        set pattern "built-in"
    next
    edit "hex"
        set pattern "built-in"
    next
    edit "credit-card"
        set pattern "\\b([2-6]{1}\\d{3})[- ]?(\\d{4})[- ]?(\\d{2})[- ]?(\\d{2})[- ]?(\\d
{2,4})\\b"
        set verify "built-in"
        set look-back 20
        set transform "\\b\\1[- ]?\\2[- ]?\\3[- ]?\\4[- ]?\\5\\b"
    next
    edit "ssn-us"
        set pattern "\\b(\\d{3})-(\\d{2})-(\\d{4})\\b"
        set verify "(?<!-)\\b(?!666|000|9\\d{2})\\d{3}-(?!00)\\d{2}-(?!0{4})\\d{4}\\b
(?!-)"
        set look-back 12
        set transform "\\b\\1-\\2-\\3\\b"
    next
end
```

- Add DLP dictionary (`config dlp dictionary`), which is a collection of data type entries.

  ```
  config dlp dictionary
      edit <name>
          config entries
              edit 1
                  set type {credit-card | hex | keyword | regex | ssn-us}
                  set pattern <string>
                  set repeat {enable | disable}
                  set status {enable | disable}
              next
          end
      next
  end
  ```

- Add new DLP sensor (`config dlp sensor)`, which defines which dictionary to check. It counts the number of dictionary matches to trigger the sensor.

  ```
  config dlp sensor
      edit <name>
          set match-type {match-all | match-any | match-eval}
          set eval <string>
          config entries
              edit <id>
                  set dictionary <dlp_dictionary>
                  set count <integer>
                  set status {enable | disable}
              next
          end
      next
  end
  ```

- Rename `config dlp sensor` to `config dlp profile`. DLP profiles allow filtering by size and file type.

  ```
  config dlp profile
      edit <name>
          set feature-set {flow | proxy}
          config rule
              edit <id>
                  set proto <protocol> <protocol> ...
                  set sensor <dlp_sensor>
                  set action {allow | log-only | block | quarantine-ip}
              next
          end
      next
  end
  ```

- Allow DLP profiles to be applied in firewall policies.

To add a custom DLP data type:

```
config dlp data-type
    edit <name>
        set pattern <string>
        set verify <string>
        set transform <string>
    next
end
```

`pattern <string>`	Enter a regular expression pattern string without a look around.
`verify <string>`	Enter a regular expression pattern string used to verify the data type.
`transform <string>`	Enter the template to transform user input to a pattern using the capture group from `pattern`.

Example 1

This configuration will block HTTPS upload traffic that includes credit card or social security number (SSN) information. The pre-defined data types for `credit-card` and `ssn-us` are used in the dictionary.

To block HTTPS upload traffic that includes credit card or SSN information:

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "dic-case1-cc-ssn"
        config entries
            edit 1
                set type "credit-card"
            next
            edit 2
                set type "ssn-us"
            next
        end
    next
end
```

2. Configure the DLP sensor:

```
config dlp sensor
    edit "sensor-case1-cc-ssn"
        config entries
            edit 1
                set dictionary "dic-case1-cc-ssn"
            next
        end
    next
end
```

3. Configure the DLP profile:

```
config dlp profile
    edit "profile-case1-cc-ssn"
        config rule
            edit 1
                set proto http-post
                set sensor "sensor-case1-cc-ssn"
                set action block
            next
        end
    next
end
```

4. Add the DLP profile to a firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "custom-deep-inspection"
        set dlp-profile "profile-case1-cc-ssn"
        set logtraffic all
        set nat enable
    next
end
```

When a credit card or SSN is included in HTTP POST traffic, a replacement message appears because it is blocked. A DLP log is generated.

Sample log

```
5: date=2022-02-15 time=09:49:04 eventtime=1644947344512841971 tz="-0800" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" filteridx=1
dlpextra="sensor-case1-cc-ssn " filtertype="rule" filtercat="file" severity="medium"
policyid=1 poluuid="905fb604-7ed4-51ec-0853-79e498591bf8" policytype="policy" sessionid=9290
epoch=64494265 eventid=0 srcip=10.1.100.106 srcport=64006 srccountry="Reserved"
srcintf="port2" srcintfrole="undefined" srcuuid="358d0f56-7ed4-51ec-50f7-a5e4525a641d"
dstip=35.209.241.59 dstport=443 dstcountry="United States" dstintf="port1"
dstintfrole="undefined" dstuuid="358d0f56-7ed4-51ec-50f7-a5e4525a641d" proto=6
service="HTTPS" filetype="unknown" direction="outgoing" action="block"
hostname="dlptest.com" url="https://dlptest.com/https-post/" agent="Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KH" filename="item_meta[6]" filesize=19
profile="profile-case1-cc-ssn"
```

Example 2

This configuration will log FTP upload traffic with the following patterns:

- keyword = demo
- regex = demo(regex){1,5}
- hex = e6b58be8af95

The dictionary entries have repeat match enabled. The DLP sensor is set so this is repeated five times.

To log FTP upload traffic that has specific keyword, regex, and hex patterns repeated for five times:

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "dic-case2-keyword-regex-hex"
        config entries
            edit 1
                set type "keyword"
                set pattern "demo"
                set repeat enable
            next
            edit 2
                set type "regex"
                set pattern "demo(regex){1,5}"
                set repeat enable
            next
            edit 3
                set type "hex"
                set pattern "e6b58be8af95"
                set repeat enable
            next
        end
    next
end
```

2. Configure the DLP sensor:

```
config dlp sensor
    edit "sensor-case2-keyword-regex-hex"
        config entries
            edit 1
                set dictionary "dic-case2-keyword-regex-hex"
                set count 5
            next
        end
    next
end
```

3. Configure the DLP profile:

```
config dlp profile
    edit "profile-case2-keyword-regex-hex"
        config rule
            edit 1
                set proto ftp
                set sensor "sensor-case2-keyword-regex-hex"
                set action log-only
            next
        end
    next
end
```

4. Add the DLP profile to a firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
```

```
            set action accept
            set srcaddr "all"
            set dstaddr "all"
            set srcaddr6 "all"
            set dstaddr6 "all"
            set schedule "always"
            set service "ALL"
            set utm-status enable
            set inspection-mode proxy
            set ssl-ssh-profile "custom-deep-inspection"
            set dlp-profile "profile-case2-keyword-regex-hex"
            set logtraffic all
            set nat enable
        next
    end
```

5. Upload a Word document that contains "demo, demo, demo, demoregexregex," using FTP.

A DLP log is generated after the FTP traffic passes.

Sample log

```
3: date=2022-02-15 time=10:42:34 eventtime=1644950554735620032 tz="-0800" logid="0954024577"
type="utm" subtype="dlp" eventtype="dlp" level="notice" vd="root" filteridx=1
dlpextra="sensor-case2-keyword-regex-hex " filtertype="rule" filtercat="file"
severity="medium" policyid=1 poluuid="905fb604-7ed4-51ec-0853-79e498591bf8"
policytype="policy" sessionid=10551 epoch=64494633 eventid=0 srcip=10.1.100.106
srcport=55647 srccountry="Reserved" srcintf="port2" srcintfrole="undefined"
srcuuid="358d0f56-7ed4-51ec-50f7-a5e4525a641d" dstip=35.163.228.146 dstport=1048
dstcountry="United States" dstintf="port1" dstintfrole="undefined" dstuuid="358d0f56-7ed4-
51ec-50f7-a5e4525a641d" proto=6 service="FTP" filetype="msofficex" direction="outgoing"
action="log-only" filename="dlp-test.docx" filesize=11627 profile="profile-case2-keyword-
regex-hex" infectedfilename="word/document.xml" infectedfilesize=2448
infectedfiletype="html" infectedfilelevel=1
```

Example 3

This configuration will block HTTPS downloads of EXE files and log HTTPS downloads of files larger than 500 KB.

To block HTTPS download of EXE files and log downloads larger than 500 KB:

1. Configure the DLP file pattern:

```
config dlp filepattern
    edit 3
        set name "case3-exe"
        config entries
            edit "exe"
                set filter-type type
                set file-type exe
            next
        end
    next
end
```

2. Configure the DLP profile:

```
config dlp profile
    edit "profile-case3-type-size"
        config rule
            edit 1
                set proto http-get
                set filter-by none
                set file-type 3
                set action block
            next
            edit 2
                set proto http-get
                set filter-by none
                set file-size 500
                set action log-only
            next
        end
    next
end
```

3. Add the DLP profile to a firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "custom-deep-inspection"
        set dlp-profile "profile-case3-type-size"
        set logtraffic all
        set nat enable
    next
end
```

4. Download an EXE file using HTTPS. The download is blocked, a replacement message appears, and a DLP log is generated.

Sample log

```
1: date=2022-02-15 time=11:54:29 eventtime=1644954869682887856 tz="-0800" logid="0954024577"
type="utm" subtype="dlp" eventtype="dlp" level="notice" vd="root" filteridx=2 dlpextra="500
kB" filtertype="none" filtercat="file" severity="medium" policyid=1 poluuid="905fb604-7ed4-
51ec-0853-79e498591bf8" policytype="policy" sessionid=12082 epoch=901683674 eventid=0
srcip=10.1.100.18 srcport=59520 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="358d0f56-7ed4-51ec-50f7-a5e4525a641d" dstip=51.81.186.201
dstport=443 dstcountry="United States" dstintf="port1" dstintfrole="undefined"
dstuuid="358d0f56-7ed4-51ec-50f7-a5e4525a641d" proto=6 service="HTTPS" direction="incoming"
action="log-only" hostname="2.na.dl.wireshark.org"
```

```
url="https://2.na.dl.wireshark.org/win64/Wireshark-win64-3.6.2.exe" agent="curl/7.61.1"
filename="Wireshark-win64-3.6.2.exe" filesize=10502090 profile="profile-case3-type-size"
```

Add option to disable the FortiGuard IP address rating

An option has been added to disable using the FortiGuard IP address rating for SSL exemptions and proxy addresses.

To disable using the FortiGuard IP address rating for SSL exemptions:

```
config firewall ssl-ssh-profile
    edit <name>
        set ssl-exemption-ip-rating {enable | disable}
    next
end
```

To disable using the FortiGuard IP address rating for proxy addresses:

```
config firewall profile-protocol-options
    edit <name>
        config http
            set address-ip-rating {enable | disable}
        end
    next
end
```

The `ssl-exemption-ip-rating` and `address-ip-rating` options are enabled by default, so when both a website domain and its IP address return different categories after being rated by FortiGuard, the IP address category takes precedence when evaluating SSL exemptions associated with the SSL inspection profile and proxy addresses associated with the proxy protocol options profile. SSL exemptions and the `ssl-exemption-ip-rating` option work in both inspection modes (proxy and flow).

When the categories associated with the website domain and IP address are different, disabling the FortiGuard IP rating ensures that the FortiGuard domain category takes precedence when evaluating the preceding objects. For most websites, the domain category is valid when its IP address is unrated by FortiGuard. Since being unrated is considered as not having a category, the FortiGate uses the domain category as the website category.

A website might have an IP category that differs from its domain category. If they are different, the FortiGate uses the rating weight of the IP address or domain name to determine the rating result and decision. The rating weight is hard-coded in the FortiGate and depending on the relative category weights, the FortiGate may use the IP category instead of the website category. If the `ssl-exemption-ip-rating` option is disabled in the SSL inspection profile, then the FortiGate uses the domain category as the website category, which ensures SSL exemption operation as intended.

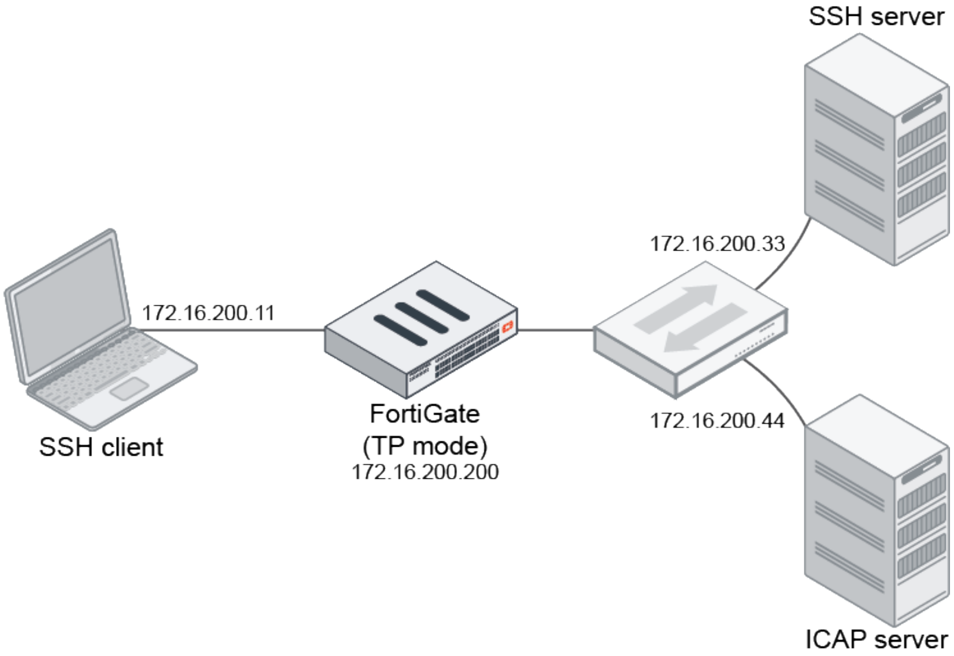
The `address-ip-rating` option in a proxy protocol options profile functions the same way as the `ssl-exemption-ip-rating` option. If the `address-ip-rating` option is disabled in a profile that is used in an explicit proxy policy that also uses a web filter profile, for HTTP or HTTPS traffic to a website that has different IP and domain categories and that matches the policy, the FortiGate will use the domain category when it evaluates categories for the web filter.

ICAP scanning with SCP and FTP

A FortiGate can forward files transferred by SCP and FTP to an ICAP server for further scanning. Previously, only HTTP and HTTPS were supported for ICAP forwarding.

Example

The FortiGate used in this example is operating in transparent mode. The SSH client, 172.16.200.11, sends a file named `today` to the SSH server at 172.16.200.33 using SCP. Since SCP transfers are encrypted inside an SSH tunnel, for the FortiGate to scan the traffic, deep inspection must be enabled in the SSL SSH profile.



To configure ICAP scanning with SCP:

1. Configure the ICAP server settings:

```
config icap server
    edit "icap_server1"
        set ip-address 172.16.200.44
    next
end
```

2. Configure the ICAP profile for SSH:

```
config icap profile
    edit "icap_profile1"
        set file-transfer ssh
        set file-transfer-server "icap_server1"
        set file-transfer-path "ssh_test"
    next
end
```

If the file transfer is over FTP, configure the profile as follows:

```
config icap profile
    edit "icap_profile1"
        set file-transfer ftp
        set streaming-content-bypass enable
        set file-transfer-server "icap_server1"
        set file-transfer-path "ftp_test"
    next
end
```

3. Configure the SSL SSH profile:

```
config firewall ssl-ssh-profile
    edit "protocols"
        config ssh
            set ports 22
            set status deep-inspection
        end
    next
end
```

4. Configure the firewall policy:

```
config firewall policy
    edit 1
        set name "ICAP"
        set srcintf "lan"
        set dstintf "mgmt"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "protocols"
        set icap-profile "icap_profile1"
    next
end
```

To test the configuration:

1. On a Linux client, copy a filed named `today` to the SSH server using SCP:

```
scp today fosqa@172.16.200.33:/home/fosqa/ssh_depot/
```

2. Capture a sniffer trace between the FortiGate and ICAP server, then verify the output from the ICAP protocol session.
   a. The client request and the file to be inspected:

```
Icap_client REQMOD:
172.016.200.200.13185-172.016.200.044.01344: REQMOD icap://172.16.200.44:1344/ssh_test ICAP/1.0
Host: 172.16.200.44:1344
```

```
X-Client-IP: 172.16.200.11
X-Server-IP: 172.16.200.33
X-Authenticated-User: TG9jYWw6Ly9hbm9ueW1vdXM=
X-Authenticated-Groups: TG9jYWw6Ly9sb2NhbGhvc3Qvbm8gYXV0aGVudGljYXRpb24=
User-Agent: FortiOS v7.2.0
Encapsulated: req-hdr=0, req-body=116

PUT /scp/today HTTP/1.1
Host: 172.16.200.11
Content-Type: application/octet-stream
Transfer-Encoding: chunked

1d
Tue Sep 20 04:01:50 UTC 2022
```

Where:

- `X-Client-IP` = the client sending the file
- `X-Server-IP` = the server receiving the file
- `Tue Sep 20 04:01:50 UTC 2022` = the content of the file, which is in clear text after the FortiGate performs deep inspection

b. The ICAP server response that the file is cleared and allowed to pass without modifications:

```
Icap-server reply:
172.016.200.044.01344-172.016.200.200.13185: ICAP/1.0 200 OK
ISTag: "GreasySpoon-1.0.7-b03"
Host: 0.0.0.0:1344
Encapsulated: req-hdr=0, req-body=136
Connection: keep-alive

PUT /scp/today HTTP/1.1
Host: 172.16.200.11
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Content-Length: 29

1d
Tue Sep 20 04:01:50 UTC 2022
```

3. On a Linux client, copy the file from the server locally using SCP:

```
scp fosqa@172.16.200.33:/home/fosqa/ssh_depot/today2/
```

4. Similar outputs are observed. The ICAP client request indicates that the file is copied from the SSH server:

```
PUT /scp/today2 HTTP/1.1
Host: 172.16.200.33
```

Add persistency for banned IP list - 7.2.1

The `banned-ip-persistency` option configures whether the banned IP list persists through a power cycle.

```
config firewall global
    set banned-ip-persistency {disabled | permanent-only | all}
end
```

`banned-ip-persistency {disabled | permanent-only | all}`	Set the persistency of banned IPs across power cycling: • `disabled`: no entries are kept across power cycling (default). • `permanent-only`: only permanent IP bans are kept across power cycling. • `all`: all IP bans are kept across power cycling.

The banned IP list is created from quarantining. For example, when quarantining is enabled for IPS, application control, and DDoS. Permanent quarantining can be added manually using `diagnose user banned-ip add src4`.

The `diagnose user quarantine <parameter>` command has changed to `diagnose user banned-ip <parameter>`.

Example 1: keep all banned IPs across power cycling

When `banned-ip-persistency` is set to `all`, all the banned IPs are saved after a reboot. In this example, an application control security profile with quarantining is already configured. After traffic is generated that triggers the quarantine rule, a quarantine list is generated.

To view the list of banned IPs:

```
# diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
10.1.100.12       Tue Jul  5 18:01:05 2022 Tue Jul  5 18:21:05 2022 APP
```

After a reboot, the banned IP list is the same:

```
# diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
10.1.100.12       Tue Jul  5 18:01:05 2022 Tue Jul  5 18:21:05 2022 APP
```

Example 2: keep only permanent banned IPs across power cycling

When `banned-ip-persistency` is set to `permanent-only`, only banned IPs with an indefinite expiry time are saved after a reboot. The permanent IP ban was already configured for 10.1.100.11 using `diagnose user banned-ip add src4 10.1.100.11 0 ips`.

To view the list of banned IPs:

```
# diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
10.1.100.12       Tue Jul  5 18:01:05 2022 Tue Jul  5 18:21:05 2022 APP
10.1.100.11       Tue Jul  5 18:06:35 2022 indefinite               IPS
```

After a reboot, only 10.1.100.11 remains in the banned IP list:

```
# diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
10.1.100.11       Tue Jul  5 18:06:35 2022 indefinite               IPS
```

Reduce memory usage on FortiGate models with 2 GB RAM or less by not running WAD processes for unused proxy features - 7.2.1

Certain unused WAD proxy processes are not started by default on FortiGate models with 2 GB of RAM or less to reduce memory usage. These process will only start when relevant proxy features are configured, such as explicit proxies, transparent proxies, or ZTNA.

Allow the YouTube channel override action to take precedence - 7.2.1

In a video filter profile, when the FortiGuard category-based filter and YouTube channel override are used together, by default a video will be blocked if it matches either category or YouTube channel and the action is set to block. This enhancement enables the channel action to override the category action. A category can be blocked, but certain channels in that category can be allowed when the `override-category` option is enabled.

For more information about this feature, see Allow the YouTube channel override action to take precedence.

Add REST API for IPS session monitoring - 7.2.4

The `/api/v2/monitor/ips/session/performance` REST API can be used to query the FortiGate for its IPS session information. This API retrieves the output of `diagnose ips session performance`, and it can provide the `diagnose ips session` information to FortiManager.

To use the API with a browser:

1. Open the browser and enter `https://<FortiGate_IP_address>/api/v2/monitor/ips/session/performance`. A token is not required.
2. The browser displays the output similar to the following:

```
{
  "http_method":"GET",
  "results":[
    {
      "pid":7093,
      "memory":129460224,
      "cycles":{
        "decoder":2613,
        "session":1025,
        "protocol":31526,
        "application":2283463,
        "match":30993,
        "nc_match":2180,
        "cross_tag":18637
      },
      "packets":{
        "decoder":74,
        "session":74,
        "protocol":74,
        "application":74,
        "match":4,
        "nc_match":98,
        "cross_tag":4
      }
    }
  ],
  "vdom":"vd1",
  "path":"ips",
  "name":"session",
  "action":"performance",
  "status":"success",
  "serial":"FG1K5D3I13800000",
  "version":"v7.2.2",
  "build":1319
}
```

To use the API with a Postman REST client or web client:

1. Configure the REST API administrator and generate the token (see REST API administrator in the FortiOS Administration Guide for more details).
2. Create a new request in the client for the HTTP method, GET, and enter the URL (`https://<FortiGate_IP_address>/api/v2/monitor/ips/session/performance?access_token=<token>`).
3. The client displays the output similar to the following:

```
{
  "http_method":"GET",
  "results":[
    {
      "pid":7475,
      "memory":127750680,
      "cycles":{
        "decoder":1922,
        "session":789,
        "protocol":3692,
        "application":907777,
        "match":4997,
        "nc_match":8029,
        "cross_tag":0
      },
      "packets":{
        "decoder":252,
        "session":252,
        "protocol":252,
        "application":205,
        "match":5,
        "nc_match":16,
        "cross_tag":0
      }
    }
  ],
  "vdom":"vd1",
  "path":"ips",
  "name":"session",
  "action":"performance",
  "status":"success",
  "serial":"FG1K5D3I13800000",
  "version":"v7.2.2",
  "build":1319
}
```

To use a VDOM parameter in the API:

1. Enter the URL in the browser or client, `https://<FortiGate_IP_address>/api/v2/monitor/ips/session/performance?vdom=root`. This example will only retrieve performance information under the root VDOM.
2. Output is displayed similar to the following:

```
{
  "http_method":"GET",
  "results":[
    {
      "pid":7093,
      "memory":129461024,
      "cycles":{
        "decoder":2511,
        "session":1058,
        "protocol":61812,
        "application":861188,
        "match":8927,
        "nc_match":1917,
        "cross_tag":16281
      },
      "packets":{
        "decoder":268,
        "session":268,
        "protocol":268,
        "application":258,
        "match":44,
        "nc_match":440,
        "cross_tag":38
      }
    }
  ],
  "vdom":"root",
  "path":"ips",
  "name":"session",
  "action":"performance",
  "status":"success",
  "serial":"FG1K5D3I13800000",
  "version":"v7.2.2",
  "build":1319
}
```

Hide proxy features in the GUI by default for models with 2 GB RAM or less - 7.2.4

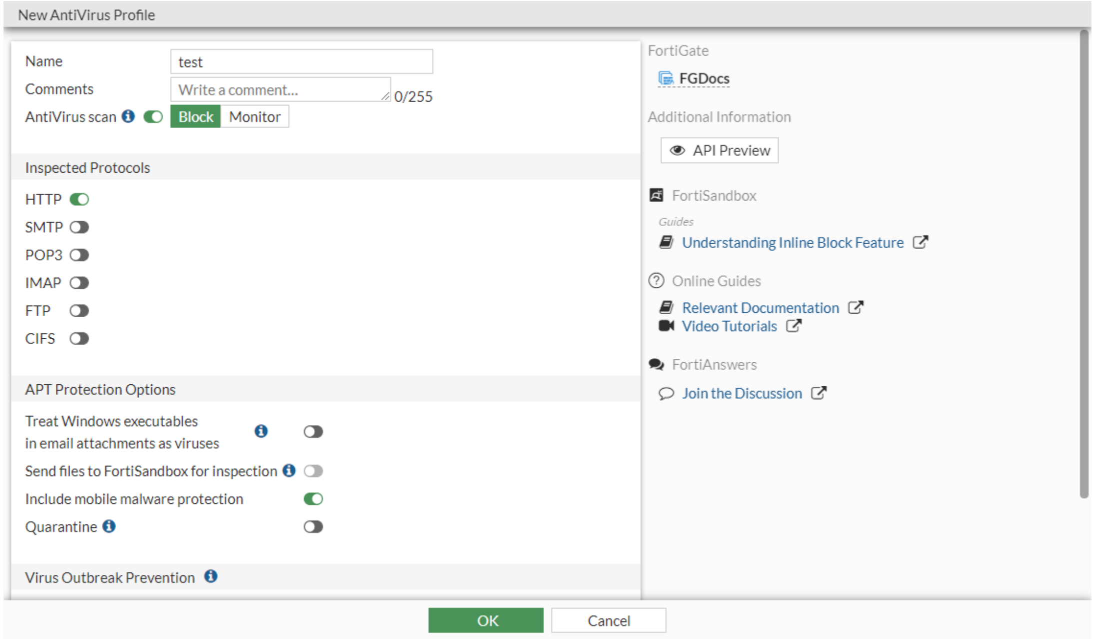
This information is also available in the FortiOS 7.2 Administration Guide:

- Proxy feature visibility in the GUI for entry-level models

This enhancement introduces the `gui-proxy-inspection` setting under `config system settings`, which is enabled on most models except for entry-level platforms with 2 GB of RAM or less. When this setting is disabled:

- Proxy-based only profiles such as *ICAP*, *Web Application Firewall*, *Video Filter*, and *Zero Trust Network Access* are disabled (grayed out) on the *System* > *Feature Visibility* page.
- The *Feature set* field is disabled on UTM profiles. Only flow-based features are shown.

  Example AV profile:



New AntiVirus Profile

Name: test
Comments: Write a comment... 0/255
AntiVirus scan: ● Block | Monitor

Inspected Protocols

HTTP ●
SMTP ○
POP3 ○
IMAP ○
FTP ○
CIFS ○

APT Protection Options

Treat Windows executables in email attachments as viruses ○
Send files to FortiSandbox for inspection ○
Include mobile malware protection ●
Quarantine ○

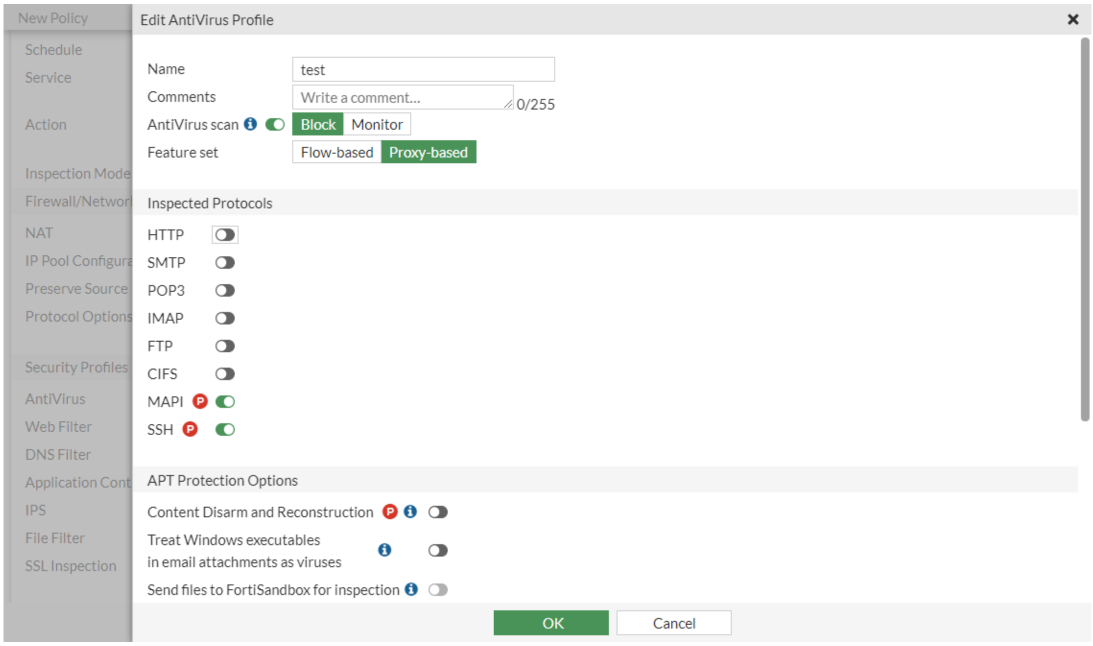
Virus Outbreak Prevention

- Firewall policy pages do not have option to select a *Flow-based* or *Proxy-based* inspection mode.
- Proxy-based UTM profiles cannot be selected within policy configurations or other areas.

Note the following exceptions:

- If the proxy feature set is enabled from the CLI or carried over from upgrading, it can be displayed in the GUI.
- If proxy-based inspection mode is enabled from the CLI or carried over from upgrading, it can be displayed in GUI firewall policy pages.

Example AV profile being edited from the *New Policy* page after upgrading:



Name: test

Comments: Write a comment... 0/255

AntiVirus scan: Block | Monitor

Feature set: Flow-based | Proxy-based

Inspected Protocols

HTTP
SMTP
POP3
IMAP
FTP
CIFS
MAPI
SSH

APT Protection Options

Content Disarm and Reconstruction

Treat Windows executables in email attachments as viruses

Send files to FortiSandbox for inspection

To enable proxy features on entry-level platforms:

```
config system settings
    set gui-proxy-inspection enable
end
```

Re-introduce DLP profiles in the GUI - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Basic DLP settings

The DLP profile is re-introduced in the GUI on the *Security Profiles > Data Leak Prevention* page. Users can configure DLP settings within the *Profiles*, *Sensors*, and *Dictionaries* tabs. DLP profiles can be added to proxy-based firewall policies and proxy policies. DLP profiles cannot be added to flow-based firewall policies and one-arm sniffers.

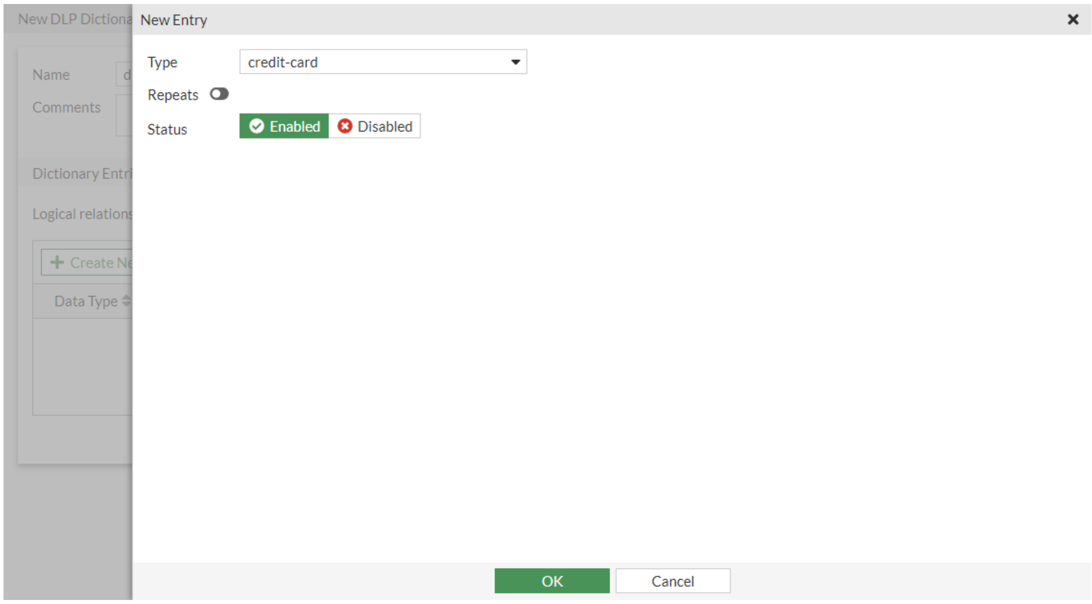
If *Data Leak Prevention* is not visible in the tree menu, go to *System > Feature Visibility* and enable it.

Example 1

This configuration will block HTTPS upload traffic that includes credit card information. The pre-defined data type for credit card is used in the dictionary.

To block HTTPS upload traffic that includes credit card information:

1. Configure the DLP dictionary:
   a. Go to *Security Profiles > Data Leak Prevention*, select the *Dictionaries* tab, and click *Create New*.
   b. Enter a name (*dic-case1*).
   c. In the *Dictionary Entries* section, click *Create New*.
   d. Set the *Type* to *credit-card* and click *OK*.



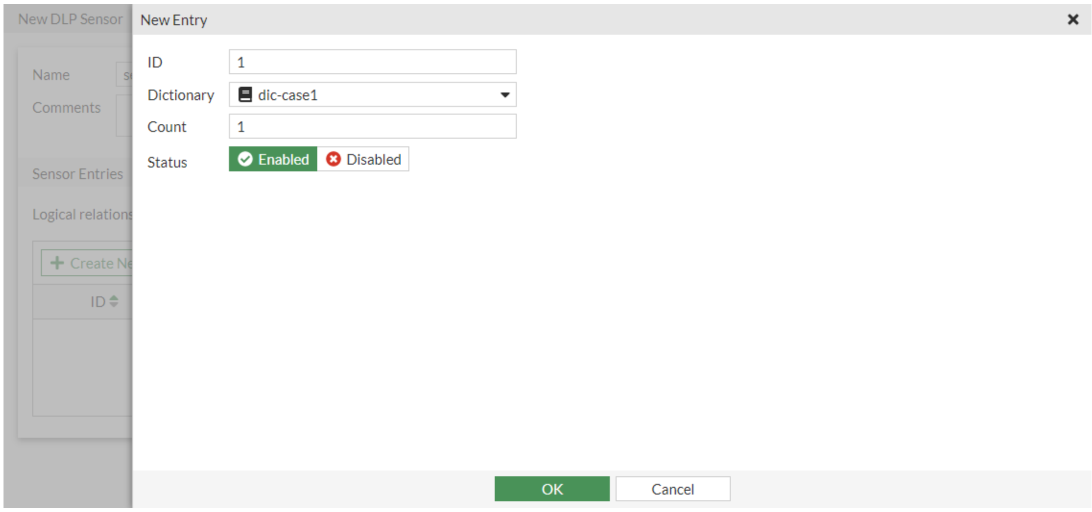
New Entry

Type: credit-card

Repeats

Status: Enabled

   e. Click *OK* to save the dictionary.
2. Configure the DLP sensor:
   a. Go to *Security Profiles > Data Leak Prevention*, select the *Sensors* tab, and click *Create New*.
   b. Enter a name (*sensor-case1*).
   c. In the *Sensor Entries* section, click *Create New*.
   d. Set the *Dictionary* to *dic-case1* and click *OK*.



New Entry

ID: 1

Dictionary: dic-case1

Count: 1

Status: Enabled

   e. Click *OK* to save the sensor.
3. Configure the DLP profile:

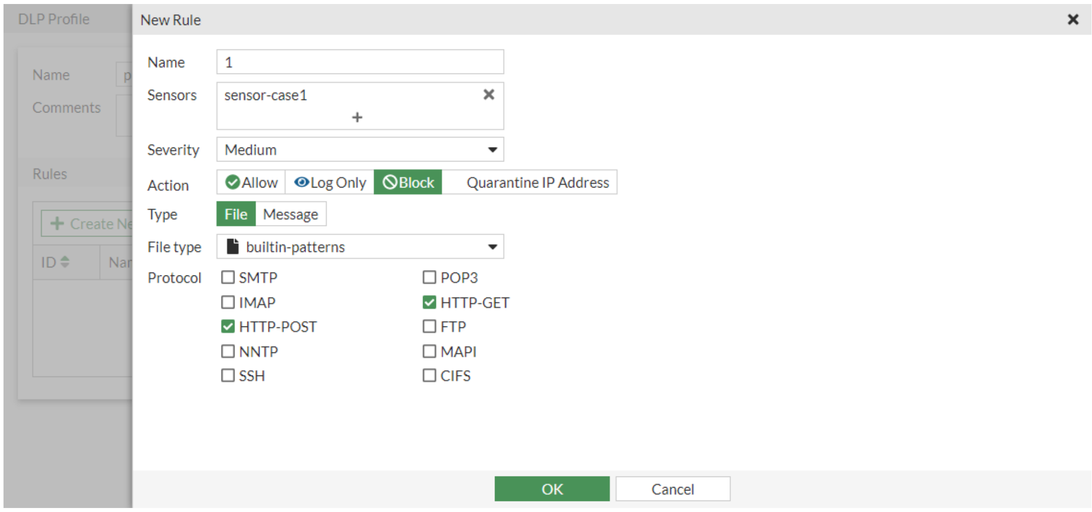
a. Go to *Security Profiles > Data Leak Prevention*, select the *Profiles* tab, and click *Create New*.

b. Enter a name (*profile-case1*).

c. In the *Rules* section, click *Create New*.

d. Configure the following settings:

Name	*1*
Sensors	*sensor-case1*
Severity	*Medium*
Action	*Block*
Type	*File*
File type	*builtin-patterns*
Protocol	*HTTP-POST*, *HTTP-GET*



Name: 1

Sensors: sensor-case1 ×
+

Severity: Medium

Action: Allow | Log Only | ● Block | Quarantine IP Address

Type: ● File | Message

File type: builtin-patterns

Protocol:
□ SMTP ☐ POP3
□ IMAP ☑ HTTP-GET
☑ HTTP-POST □ FTP
□ NNTP □ MAPI
□ SSH □ CIFS

e. Click *OK*.

f. Click *OK* to save the profile.

4. Add the DLP profile to a firewall policy:

a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.

b. Set the *Inspection Mode* to *Proxy-based*.

c. In the *Security Profiles* section, enable *DLP Profile* and select *profile-case1*.

d. Configure the other settings as needed.

e. Click *OK*.

When a credit card is included in HTTP POST traffic, the file is blocked and a DLP log is generated.

Sample log

```
1: date=2022-10-26 time=11:25:01 eventtime=1666808700281057923 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" filteridx=1
filtername="1" dlpextra="builtin-patterns;sensor-case1" filtertype="sensor" filtercat="file"
severity="medium" policyid=1 poluuid="891a526a-51cd-51ed-577a-6505bec88af9"
policytype="policy" sessionid=3905 epoch=2143297701 eventid=0 srcip=10.1.100.11
srcport=40370 srccountry="Reserved" srcintf="port2" srcintfrole="undefined"
```

```
srcuuid="502d2c8e-51cd-51ed-a24e-a091f4ff6fed" dstip=172.16.200.55 dstport=443
dstcountry="Reserved" dstintf="port1" dstintfrole="undefined" dstuuid="502d2c8e-51cd-51ed-
a24e-a091f4ff6fed" proto=6 service="HTTPS" filetype="msoffice" direction="outgoing"
action="block" hostname="172.16.200.55" url="https://172.16.200.55/cgi-bin/upload.pl"
agent="curl/7.58.0" httpmethod="POST" filename="credit_card.doc" filesize=22016
profile="profile-case1"
```

Example 2

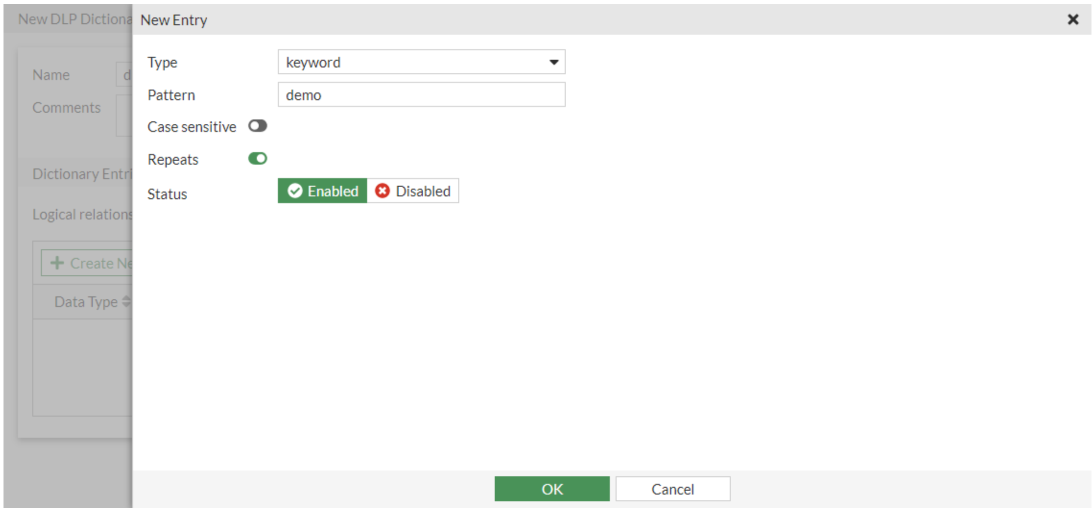
This configuration will log FTP upload traffic with the following patterns:

- keyword = demo
- regex = demo(regex){1,5}
- hex = e6b58be8af95

The dictionary entries have repeat match enabled. The DLP sensor is set so this is repeated five times.

To log FTP upload traffic that has specific keyword, regex, and hex patterns repeated for five times:

1. Configure the DLP dictionary with three entries:
   a. Go to *Security Profiles > Data Leak Prevention*, select the *Dictionaries* tab, and click *Create New*.
   b. Enter a name (*dic-case2*).
   c. In the *Dictionary Entries* section, click *Create New*.
   d. Set the *Type* to *keyword* and the *Pattern* to *demo*.
   e. Enable *Repeats* and click *OK*.



New Entry

Type: keyword

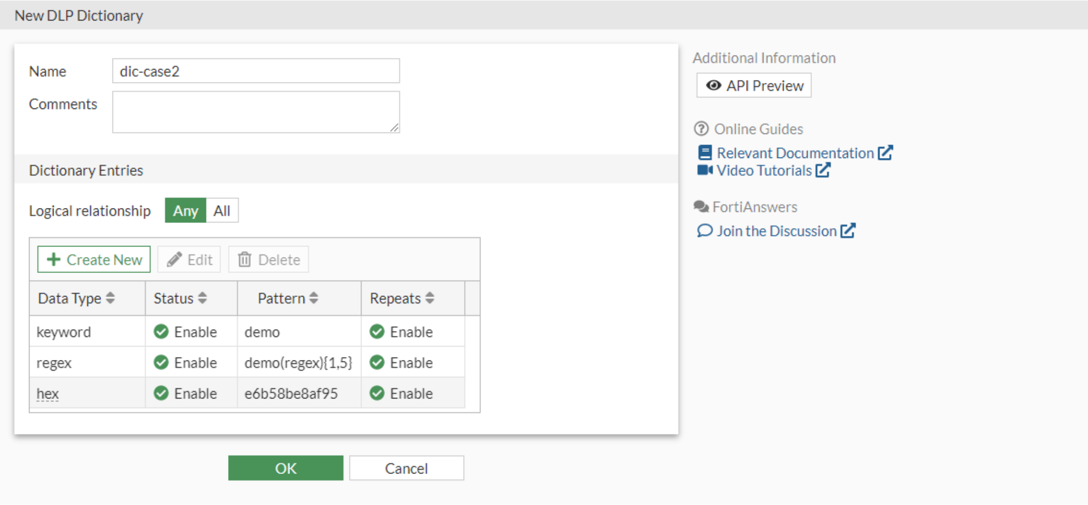
Pattern: demo

Case sensitive: off

Repeats: on

Status: Enabled

   f. Repeat these steps to add dictionary entries for the following (with *Repeats* enabled):
      i. Set the *Type* to *regex* and the *Pattern* to *demo(regex){1,5}*.
      ii. Set the *Type* to *hex* and the *Pattern* to *e6b58be8af95*.



New DLP Dictionary

Name: dic-case2

Comments:

Dictionary Entries

Logical relationship: Any | All

Data Type	Status	Pattern	Repeats
keyword	✓ Enable	demo	✓ Enable
regex	✓ Enable	demo(regex){1,5}	✓ Enable
hex	✓ Enable	e6b58be8af95	✓ Enable

g. Click *OK* to save the dictionary.

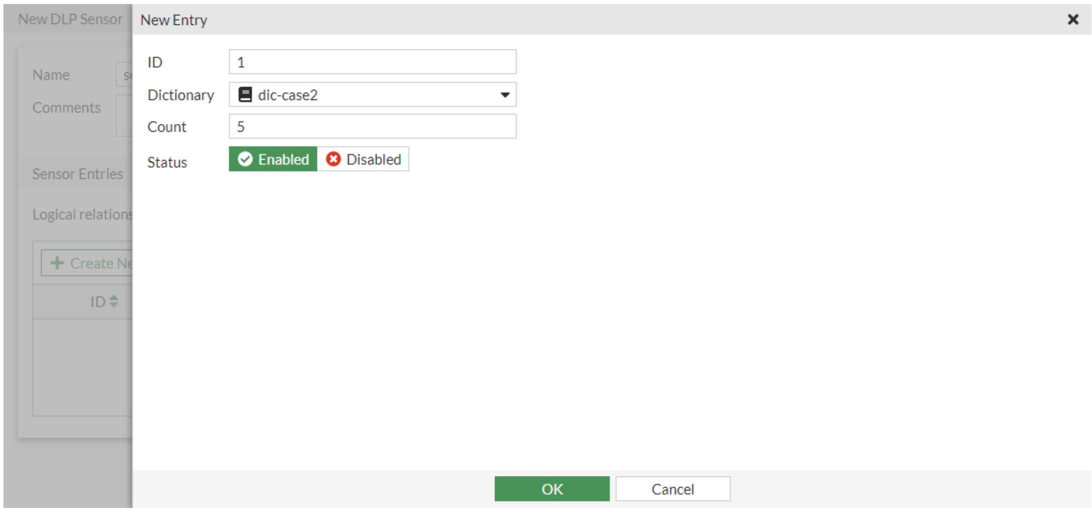
2. Configure the DLP sensor:

   a. Go to *Security Profiles > Data Leak Prevention*, select the *Sensors* tab, and click *Create New*.

   b. Enter a name (*sensor-case2*).

   c. In the *Sensor Entries* section, click *Create New*.

   d. Set the *Dictionary* to *dic-case2*, set the *Count* to *5*, and click *OK*.



New Entry

ID: 1

Dictionary: dic-case2

Count: 5

Status: Enabled | Disabled

   e. Click *OK* to save the sensor.

3. Configure the DLP profile:

   a. Go to *Security Profiles > Data Leak Prevention*, select the *Profiles* tab, and click *Create New*.

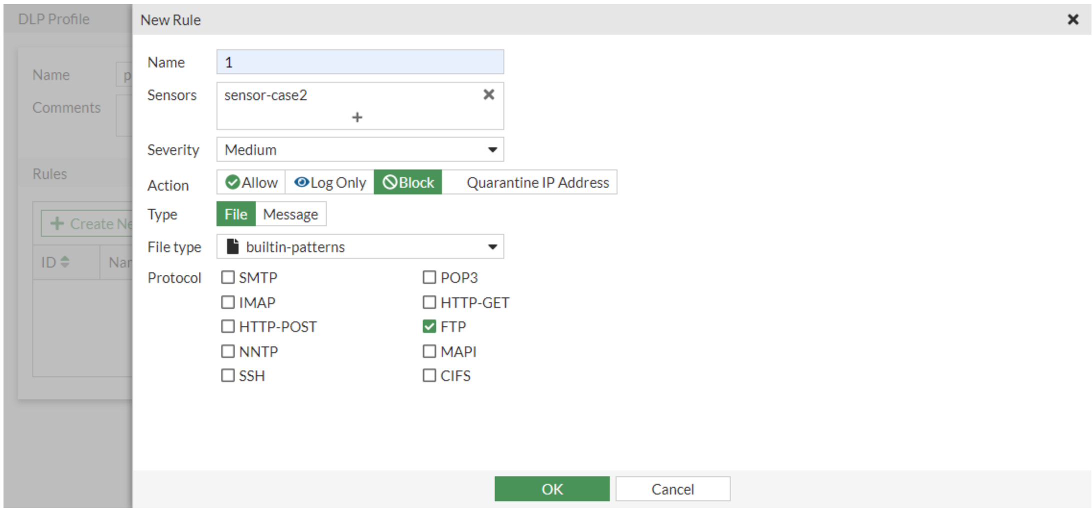
   b. Enter a name (*profile-case2*).

   c. In the *Rules* section, click *Create New*.

   d. Configure the following settings:

Name	*1*
Sensors	*sensor-case2*

Severity	*Medium*
Action	*Block*
Type	*File*
File type	*builtin-patterns*
Protocol	*FTP*



Name: 1
Sensors: sensor-case2
Severity: Medium
Action: ○ Allow ○ Log Only ● Block ○ Quarantine IP Address
Type: ● File ○ Message
File type: builtin-patterns
Protocol:
□ SMTP □ POP3
□ IMAP □ HTTP-GET
□ HTTP-POST ☑ FTP
□ NNTP □ MAPI
□ SSH □ CIFS

   e. Click *OK*.
   f. Click *OK* to save the profile.
4. Add the DLP profile to a firewall policy:
   a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
   b. Set the *Inspection Mode* to *Proxy-based*.
   c. In the *Security Profiles* section, enable *DLP Profile* and select *profile-case2*.
   d. Configure the other settings as needed.
   e. Click *OK*.
5. Upload a Word document that contains "demo, demo, demo, demoregexregex," using FTP.

   A DLP log is generated after the FTP traffic passes.

Sample log

```
1: date=2022-10-26 time=12:37:57 eventtime=1666813077679725858 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" filteridx=1
filtername="1" dlpextra="builtin-patterns;sensor-case2" filtertype="sensor" filtercat="file"
severity="medium" policyid=1 poluuid="891a526a-51cd-51ed-577a-6505bec88af9"
policytype="policy" sessionid=6267 epoch=909159520 eventid=0 srcip=10.1.100.11 srcport=52858
srccountry="Reserved" srcintf="port2" srcintfrole="undefined" srcuuid="502d2c8e-51cd-51ed-
a24e-a091f4ff6fed" dstip=172.16.200.55 dstport=43411 dstcountry="Reserved" dstintf="port1"
dstintfrole="undefined" dstuuid="502d2c8e-51cd-51ed-a24e-a091f4ff6fed" proto=6 service="FTP"
filetype="msoffice" direction="outgoing" action="block" filename="realizedDoc.doc"
filesize=26624 profile="profile-case2"
```

Remove option to block QUIC by default in application control - 7.2.4

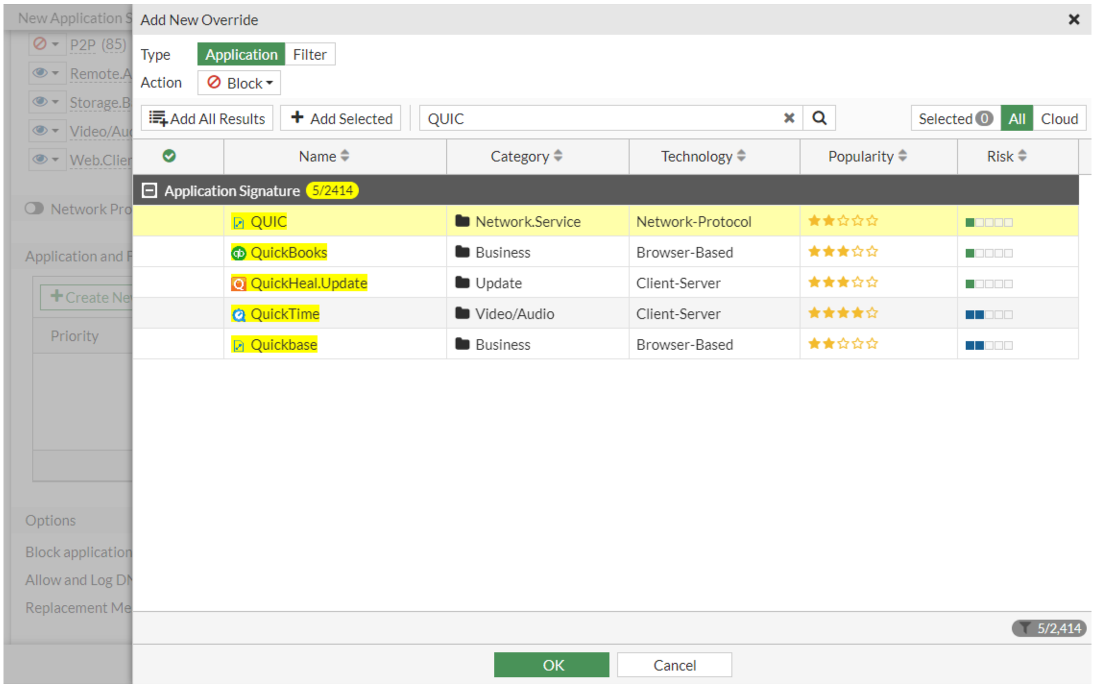
This information is also available in the FortiOS 7.2 Administration Guide:

- Blocking QUIC manually

Blocking QUIC by default in the application control profile is no longer necessary since HTTP3 over QUIC is fully supported by FortiOS. The `allow-quic` option has been removed from the application control profile (`config application list`) settings. The *QUIC* option has been removed from the *Application Sensor* configuration page in the GUI. Users can still select the QUIC application signature (40169) to manually block QUIC.

To block the QUIC application signature in the GUI:

1. Go to *Security Profiles > Application Control* and click *Create New*.
2. Enter a name (*test*).
3. Add a filter override for the QUIC application signature:
   a. In the *Application and Filter Overrides* section, click *Create New*. The *Add New Override* pane appears.
   b. In the search box, enter *QUIC* and press `Enter`.
   c. Select the *QUIC* entry and click *Add Selected*.



Type: Application | Filter

Action: Block

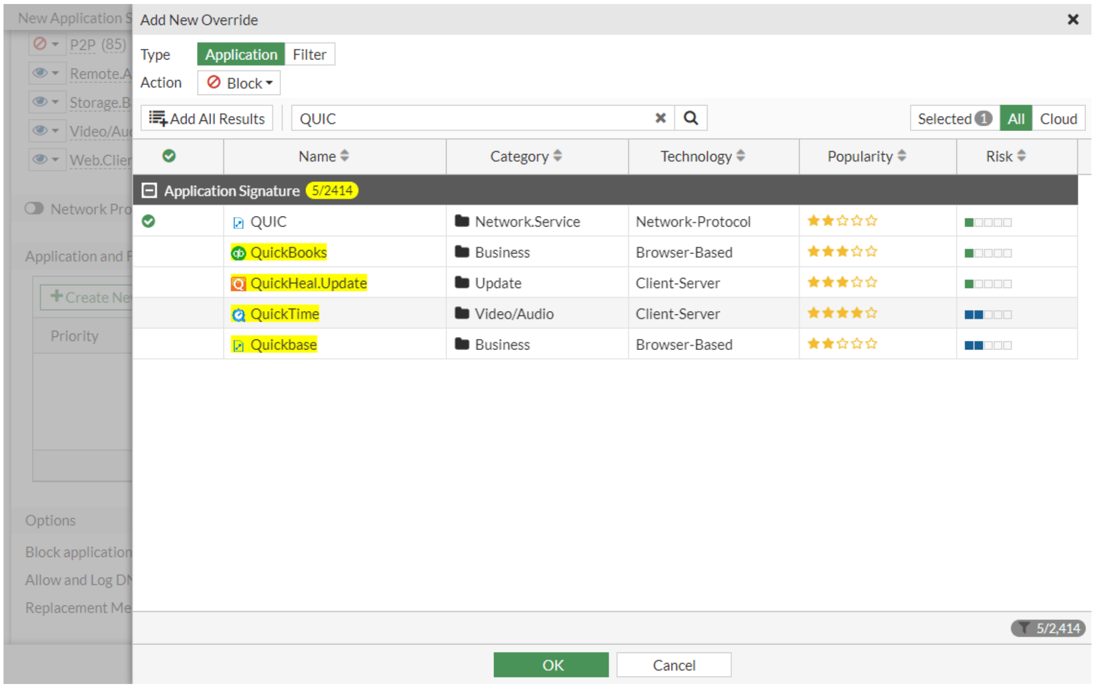
Search: QUIC

Application Signature 5/2414

Name	Category	Technology	Popularity	Risk
QUIC	Network.Service	Network-Protocol	★★☆☆☆	■□□□□
QuickBooks	Business	Browser-Based	★★★☆☆	■□□□□
QuickHeal.Update	Update	Client-Server	★★★☆☆	■□□□□
QuickTime	Video/Audio	Client-Server	★★★★☆	■■□□□
Quickbase	Business	Browser-Based	★★☆☆☆	■■□□□

5/2,414

d. Click *OK*.



Add New Override

Type: Application | Filter

Action: Block

Add All Results | QUIC | Selected 1 | All | Cloud

	Name	Category	Technology	Popularity	Risk
Application Signature 5/2414					
✓	QUIC	Network.Service	Network-Protocol	★★☆☆☆	■□□□□
	QuickBooks	Business	Browser-Based	★★★☆☆	■□□□□
	QuickHeal.Update	Update	Client-Server	★★★☆☆	■□□□□
	QuickTime	Video/Audio	Client-Server	★★★★☆	■■□□□
	Quickbase	Business	Browser-Based	★★☆☆☆	■■□□□

5/2,414

OK | Cancel

4. Configure the other sensor settings as needed.
5. Click *OK*.

To block the QUIC application signature in the CLI:

```
config application list
    edit "test"
        set other-application-log enable
        config entries
            edit 1
                set application 40169
                set action block
                set log enable
            next
        end
    next
end
```

Sample traffic log

```
1: date=2022-11-01 time=18:45:48 eventtime=1667353547840005082 tz="-0700" logid="0000000013"
type="traffic" subtype="forward" level="notice" vd="vd1" srcip=10.1.100.141 srcport=60268
srcintf="port2" srcintfrole="undefined" dstip=142.250.217.98 dstport=443 dstintf="port1"
dstintfrole="undefined" srccountry="Reserved" dstcountry="United States" sessionid=2978
proto=17 action="accept" policyid=1 policytype="policy" poluuid="72a572a8-5a33-51ed-fa85-
db33d77e4804" policyname="test" service="udp/443" trandisp="snat" transip=172.16.200.1
transport=60268 appid=40169 app="QUIC" appcat="Network.Service" apprisk="low" applist="test"
appact="drop-session" duration=183 sentbyte=6390 rcvdbyte=0 sentpkt=5 rcvdpkt=0
utmaction="block" countapp=5 utmref=65535-1102
```

Improve replacement message displayed in blocked videos - 7.2.5

This information is also available in the FortiOS 7.2 Administration Guide:

- Replacement messages displayed in blocked videos

This enhancement improves how a replacement message is displayed for YouTube videos blocked by video filtering. When a user visits a video directly by a URL, a full page replacement message is displayed. When a user loads a video from the YouTube website (homepage or recommended videos), the page loads and the replacement message is displayed in the video frame.

For more information about this feature, see Improve replacement message displayed in blocked videos.

Introduce SIP IPS profile as a complement to SIP ALG - 7.2.5

This information is also available in the FortiOS 7.2 Administration Guide:

- SIP message inspection and filtering

In FortiOS 7.0, flow-based SIP inspection was introduced, which is handled by the IPS Engine. When a VoIP profile is applied to a firewall policy, the inspection mode determines whether SIP ALG or flow-based SIP is used. Therefore, SIP ALG and flow-based SIP were mutually exclusive. You could not use both at the same time.

Proxy-based SIP ALG is able to handle features such as pin hole creation and NAT that flow-based SIP inspection cannot. Flow-based SIP can handle features such as MSRP decoding and scanning that proxy-based SIP ALG cannot.

To solve this problem, FortiOS 7.2.5 introduces a new IPS-based VoIP profile (`ips-voip-filter`) that allows flow-based SIP to complement SIP ALG while working together.

The VoIP profile selection within a firewall policy is restored to pre-7.0 behavior. The `voip-profile` can be selected regardless of the `inspection-mode` in the firewall policy.

For more information about this feature, see Introduce SIP IPS profile as a complement to SIP ALG.

VPN

This section includes information about VPN related new features:

- IPsec and SSL VPN on page 434

IPsec and SSL VPN

This section includes information about IPsec and SSL VPN related new features:

- Add log field to identify ADVPN shortcuts in VPN logs on page 434
- Show the SSL VPN portal login page in the browser's language on page 435
- SLA link monitoring for dynamic IPsec and SSL VPN tunnels on page 437
- IPsec IKE load balancing based on FortiSASE account information 7.2.5 on page 440
- Securely exchange serial numbers between FortiGates connected with IPsec VPN 7.2.6 on page 440

Add log field to identify ADVPN shortcuts in VPN logs

The `advpnsc` log field in VPN event logs indicates that a VPN event is based on an ADVPN shortcut. A value of `1` indicates the tunnel is an ADVPN shortcut, and `0` indicates it is not.

Sample log

```
# execute log filter field advpnsc 1
# execute log display
35 logs found.
10 logs returned.
1: date=2022-01-05 time=11:37:15 eventtime=1641411435027292611 tz="-0800" logid="0101037138"
type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec connection status
changed" msg="IPsec connection status change" action="tunnel-up" remip=172.16.106.46
locip=192.168.15.3 remport=64916 locport=4500 outintf="port1"
cookies="6ac548129ad085a6/9fb073b8e796e30b" user="C = US, ST = California, L = Sunnyvale, O
= Fortinet, OU = FortiGate, CN = FGVMSLTM20003739, emailAddress = support@fortinet.com"
group="N/A" useralt="C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate,
CN = FGVMSLTM20003739, emailAddress = support@fortinet.com" xauthuser="N/A" xauthgroup="N/A"
assignip=N/A vpntunnel="_OCVPN3-0a_0" tunnelip=0.0.0.0 tunnelid=724776109 tunneltype="ipsec"
duration=0 sentbyte=0 rcvdbyte=0 nextstat=0 advpnsc=1
```

This sample log is based on the following hub and spoke VPN configuration:

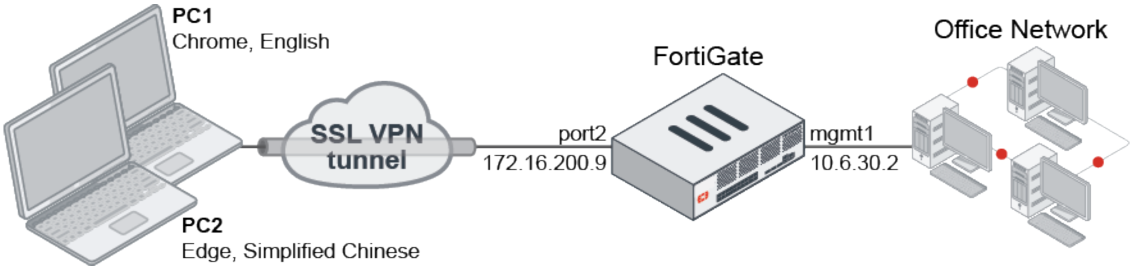
```
# diagnose vpn tunnel list
...
name=_OCVPN3-0a_0 ver=2 serial=c 192.168.15.3:4500->172.16.106.46:64916 tun_id=172.16.106.46
tun_id6=::172.16.106.46 dst_mtu=1500 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/976 options[03d0]=create_dev
no-sysctl rgwy-chg rport-chg frag-rfc accept_traffic=1 overlay_id=1
parent=_OCVPN3-0a index=0
```

```
proxyid_num=1 child_num=0 refcnt=6 ilast=9 olast=9 ad=r/2
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=0 interval=10 remote_port=64916
proxyid=_OCVPN3-0a proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=1a203 type=00 soft=0 mtu=1422 expire=43176/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43186/43200
  dec: spi=42f2d4c4 esp=aes key=16 84cbc50be871a5bbde4688621ae92101
       ah=sha1 key=20 5543e35e1cfe3cd59d9a5e3660adfe9d69e03ebb
  enc: spi=aceda538 esp=aes key=16 a0aa39ceadbaa5ef96644371bd39b5c7
       ah=sha1 key=20 c7dee396faa14ff2791bef8591ac82938f2e93fe
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Show the SSL VPN portal login page in the browser's language

By default, the browser's language preference is automatically detected and used by the SSL VPN portal login page. The system language can still be used by changing the settings on the SSL-VPN Settings page of the GUI, or disabling browser-language detection in the CLI:

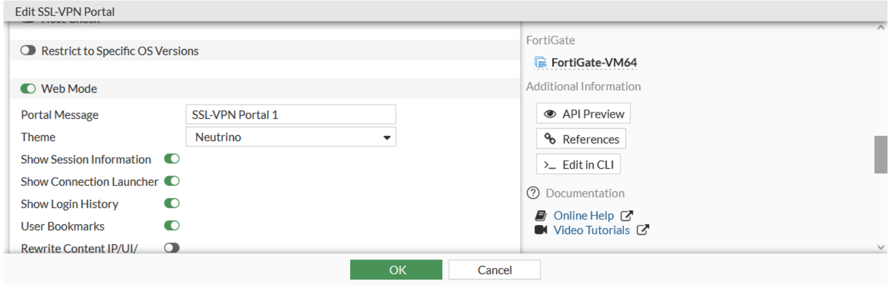
```
config vpn ssl settings
    set browser-language-detection disable
end
```



In this example, the *sslvpnadmin* user account is used for SSL VPN connections on the *testportal1* SSL VPN portal. The account is shared by users from different countries that use different browsers and different languages in their browsers. The user on PC1 uses Chrome in English, and the user on PC2 uses Edge in Simplified Chinese. When a user logs in to the SSL VPN web portal, all of the pages are shown in the same language as their browser.

To configure the SSL VPN portal to use the client's browser language:

1. Configure the SSL VPN portal:
   a. Go to *VPN* > *SSL-VPN Portals* and edit the SSL VPN portal.
      For information about configuring SSL VPN portals, see SSL VPN in the FortiOS Administration Guide.
   b. Enable *Web Mode*.



Edit SSL-VPN Portal

○ Restrict to Specific OS Versions

● Web Mode

Portal Message: SSL-VPN Portal 1

Theme: Neutrino

Show Session Information ●

Show Connection Launcher ●

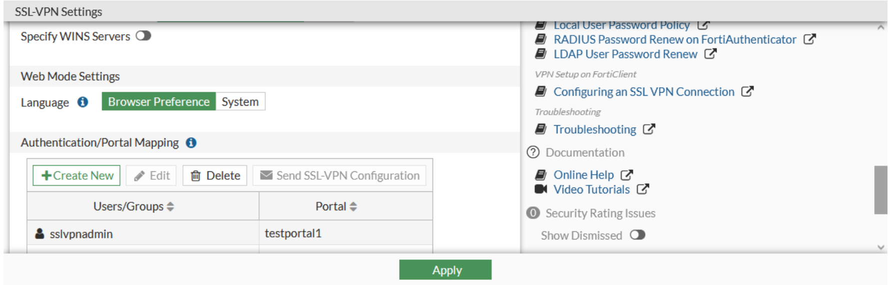
Show Login History ●

User Bookmarks ●

Rewrite Content IP/UI/ ○

   c. Click *OK*.

2. Set the language preference:
   a. Go to *VPN > SSL-VPN Settings*.
   b. Under *Web Mode Settings*, set *Language* to *Browser Preference*.



SSL-VPN Settings

Specify WINS Servers ○

Web Mode Settings

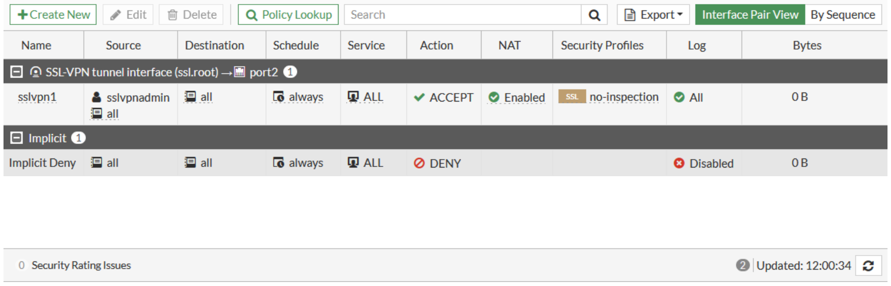
Language: [✓ Browser Preference] System

Authentication/Portal Mapping

Users/Groups	Portal
sslvpnadmin	testportal1

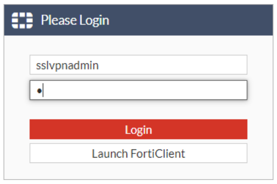
   c. Click *Apply*.

3. Add the *sslvpnadmin* user to the policy used by the SSL VPN portal.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
SSL-VPN tunnel interface (ssl.root) → port2 1									
sslvpn1	sslvpnadmin all	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	✓ All	0 B
Implicit 1									
Implicit Deny	all	all	always	ALL	⊘ DENY			✗ Disabled	0 B

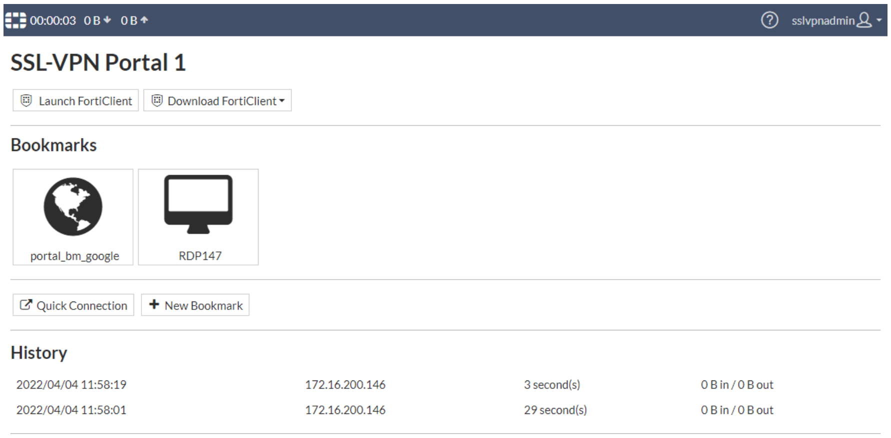
4. Confirm that the configuration works:
   - When the user on PC1 logs in to the SSL VPN portal using Chrome in English, all of the pages are shown in English.



Please Login

sslvpnadmin

•



00:00:03 0 B 0 B sslvpnadmin

SSL-VPN Portal 1

Launch FortiClient | Download FortiClient

Bookmarks

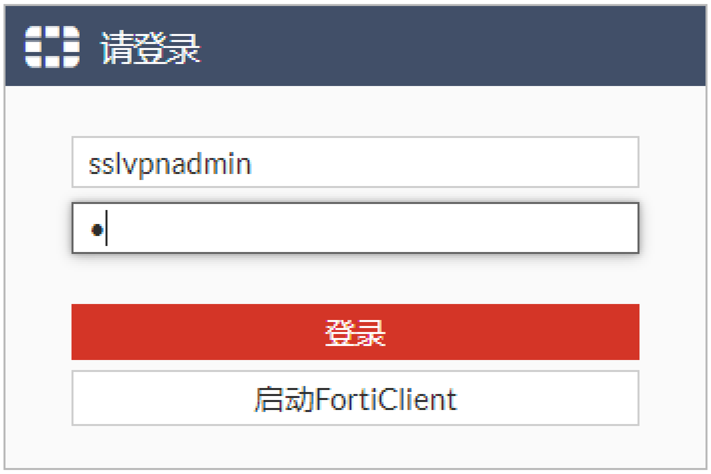
portal_bm_google | RDP147

Quick Connection | New Bookmark

History

2022/04/04 11:58:19	172.16.200.146	3 second(s)	0 B in / 0 B out
2022/04/04 11:58:01	172.16.200.146	29 second(s)	0 B in / 0 B out

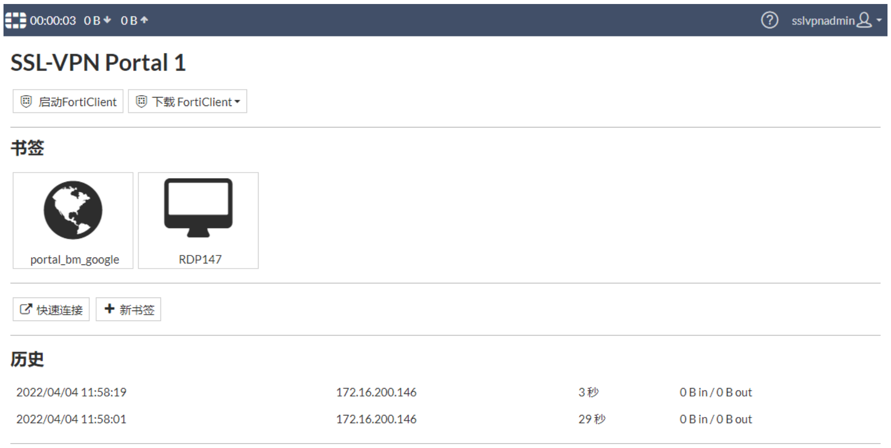
- When the user on PC2 logs in to the SSL VPN portal using Edge in Simplified Chinese, all of the pages are shown in Simplified Chinese.



请登录

sslvpnadmin

●



00:00:03 0 B 0 B sslvpnadmin

SSL-VPN Portal 1

启动FortiClient | 下载 FortiClient

书签

portal_bm_google | RDP147

快速连接 | 新书签

历史

2022/04/04 11:58:19	172.16.200.146	3 秒	0 B in / 0 B out
2022/04/04 11:58:01	172.16.200.146	29 秒	0 B in / 0 B out

SLA link monitoring for dynamic IPsec and SSL VPN tunnels

The link health monitor settings can measure SLA information of dynamic VPN interfaces, which assign IP addresses to their clients during tunnel establishment. This includes SSL VPN tunnels, IPsec remote access, and IPsec site-to-site tunnels.

This feature currently only supports IPv4 and the ICMP monitoring protocol. In the IPsec tunnel settings, `net-device` must be disabled.

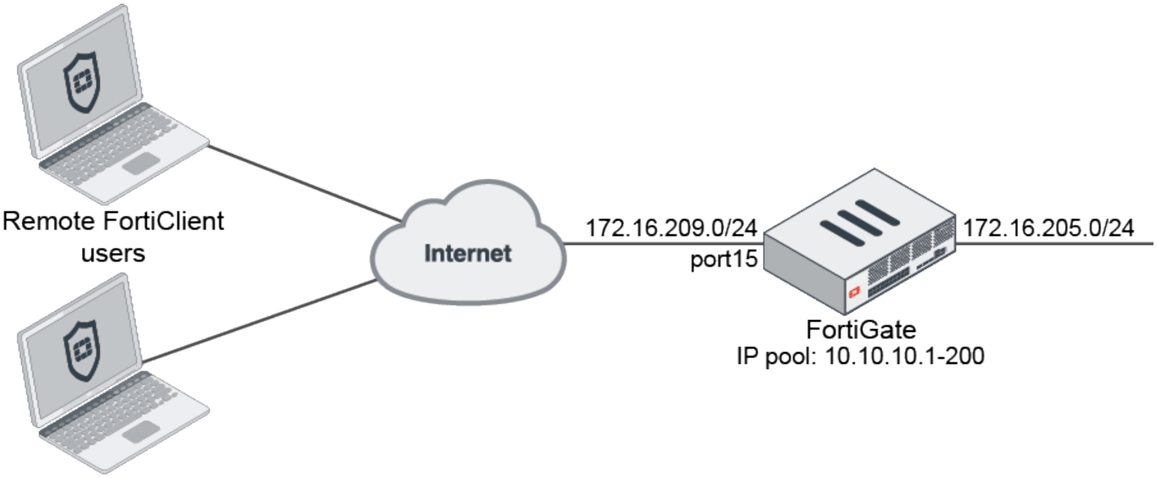
```
config system link-monitor
    edit <name>
        set server-type {static | dynamic}
    next
end
```

To view the dial-up tunnel statistics:

```
# diagnose sys link-monitor tunnel {name | all} [<tunnel_name>]
```

Example

In this example, endpoint users dial up using FortiClient to create IPSec tunnels with the FortiGate and obtain IP addresses. The link monitor on the FortiGate's dynamic VPN interface detects the path quality to the endpoints.



To configure SLA link health monitoring in dynamic IPsec tunnels:

1. Configure the IPsec phase 1 interface:

```
config vpn ipsec phase1-interface
    edit "for_Branch"
        set type dynamic
        set interface "port15"
        set mode aggressive
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set dhgrp 5
        set xauthtype auto
        set authusrgrp "vpngroup"
        set assign-ip-from name
        set ipv4-netmask 255.255.255.0
        set dns-mode auto
        set ipv4-split-include "172.16.205.0"
        set ipv4-name "client_range"
        set save-password enable
        set psksecret **********
        set dpd-retryinterval 60
    next
end
```

2. Configure the IPsec phase 2 interface:

```
config vpn ipsec phase2-interface
    edit "for_Branch_p2"
        set phase1name "for_Branch"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set dhgrp 5
    next
end
```

3. Configure the dynamic interface:

```
config system interface
    edit "for_Branch"
        set vdom "root"
        set ip 10.10.10.254 255.255.255.255
        set type tunnel
        set remote-ip 10.10.10.253 255.255.255.0
        set snmp-index 100
        set interface "port15"
    next
end
```

4. Add the IPsec dial-up tunnel to the link health monitor:

```
config system link-monitor
    edit "1"
        set srcintf "for_Branch"
        set server-type dynamic
    next
end
```

5. Once endpoint users have connected using FortiClient, verify the tunnel information:

```
# get vpn ipsec tunnel summary
'for_Branch_0' 10.1.100.23:0  selectors(total,up): 1/1  rx(pkt,err): 21091/0  tx
(pkt,err): 20741/0
'for_Branch_1' 10.1.100.13:0  selectors(total,up): 1/1  rx(pkt,err): 19991/0  tx
(pkt,err): 20381/0
```

6. Verify the link health monitor status:

```
# diagnose sys link-monitor tunnel all
for_Branch_0 (1): state=alive, peer=10.10.10.1, create_time=2022-02-08 10:43:11,
srcintf=for_Branch, latency=0.162, jitter=0.018, pktloss=0.000%
for_Branch_1 (1): state=alive, peer=10.10.10.2, create_time=2022-02-08 10:49:24,
srcintf=for_Branch, latency=0.266, jitter=0.015, pktloss=0.000%
```

7. Manually add 200 ms latency on the path between the FortiGate and FortiClients.

8. Verify the link health monitor status again:

```
# diagnose sys link-monitor tunnel all
for_Branch_0 (1): state=alive, peer=10.10.10.1, create_time=2022-02-08 10:43:11,
srcintf=for_Branch, latency=200.177, jitter=0.021, pktloss=0.000%
for_Branch_1 (1): state=alive, peer=10.10.10.2, create_time=2022-02-08 10:49:24,
srcintf=for_Branch, latency=200.257, jitter=0.017, pktloss=0.000%
```

IPsec IKE load balancing based on FortiSASE account information - 7.2.5

This information is also available in the FortiOS 7.2 Administration Guide:

- IPsec IKE load balancing based on FortiSASE account information

The FortiGate device ID is carried by the IKEv2 message NOTIFY payload when it is configured.

```
config vpn ipsec phase1-interface
    edit <name>
        set dev-id-notification enable
        set dev-id <string>
    next
end
```

This device ID configuration is required when the FortiGate is configured as a secure edge LAN extension for FortiSASE. It allows FortiSASE to distribute IKE/IPsec traffic according to the FortiGate device ID to achieve load balancing.

For more information about this feature, see IPsec IKE load balancing based on FortiSASE account information.

Securely exchange serial numbers between FortiGates connected with IPsec VPN - 7.2.6

This information is also available in the FortiOS 7.2 Administration Guide:

- Securely exchange serial numbers between FortiGates connected with IPsec VPN

Serial numbers can be securely exchanged between FortiGates connected with IPsec VPN. This feature is supported in IKEv2, IKEv1 main mode, and IKEv1 aggressive mode. The exchange is only performed with participating FortiGates that have enabled the `exchange-fgt-device-id` setting under `config vpn ipsec phase1-interface`.

For more information about this feature, see Securely exchange serial numbers between FortiGates connected with IPsec VPN.

User and authentication

This section includes information about user and authentication related new features:

Authentication

This section includes information about authentication related new features:

RADIUS Termination-Action AVP in wired and wireless scenarios

When authenticating with RADIUS in a wired or wireless scenario, the FortiGate can support proper handling of the Termination-Action AVP.

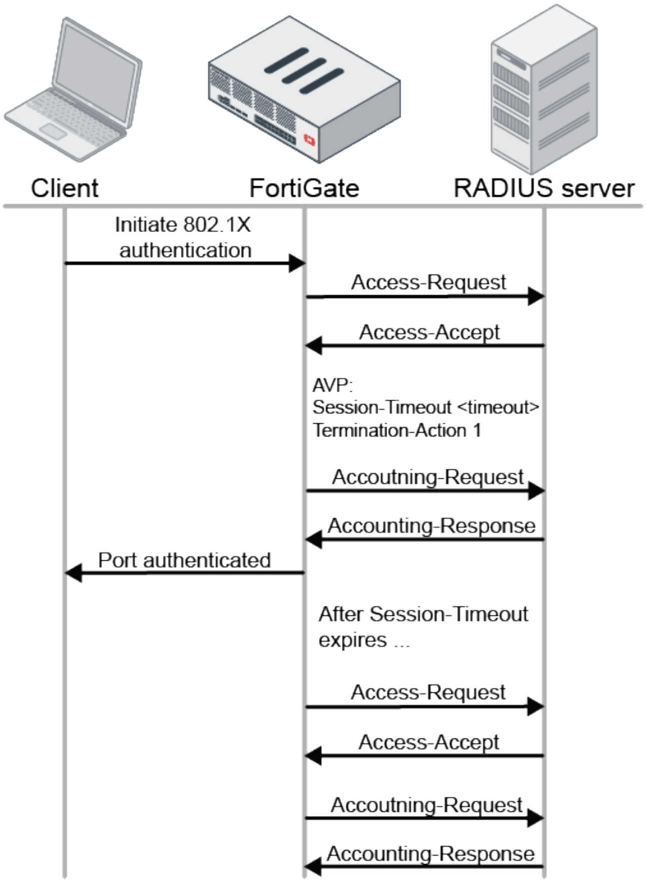
In a wired scenario, a hardware switch configured with 802.1X security authentication can read the Termination-Action attribute value from the RADIUS Access-Accept response. If the Termination-Action is 1, the FortiGate will initiate re-authentication when the session time has expired. During re-authentication, the port stays authorized. If the Termination-Action is 0, the session will be terminated.

In a wireless scenario, when a virtual AP is configured with WPA2-Enterprise security with RADIUS and has CoA enabled, it processes the RADIUS CoA request immediately upon receiving it and re-authenticates when the Termination-Action is 1.

Wired example

This example has a FortiGate configured with a hardware switch with two ports: port3 and port5. The hardware switch is enabled with 802.1X security and assigned to a RADIUS user group. Upon a successful authentication, the RADIUS server responds with an Access-Accept containing the authentication Session-Timeout and Termination-Action attributes. In this example, the Termination-Action value is 1, which informs the client to re-authenticate when the session time expires. During this time, the FortiGate keeps the client/port authorized while it initiates the re-authentication with the RADIUS server.

The message exchange is as follows:



To configure the RADIUS server and the FortiGate to handle the Termination-Action AVP:

1. On the RADIUS server, configure the Termination-Action AVP with the value `RADIUS-Request (1)` to indicate that re-authentication should occur upon expiration of the Session-Time.
2. On the FortiGate, configure the RADIUS server:

```
config user radius
    edit "rad1"
        set server "172.18.60.203"
        set secret ENC **********
        set radius-coa enable
        config accounting-server
            edit 1
                set status enable
                set server "172.18.60.203"
                set secret ENC **********
            next
        end
    next
end
```

3. Configure the RADIUS user group:

```
config user group
    edit "group_radius"
        set member "rad1"
    next
end
```

4. **Configure the hardware switch with 802.1X enabled.**
   a. Configure the virtual switch settings:

```
config system virtual-switch
    edit hw2
        set physical-switch "sw0"
        config port
            edit port3
            next
            edit port5
            next
        end
    next
end
```

   b. Configure the interface settings:

```
config system interface
    edit hw2
        set vdom vdom1
        set ip 6.6.6.1 255.255.255.0
        set allowaccess ping https ssh
        set stp enable
        set security-mode 802.1X
        set security-groups "group_radius"
    next
end

WARNING: Changing 802.1X could interrupt network connectivity on affected interfaces.
Do you want to continue? (y/n)y
```

5. On the client device, initiate 802.1X authentication, then verify that the switch port shows as authorized:

```
# diagnose sys 802-1x status
Virtual switch 'hw2' (default mode) 802.1x member status:
  port3: Link up, 802.1X state: unauthorized
  port5: Link up, 802.1X state: authorized
```

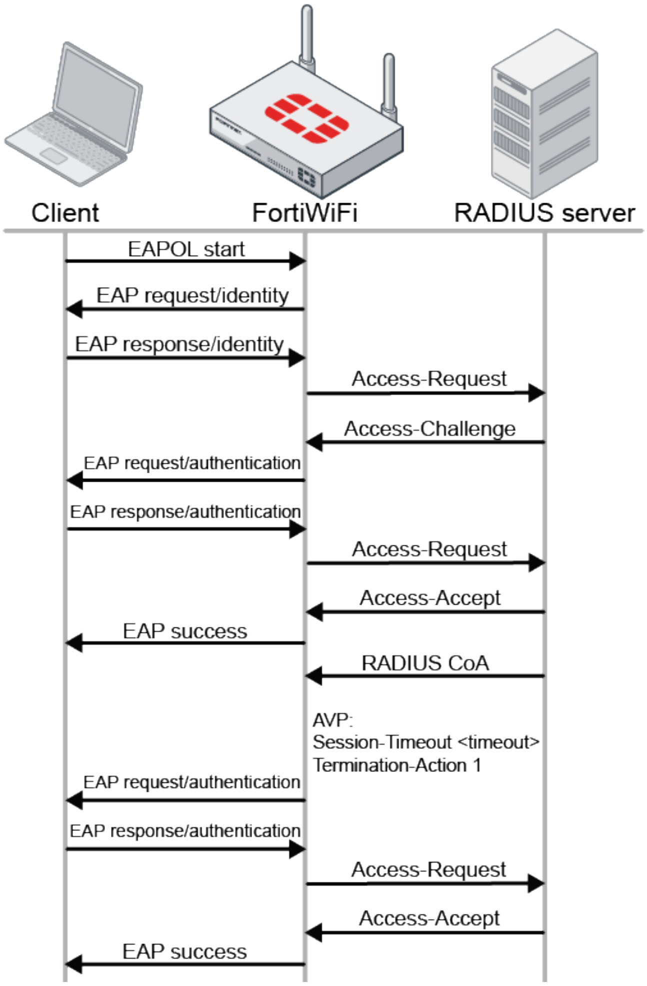
6. After successful authentication, wait for the session to timeout.
7. The FortiGate will keep the 802.1X port authenticated, and initiate re-authentication with the same Acct-Session-Id to the RADIUS server. The 802.1X status of the port remains unchanged:

```
# diagnose sys 802-1x status
Virtual switch 'hw2' (default mode) 802.1x member status:
  port3: Link up, 802.1X state: unauthorized
  port5: Link up, 802.1X state: authorized
```

Wireless example

In this example, a virtual AP is configured with WPA2-Enterprise security with RADIUS and has CoA enabled. After a wireless user authenticates and connects to the wireless SSID, the RADIUS server triggers a CoA event with AVPs Session-timeout and a Termination-Action of 1. This signals the FortiGate to trigger re-authentication of the client, which the client immediately performs to stay connected to the wireless SSID.

The message exchange is as follows:



To configure the FortiGate to handle the Termination-Action AVP:

1. Configure the RADIUS server:

```
config user radius
    edit "peap"
        set server "172.16.200.55"
        set secret **********
        set radius-coa enable
    next
end
```

2. Configure the VAP:

```
config wireless-controller vap
    edit "wifi"
        set ssid "FWF-60E-coa"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "peap"
        set schedule "always"
    next
end
```

3. Verify that the wireless station connects to the SSID:

```
# diagnose wireless-controller wlac -d sta online
   vf=0 wtp=1 rId=1 wlan=wifi vlan_id=0 ip=10.10.80.2 ip6=:: mac=**:**:**:**:**:** vci=
host=wifi-qa-01 user=test1 group=group1 signal=-28 noise=-95 idle=1 bw=0 use=6 chan=149
radio_type=11AC security=wpa2_only_enterprise mpsk= encrypt=aes cp_authed=no online=yes
mimo=2
```

4. From the RADIUS server, manually trigger a RADIUS CoA event.
   a. RADIUS CoA sent to the FortiGate:

```
Sent CoA-Request Id 7 from 0.0.0.0:54158 to 172.16.200.201:3799 length 39
    User-Name = "test1"
    Session-Timeout = 120
    Termination-Action = RADIUS-Request
```

   b. RADIUS CoA-ACK received from the FortiGate:

```
Received CoA-ACK Id 7 from 172.16.200.201:3799 to 0.0.0.0:0 length 44
    Event-Timestamp = "Jan  5 2022 14:43:12 PST"
    Message-Authenticator = 0x3311ba3b763d68da653ab34351b0308
```

5. On the wireless station console, verify that the re-authentication happens immediately:

```
root@wifi-qa-01:/home/wpa-test# wlan1: CTRL-EVENT-EAP-STARTED EAP authentication started
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 25 (PEAP) selected
EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed
wlan1: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
wlan1: PMKSA-CACHE-REMOVED **:**:**:**:**:** 0
wlan1: PMKSA-CACHE-ADDED **:**:**:**:**:** 0
wlan1: WPA: Key negotiation completed with **:**:**:**:**:** [PTK=CCMP GTK=CCMP]
```

Improve response time for direct FSSO login REST API

Upon receiving direct FSSO logon REST API requests, the FortiGate now returns the HTTP response code instantaneously and offloads the LDAP group membership query to a backend API. This improves response times, and prevents delays and backlogs when many requests are sent in a short time period.

The direct FSSO logon REST API was added to FortiOS in 6.4.4 to allow an authenticated user from a third party service to be queried against LDAP by the FortiGate for group membership. This provides SSO capabilities for the end user of the third party service when integrated with the FortiGate.

Example

This example compares the difference in HTTP response time before and after the feature implementation.

The following process flow occurs:

1. A user logs on to the third party service.
2. The third party service calls the REST API to relay the authenticated user to the FortiGate, so that the FortiGate can provide SSO service to this user.
3. The FortiGate receives the HTTP POST request and responds immediately.

4. In the meantime, the FortiGate sends the username to fnbamd to further query the user against LDAP for its group membership.
5. The query is successful in the user group. The user, IP, and group are added to the firewall authentication table on the FortiGate.

Before	After
`{`	`{`
`"http_method":"POST",`	`"http_method":"POST",`
`"status":"success",`	`"status":"success",`
`"http_status":200,`	`"http_status":200,`
`"vdom":"root",`	`"vdom":"root",`
`"path":"user",`	`"path":"user",`
`"name":"firewall",`	`"name":"firewall",`
`"action":"auth",`	`"action":"auth",`
`"serial":"FG4H1E0000000000",`	`"serial":"FG4H1E0000000000",`
`"version":"v7.0.4",`	`"version":"v7.2.0",`
`"build":291`	`"build":1095`
`}`	`}`
`real    0m3.770s`	**`real    0m0.115s`**
`user    0m0.048s`	`user    0m0.040s`
`sys 0m0.020s`	`sys 0m0.032s`

Note the HTTP response time is shorter after the implementation.

Configuring client certificate authentication on the LDAP server

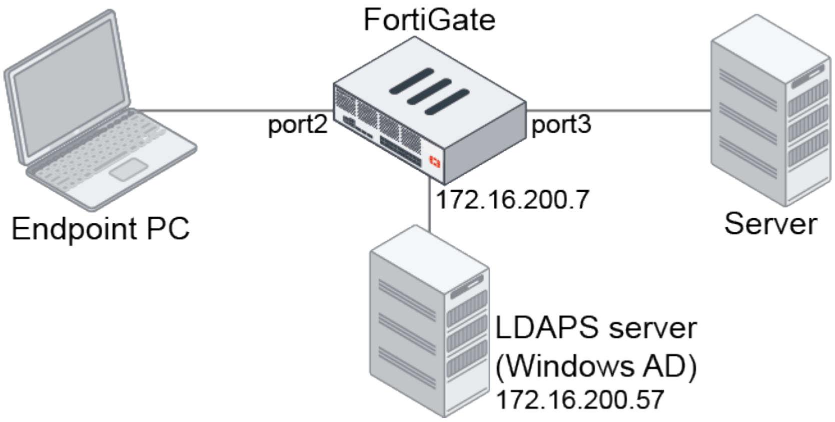
Administrators can configure a FortiGate client certificate in the LDAP server configuration when the FortiGate connects to an LDAPS server that requires client certificate authentication.

```
config user ldap
    edit <ldap_server>
        set client-cert-auth {enable | disable}
        set client-cert <source>
    next
end
```

Example

In this example, the FortiGate is configured as an explicit web proxy. It connects to the Windows AD server through LDAPS, where the Windows server requires a client certificate to connect. The client certificate is configured in the CLI.

The endpoint PC connecting to the web server will first need to authenticate to the explicit web proxy before accessing the server.



While this example demonstrates an LDAP client certificate for an explicit proxy configuration, LDAP client certificates can be used in firewall authentication, transparent proxy, ZTNA, and where ever LDAP configurations are used on the FortiGate.

To configure a client certificate on the LDAP server:

1. Enable the explicit web proxy on port2:

```
config system interface
    edit "port2"
        set explicit-web-proxy enable
    next
end
```

2. Upload the client certificate to the FortiGate:

```
config vpn certificate local
    edit "Zach"
        set password **********
        set private-key <private key>
        set certificate <certificate>
    next
end
```

3. Configure the LDAP server settings:

```
config user ldap
    edit "ldaps"
        set server "172.16.200.57"
        set server-identity-check disable
        set cnid "CN"
        set dn "CN=Users,DC=ftnt,DC=com"
        set secure ldaps
        set port 636
        set client-cert-auth enable
        set client-cert "Zach"
    next
end
```

4. Configure the authentication scheme:

```
config authentication scheme
    edit "1"
```

```
            set method basic
            set user-database "ldaps"
        next
    end
```

5. Configure the authentication rule:

```
config authentication rule
    edit "1"
        set srcintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set active-auth-method "1"
    next
end
```

6. Configure the user group:

```
config user group
    edit "test"
        set member "ldaps"
    next
end
```

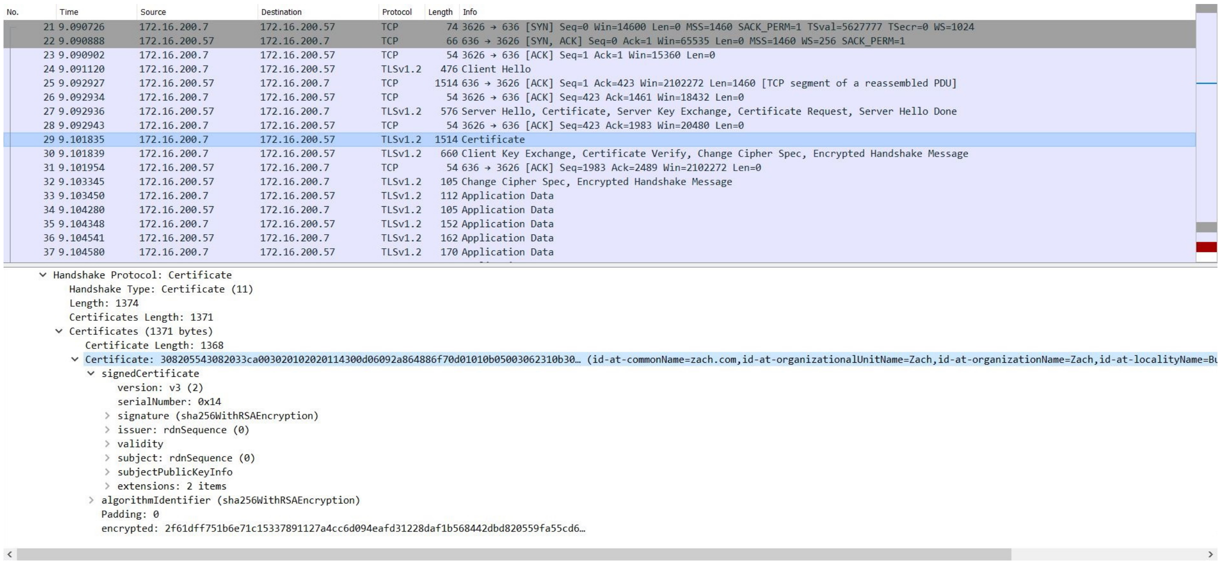
7. Configure the proxy policy with the user group:

```
config firewall proxy-policy
    edit 1
        set proxy explicit-web
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set schedule "always"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set groups "test"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection-clone"
        set av-profile "av"
    next
end
```

Testing and verification

When traffic from the endpoint PC matches a policy and triggers authentication, the FortiGate starts the LDAPS TLS connection handshake with the Windows AD. The LDAPS server requests a client certificate to identify the FortiGate as a client. The FortiGate provides a configured client certificate, issued to zach.com, to the LDAPS server.

The following communication between the FortiGate and the LDAPS server shows the client certificate is sent by the FortiGate:



```
No.     Time          Source          Destination     Protocol  Length Info
     21 9.090726      172.16.200.7    172.16.200.57   TCP         74 3626 → 636 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5627777 TSecr=0 WS=1024
     22 9.090888      172.16.200.57   172.16.200.7    TCP         66 636 → 3626 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
     23 9.090902      172.16.200.7    172.16.200.57   TCP         54 3626 → 636 [ACK] Seq=1 Ack=1 Win=15360 Len=0
     24 9.091120      172.16.200.7    172.16.200.57   TLSv1.2    476 Client Hello
     25 9.092927      172.16.200.57   172.16.200.7    TCP       1514 636 → 3626 [ACK] Seq=1 Ack=423 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
     26 9.092934      172.16.200.7    172.16.200.57   TCP         54 3626 → 636 [ACK] Seq=423 Ack=1461 Win=18432 Len=0
     27 9.092936      172.16.200.57   172.16.200.7    TLSv1.2    576 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
     28 9.092943      172.16.200.7    172.16.200.57   TCP         54 3626 → 636 [ACK] Seq=423 Ack=1983 Win=20480 Len=0
     29 9.101835      172.16.200.7    172.16.200.57   TLSv1.2   1514 Certificate
     30 9.101839      172.16.200.7    172.16.200.57   TLSv1.2    660 Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
     31 9.101954      172.16.200.57   172.16.200.7    TCP         54 636 → 3626 [ACK] Seq=1983 Ack=2489 Win=2102272 Len=0
     32 9.103345      172.16.200.57   172.16.200.7    TLSv1.2    105 Change Cipher Spec, Encrypted Handshake Message
     33 9.103450      172.16.200.7    172.16.200.57   TLSv1.2    112 Application Data
     34 9.104280      172.16.200.57   172.16.200.7    TLSv1.2    105 Application Data
     35 9.104348      172.16.200.7    172.16.200.57   TLSv1.2    152 Application Data
     36 9.104541      172.16.200.57   172.16.200.7    TLSv1.2    162 Application Data
     37 9.104580      172.16.200.7    172.16.200.57   TLSv1.2    170 Application Data
```

```
    Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1374
        Certificates Length: 1371
      Certificates (1371 bytes)
            Certificate Length: 1368
          Certificate: 308205543082033ca003020102020114300d06092a864886f70d01010b05003062310b30… (id-at-commonName=zach.com,id-at-organizationalUnitName=Zach,id-at-organizationName=Zach,id-at-localityName=Bu
              signedCertificate
                    version: v3 (2)
                    serialNumber: 0x14
                  > signature (sha256WithRSAEncryption)
                  > issuer: rdnSequence (0)
                  > validity
                  > subject: rdnSequence (0)
                  > subjectPublicKeyInfo
                  > extensions: 2 items
              > algorithmIdentifier (sha256WithRSAEncryption)
                Padding: 0
                encrypted: 2f61dff751b6e71c15337891127a4cc6d094eafd31228daf1b568442dbd820559fa55cd6…
```

Tracking rolling historical records of LDAP user logins

Authenticated LDAP users can be tracked by logging the users' group memberships, logon timestamps, and logout timestamps into local files on a log disk over a rolling four-week period. The historical records can be queried from the CLI. This feature is only enabled on FortiGate models with a log disk.

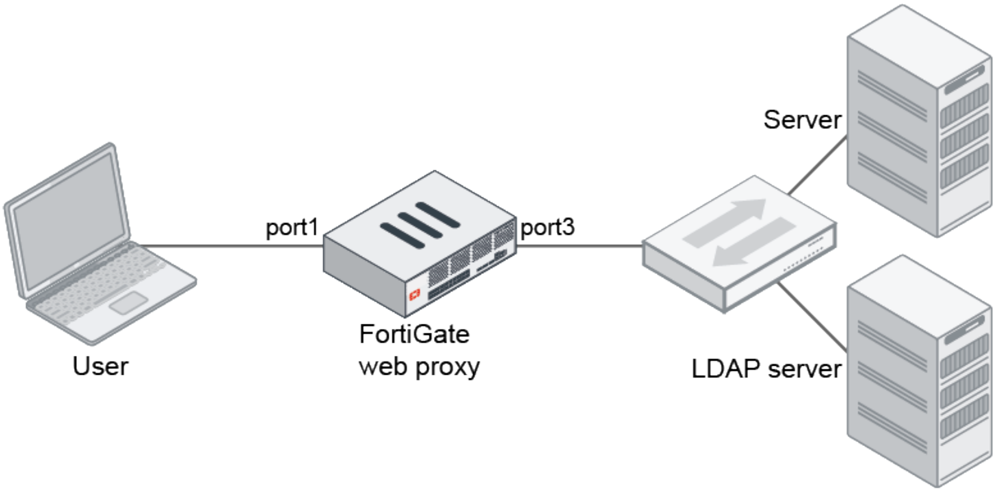
To view active user logged information:

```
# diagnose user-device-store user-stats query <yyyy-mm-dd> <range_in_days>
```

Example

In this example, the FortiGate is configured with an explicit web proxy and an LDAP server. When an LDAP user is authenticated by an IP-based authentication method in WAD, the WAD user is considered to be in an active logon status. This WAD user is listed in the `diagnose wad user list` output. If the user is removed from WAD as an authenticated, such as when the IP-based authentication expires, then the user is considered to become inactive (logout status). The user is no longer listed in the `diagnose wad user list` output.

The WAD user's group membership information and their logon and logout timestamps are written into local files on the FortiGate's disk. There is one log file for each day, and the FortiGate can maintain up to 28 log files over a rolling period of 28 days (four weeks). This means after 28 days with 28 files stored, on the 29th day, the first file will be removed and a new file will be created for the 29th day.



This feature works on other configurations such as firewall authentication, transparent web proxy, ZTNA, and SSL VPN where an LDAP server is used.

To configure the FortiGate:

1. Enable the explicit web proxy on port1:

```
config system interface
    edit "port1"
        set explicit-web-proxy enable
        set explicit-ftp-proxy enable
        set snmp-index 3
    next
end
```

2. Configure the LDAP server:

```
config user ldap
    edit "ldap-test"
        set server "172.16.200.98"
        set cnid "cn"
        set dn "dc=fortinetqa,dc=local"
        set type regular
        set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
        set password **********
    next
end
```

3. Configure the authentication scheme:

```
config authentication scheme
    edit "basic-ldap"
        set method basic
        set user-database "ldap-test"
    next
end
```

4. Configure the authentication rule:

```
config authentication rule
    edit "basic-ldap"
        set srcaddr "all"
        set active-auth-method "basic-ldap"
        set web-portal disable
    next
end
```

5. Configure the user group:

```
config user group
    edit "ldap-group"
        set member "ldap" "ldap-test"
    next
end
```

6. Configure the proxy policy:

```
config firewall proxy-policy
    edit 1
        set proxy explicit-web
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set service "web"
        set action accept
        set schedule "always"
        set groups "ldap-group"
        set utm-status enable
        set ssl-ssh-profile "deep-custom"
        set av-profile "av"
    next
end
```

   When users pass through the explicit proxy and log in and out through LDAP, their login and logout records will be logged to the disk.

In this example, there are two LDAP users, test1 and test3, with the following activity:

1. test3 logs on at 22:30:22 on February 23, 2022, then logs out at 22:31:09 on the same day.
2. test1 logs on at 23:55:02 on February 23, 2022, then logs out at 00:05:02 on February 24, 2022.
3. test3 logs on at 16:29:44 on February 24, 2022, then logs out at 16:39:44 on the same day.

The logon and logout timestamp information, and the group membership information for users test1 and test3 will be logged into two local files on the log disk.

To view the active user logged information for two days back from February 24, 2022:

```
# diagnose user-device-store user-stats query 2022-02-24 2

Record #0:
        'username' = 'test3'
        'groupname' = 'CN=Domain Admins,CN=Users,DC=FORTINETQA,DC=local'
        'groupname' = 'CN=FSSO,OU=QA,DC=FORTINETQA,DC=local'
        'logon' = '2022-02-23 22:30:22'
        'logout' = '2022-02-23 22:31:09'
```

```
Record #1:
        'username' = 'test1'
        'groupname' = 'CN=Domain Admins,CN=Users,DC=FORTINETQA,DC=local'
        'groupname' = 'CN=FSSO,OU=QA,DC=FORTINETQA,DC=local'
        'groupname' = 'CN=mytest-grp,OU=QA,DC=FORTINETQA,DC=local'
        'logon' = '2022-02-23 23:55:02'

Record #2:
        'username' = 'test1'
        'groupname' = 'CN=Domain Admins,CN=Users,DC=FORTINETQA,DC=local'
        'groupname' = 'CN=FSSO,OU=QA,DC=FORTINETQA,DC=local'
        'groupname' = 'CN=mytest-grp,OU=QA,DC=FORTINETQA,DC=local'
        'logon' = '2022-02-23 23:55:02'
        'logout' = '2022-02-24 00:05:02'

Record #3:
        'username' = 'test3'
        'groupname' = 'CN=Domain Admins,CN=Users,DC=FORTINETQA,DC=local'
        'groupname' = 'CN=FSSO,OU=QA,DC=FORTINETQA,DC=local'
        'logon' = '2022-02-24 16:29:44'
        'logout' = '2022-02-24 16:39:44'

Returned 4 records.
```

There is one record (`logon`) for test1 on `2022-02-23` because they remained active after midnight (until 00:05:02). There is another record for `2022-02-24` with logon and logout timestamps for test1.

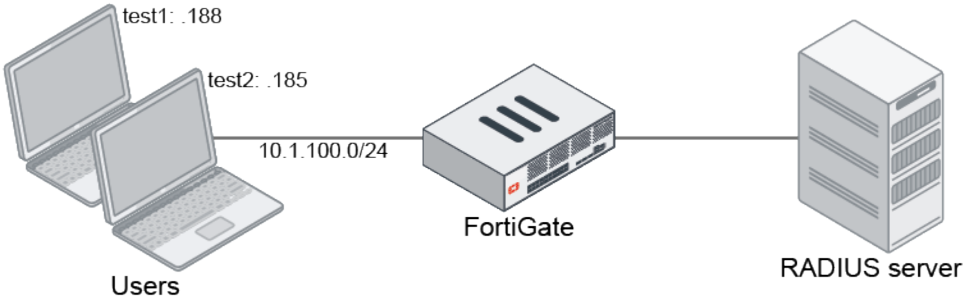
Using a comma as a group delimiter in RADIUS accounting messages

The `set delimiter` RADIUS option allows the FortiGate to set the RADIUS accounting message group delimiter to a comma (,) instead of a plus sign (+) when using RSSO. The default delimiter is still a plus sign.

```
config user radius
    edit <name>
        set delimiter {plus | comma}
    next
end
```

Example

In this example, the FortiGate is configured for RSSO. The FortiGate will read accounting messages from the RADIUS server to determine which user is logged in to which group.



Two users, test1 and test2, belong to multiple groups. The RADIUS server sends accounting messages where groups are delimited by commas. With the comma delimiter, the FortiGate can parse the groups properly and assign users to the correct user group. User test1 belongs to the `rsso1` group, and test2 belongs to the `rsso-group` group.

To configure a comma delimiter in RADIUS accounting messages:

1. Configure the RADIUS server entry:

```
config user radius
    edit "rsso1"
        set rsso enable
        set rsso-radius-response enable
        set rsso-secret **********
        set rsso-endpoint-attribute User-Name
        set delimiter comma
    next
end
```

2. Configure the RSSO user groups:

```
config user group
       edit "rsso1"
        set group-type rsso
        set sso-attribute-value "group3"
       next
       edit "rsso-group"
        set group-type rsso
        set sso-attribute-value "group1"
    next
end
```

Both users should be authenticated with the correct FortiGate RSSO groups. When the users log off and the FortiGate receives a RSSO logoff event notification, the users should be removed from the list of authenticated firewall users.

To verify that the users are parsed to the correct groups:

1. Enable RADIUS debugging messages and verify the RADIUS accounting events:

```
# diagnose debug application radiusd -1
# diagnose debug enable
...
Received radius accounting event
vd 0:root Add/Update auth logon for IP 10.1.100.188 for user test1
DB 0 insert [ep='test1' pg='groupX,group5,group3' ip='10.1.100.188/32'] success
Send accounting response
Received radius accounting event
vd 0:root Add/Update auth logon for IP 10.1.100.185 for user test2
DB 0 insert [ep='test2' pg='groupY,group6,group1' ip='10.1.100.185/32'] success
Send accounting response
```

2. Verify the list of authenticated firewall users:

```
# diagnose firewall auth list l

10.1.100.185, test2
        type: rsso, id: 0, duration: 18, idled: 18
        flag(10): radius
        server: root
        packets: in 0 out 3, bytes: in 0 out 152
        group_id: 15
        group_name: rsso-group
10.1.100.188, test1
        type: rsso, id: 0, duration: 44, idled: 44
        flag(10): radius
        server: root
        packets: in 0 out 0, bytes: in 0 out 0
        group_id: 34
        group_name: rsso1

----- 2 listed, 0 filtered ------
```

3. Once the RSSO logoff events are triggered, verify the RADIUS accounting events in the debugging messages:

```
...
Received radius accounting event
vd 0:root Remove auth logon for IP 10.1.100.188 for user test1
DB 0 remove by IP [ep='test1' pg='groupX,group5,group3' ip='10.1.100.188/32'] success
Send accounting response
Received radius accounting event
vd 0:root Remove auth logon for IP 10.1.100.185 for user test2
DB 0 remove by IP [ep='test2' pg='groupY,group6,group1' ip='10.1.100.185/32'] success
Send accounting response
```

4. Verify the list of authenticated firewall users. Both users logged off, so there are no firewall users:

```
# diagnose firewall auth list 1

----- 0 listed, 0 filtered ------
```

Vendor-Specific Attributes for TACACS - 7.2.1

Vendor-Specific Attributes (VSAs) can be used with TACACS authentication and authorization in wildcard system administrator access to FortiGates from browsers and SSH. The memberof VSA can be used in remote TACACS user group for group matching. The vdom VSA returned from TACACS can be used to overwrite the VDOM in the system admin settings. The admin_prof VSA returned from TACACS can be used to overwrite the accprofile in the system admin settings.

Example

In this example, a FortiGate is configured with multiple VDOMs, and the root acts as the management VDOM. Administrators attempt to log in with SSH or HTTPS through each VDOM.

Using the VSA values for the vdom and admin_prof attributes returned from the TACACS server, the FortiGate can allow access only to the VDOMs returned with the permissions from the corresponding administrator profile. If no VSA values are returned from TACACS, then the FortiGate uses the default values under the config system admin settings.

The TACACS server settings are configured as follows:

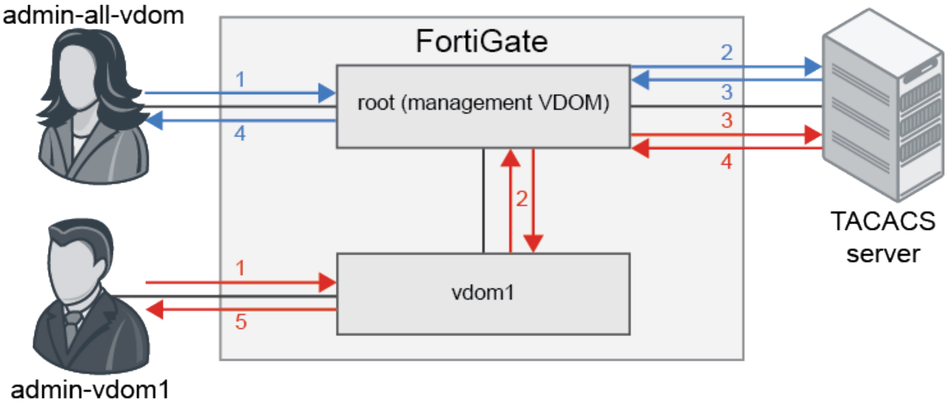
```
user = admin-all-vdom {
    default service = permit
    member = sys_admin_all_vdom
    …
}
user = admin-vdom1 {
    default service = permit
    member = sys_admin_vdom1
    …
}
group = sys_admin_all_vdom {
default service = permit
    service = fortigate {
        memberof = group3
        admin_prof = admin_all_vdom
    }
}
group = sys_admin_vdom1 {
default service = permit
    service = fortigate {
        memberof = group3
        admin_prof = admin_vdom1
        vdom = vdom1
    }
}
```

For multiple VDOMs, each VDOM must be specified in a separate field. For example, for access to vdom1 and vdom2:

```
vdom = vdom1
vdom = vdom2
```

Some TACACS servers, such as Linux TACACS servers, may only return the last VDOM specified.

The authentication process is as follows:



Authentication for admin-all-vdom:

1. The administrator attempts to log in to the FortiGate over the remote TACACS user group, `remote-tacacs`.
2. The FortiGate sends an authorization request to the TACACS server.
3. TACACS authenticates the admin-all-vdom user. The user matches the `sys_admin_all_vdom` TACACS group. TACACS returns following VSA values:

- memberof = group3
- admin_prof = admin_all_vdom

4. The FortiGate authenticates and authorizes the user based on the returned memberof group. The admin_prof value overwrites the accprofile setting configured under system admin. Since no other VDOM VSA is returned, the FortiGate matches the user to the default VDOM configured under system admin, which is admin_no_access.

Authentication for admin-vdom1:

1. The administrator attempts to log in to the FortiGate over the remote TACACS user group, remote-tacacs.
2. vdom1 forwards the request to the management VDOM, which is the root.
3. The FortiGate sends an authorization request to the TACACS server through the management VDOM.
4. TACACS authenticates the admin-vdom1 user. The user matches the sys_admin_vdom1 TACACS group. TACACS returns following VSA values:
   - memberof = group3
   - admin_prof = admin_vdom1
   - vdom = vdom1
5. The FortiGate authenticates and authorizes the user based on the returned memberof group. The other VSA values overwrite the accprofile and VDOM settings configured under system admin. The user is only allowed to access vdom1 with the administrative permissions allowed for admin_vdom1.

To configure the FortiGate:

1. Create two system administrator profiles.
   a. Configure admin_vdom1 who has read-write access to vdom1 (except for firewall policies) and is redistricted from using diagnose commands in the CLI:

```
config system accprofile
    edit "admin_vdom1"
        set secfabgrp read-write
        set ftviewgrp read-write
        set authgrp read-write
        set fwgrp custom
        set system-diagnostics disable
        config fwgrp-permission
            set policy read
            set address read
            set service read
            set schedule read
            set others read
        end
    next
end
```

   b. Configure admin_all_vdom who has read-write access to all VDOMs, but not with super_admin permissions:

```
config system accprofile
    edit "admin_all_vdom"
        set secfabgrp read-write
        set ftviewgrp read-write
        set authgrp read-write
        set sysgrp read
        set netgrp read-write
        set loggrp read-write
        set fwgrp read-write
        set vpngrp read
        set utmgrp read
        set wanoptgrp read
        set wifi read
    next
end
```

2. Configure the TACACS server:

```
config user tacacs+
    edit "tac1"
        set server "10.1.100.34"
        set key XXXXXXXXXXXX
        set authorization enable
    next
end
```

3. Configure the remote TACACS group with group matching:

```
config user group
    edit "remote-tacacs"
        set member "tac1"
        config match
            edit 1
                set server-name "tac1"
                set group-name "group3"
            next
        end
    next
end
```

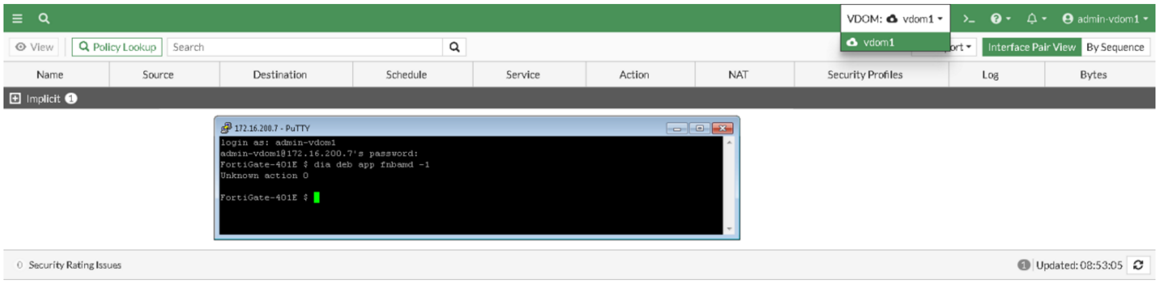
4. Configure the wildcard administrative user assigned to the remote TACACS group:

```
config system admin
    edit "remote-admin"
        set remote-auth enable
        set accprofile "admin_no_access"
        set vdom "root" "vdom1"
        set wildcard enable
        set remote-group "remote-tacacs"
        set accprofile-override enable
        set vdom-override enable
    next
end
```

To verify the configuration:

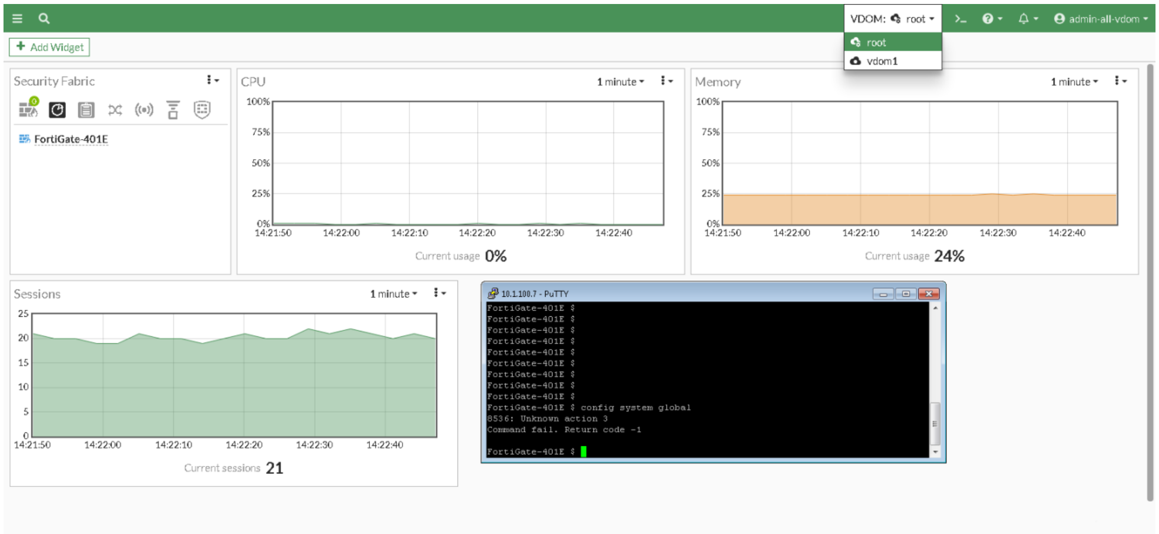
1. Log in as admin-vdom1 using a browser and SSH. The following behavior is expected:
    - The user can only access vdom1 (returned by TACACS in the `vdom` VSA).
    - The user can view firewall policies, but they cannot not create new policies.

- The user cannot run `diagnose debug application` commands in the PuTTY SSH session.



```
login as: admin-vdom1
admin-vdom1@172.16.200.7's password:
FortiGate-401E $ dia deb app fnbamd -1
Unknown action 0

FortiGate-401E $
```

2. Log in as admin_all_vdom using a browser and SSH. The following behavior is expected:
    - The user has no VSA VDOM configured on the TACACS server, so the default setting in the `system admin` configuration should apply. The user can access the root and vdom1 VDOMs.
    - The user has no access to `system global` in the CLI, and the prompt symbol is a `$` instead of a `#`.



```
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $
FortiGate-401E $ config system global
8536: Unknown action 3
Command fail. Return code -1

FortiGate-401E $
```

Synchronizing LDAP Active Directory users to FortiToken Cloud using the two-factor filter - 7.2.1

To synchronize Active Directory users and apply two-factor authentication using FortiToken Cloud, two-factor authentication can be enabled in the `user ldap` object definition in FortiOS. By default, FortiOS retrieves all Active Directory users in the LDAP server with a valid email or mobile number (`mail` and `mobile` attributes), and synchronizes the users to FortiToken Cloud. Users are then created on FortiToken Cloud and activation is sent out using email or SMS.

Two-factor filters can be used to reduce the number of the Active Directory users returned, and only synchronize the users who meet the filter criteria.

For more information about this feature, see Synchronizing LDAP Active Directory users to FortiToken Cloud using the group filter. This example is for FortiOS 7.0.6 and uses the `group-filter` option, which is replaced with `two-factor-filter` in FortiOS 7.2.1 and later.

Specify the SAN field to use for LDAP-integrated certificate authentication - 7.2.4

This information is also available in the FortiOS 7.2 Administration Guide:

- Using the SAN field for LDAP-integrated certificate authentication

Before this enhancement, certificate-based authentication against Active Directory LDAP (AD LDAP) only supported the UserPrincipleName (UPN) as the unique identifier in the Subject Alternative Name (SAN) field in peer user certificates. This enhancement extends the use case to cover the RFC 822 Name (corporate email address) defined in the SAN extension of the certificate to contain the unique identifier used to match a user in AD LDAP. It also allows the DNS defined in the user certificate to be used as a unique identifier.

```
config user ldap
    edit <name>
        set account-key-upn-san {othername | rfc822name | dnsname}
    next
end
```

`account-key-upn-san {othername | rfc822name | dnsname}`	Define the SAN in the certificate for UserPrincipleName matching: • othername: match to UserPrincipleName (UPN) on AD LDAP server (default) • rfc822name: match to RFC 822 email address • dnsname: match to DNS name

The LDAP server configurations are applied to the user peer configuration when the PKI user is configured.

```
config user peer
    edit <name>
        set ca <string>
        set cn <string>
        set ldap-server <string>
        set ldap-mode principal-name
    next
end
```

When a user authenticates to the FortiGate for an administrative log in, SSL VPN, IPsec dialup, or firewall authentication using a user certificate, it presents a signed certificate issued by a trusted CA to the FortiGate. The following sequence of events occurs as the FortiGate processes the certificate for authentication:

1. The FortiGate verifies if the certificate is issued by a trusted CA. If the CA is not a public CA, ensure that the CA certificate is uploaded and trusted by the FortiGate, and is applied to the user peer configurations (`set ca <string>`).
2. The FortiGate verifies that the CN field of the certificate matches the CN specified in the user peer configurations (`set cn <string>`).
3. If the `user peer` configuration has `ldap-server` configured and the `ldap-mode` is set to `principal-name`, the FortiGate uses the unique identifier in the certificate to authenticate against the LDAP server.
    a. If `set account-key-upn-san othername` is configured (the default setting), the FortiGate uses the UPN in the certificate's SAN field to authenticate against LDAP.
    b. If `set account-key-upn-san rfc822name` is configured, the FortiGate uses the RFC 822 Name in the certificate's SAN field to authenticate against LDAP.
    c. If `set account-key-upn-san dnsname` is configured, the FortiGate uses the DNS name in the certificate to authenticate against LDAP.

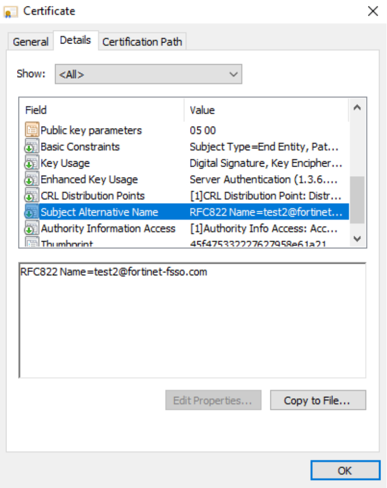
4. By default, the FortiGate tries to match the UserPrincipleName (UPN) attribute on the AD LDAP. If this needs to be changed to another field, configure the `account-key-filter` setting on the LDAP configuration:

```
config user ldap
    edit <name>
        set account-key-filter <string>
    next
end
```

Example

In this example, a user certificate is issued by a customer's CA to a user. The user uses this certificate to authenticate to the SSL VPN web portal. The administrator decides to use the RFC 822 Name in the SAN field to authenticate against their corporate AD LDAP. The Active Directory attribute to check against the RFC 822 Name field is the mail attribute.

User certificate information:



Field	Value
Public key parameters	05 00
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Subject Alternative Name	RFC822 Name=test2@fortinet...
Authority Information Access	[1]Authority Info Access: Acc...
Thumbprint	45f475332227627958e61a21

RFC822 Name=test2@fortinet-fsso.com

The configuration used in this example assumes the following:

- The CA certificate has already been uploaded to the FortiGate.
- The SSL VPN configurations have already been configured, pending the assignment of the PKI user group.

To configure the authentication settings:

1. Configure the LDAP server:

```
config user ldap
    edit "ad-ldap-peer-user"
        set server "10.1.100.131"
        set cnid "cn"
        set dn "dc=fortinet-fsso,dc=com"
        set type regular
        set username "cn=Administrator,cn=users,dc=fortinet-fsso,dc=com"
        set password ENC XXXXXXXXXXXXXXXXX
        set password-renewal enable
        set account-key-upn-san rfc822name
        set account-key-filter "(&(mail=%s)(!
(UserAccountControl:1.2.840.113556.1.4.803:=2)))"
```

```
    next
end
```

By default, the `account-key-filter` filters on the UPN attribute uses the following string: (&(**userPrincipalName=%s**)(!(UserAccountControl:1.2.840.113556.1.4.803:=2))).

- (userPrincipalName=%s) matches the UPN attribute on the AD LDAP.
- (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) filters out inactive and locked AD accounts.

2. Configure the local peer user:

```
config user peer
    edit "peer-RFC822-name"
        set ca "CA_Cert_2"
        set cn "test2"
        set ldap-server "ad-ldap-peer-user"
        set ldap-mode principal-name
    next
end
```

3. Configure the firewall user group for SSL VPN authentication:

```
config user group
    edit "vpn-group"
        set member "peer-RFC822-name"
    next
end
```

4. Apply the user group to the SSL VPN configuration and firewall policy.

Verification

When the SSL VPN user authenticates in a browser, the FortiOS fnbamd daemon first validates the certificate supplied by the user. If the certificate check is successful, the information in the SAN field of the user certificate is used to find a matching user record on the AD LDAP.

To verify the configuration:

```
# diagnose debug app fnbamd -1
# diagnose debug enable
```

The output includes the following information.

- Validate the certificate:

```
...
    __check_crl-***CERTIFICATE IS GOOD***
[567] fnbamd_cert_verify-Issuer found: CA_Cert_2 (SSL_DPI opt 1)
[500] fnbamd_cert_verify-Following cert chain depth 1
[675] fnbamd_cert_check_group_list-checking group with name 'vpn-group'
[490] __check_add_peer-check 'peer-RFC822-name'
[366] peer_subject_cn_check-Cert subject 'C = CA, ST = BC, L = Burnaby, CN = test2'
[294] __RDN_match-Checking 'CN' val 'test2' -- match.
[404] peer_subject_cn_check-CN is good.
```

- Bind to LDAP and try to match the content of the SAN in the user certificate with the user record in the AD LDAP:

```
...
_cert_ldap_query-LDAP query, idx 0
[448] __cert_ldap_query-UPN = 'test2@fortinet-fsso.com'
```

```
[1717] fnbamd_ldap_init-search filter is: (&(mail=test2@fortinet-fsso.com)(!
(UserAccountControl:1.2.840.113556.1.4.803:=2)))
```

- Confirm the successful match:

```
...
     __cert_ldap_query_cb-LDAP ret=0, server='ad-ldap-peer-user', req_id=269178889
[388] __cert_ldap_query_cb-Matched peer 'peer-RFC822-name'
...
[1066] fnbamd_cert_auth_copy_cert_status-req_id=269178889
[1074] fnbamd_cert_auth_copy_cert_status-Matched peer user 'peer-RFC822-name'
[833] fnbamd_cert_check_matched_groups-checking group with name 'vpn-group'
[895] fnbamd_cert_check_matched_groups-matched
[1193] fnbamd_cert_auth_copy_cert_status-Cert st 290, req_id=269178889
[209] fnbamd_comm_send_result-Sending result 0 (nid 672) for req 269178889, len=2155
```

Secure access

This section includes information about secure access related new features:

- Wireless on page 463
- Switch controller on page 533
- NAC on page 558
- FortiExtender on page 561

Wireless

This section includes information about wireless related new features:

- Disable dedicated scanning on FortiAP F-Series profiles on page 465
- Allow pre-authorization of a FortiAP by specifying a Wildcard Serial Number on page 463
- Improve WiFi channel selection GUI on page 469
- Support Layer 3 roaming for tunnel mode on page 470
- Report wireless client app usage for clients connected to bridge mode SSIDs on page 477
- Support enabling or disabling 802.11d 7.2.1 on page 480
- Improve MAC address filtering 7.2.1 on page 482
- Support Layer 3 roaming for bridge mode 7.2.1 on page 486
- Redesign rate control CLI 7.2.1 on page 494
- Add GUI visibility for Advanced Wireless Features 7.2.1 on page 498
- Add profile support for FortiAP G-series models supporting WiFi 6E Tri-band and Dual 5 GHz modes 7.2.1 on page 509
- WPA3 enhancements to support H2E only and SAE-PK 7.2.1 on page 516
- Implement multi-processing for wireless daemon for large-scale FortiAP management 7.2.4 on page 519
- Allow custom RADIUS NAS-ID 7.2.4 on page 522
- Support wireless client mode on FortiWiFi 80F series models 7.2.4 on page 524
- Support displaying details about wired clients connected to the FortiAP LAN port 7.2.4 on page 529
- Simplify BLE iBeacon provisioning for RTLS deployments 7.2.5 on page 531

Allow pre-authorization of a FortiAP by specifying a Wildcard Serial Number

This enhancement allows a FortiGate Wireless Controller to pre-authorize a FortiAP by specifying a Wildcard Serial Number (SN) that represents the model of FortiAP you want to authorize. You can pre-configure and pre-authorize a template FortiAP SN to represent the SN of specific FortiAP models. When a physical FortiAP connects, the pre-configured SN is replaced by the actual SN of the FortiAP, and the FortiAP can be automatically authorized.

For example, a Wildcard Serial Number of FP231F****000001 will allow the first FortiAP-231F to register to the Wireless Controller to be authorized automatically and adopt profile configurations.

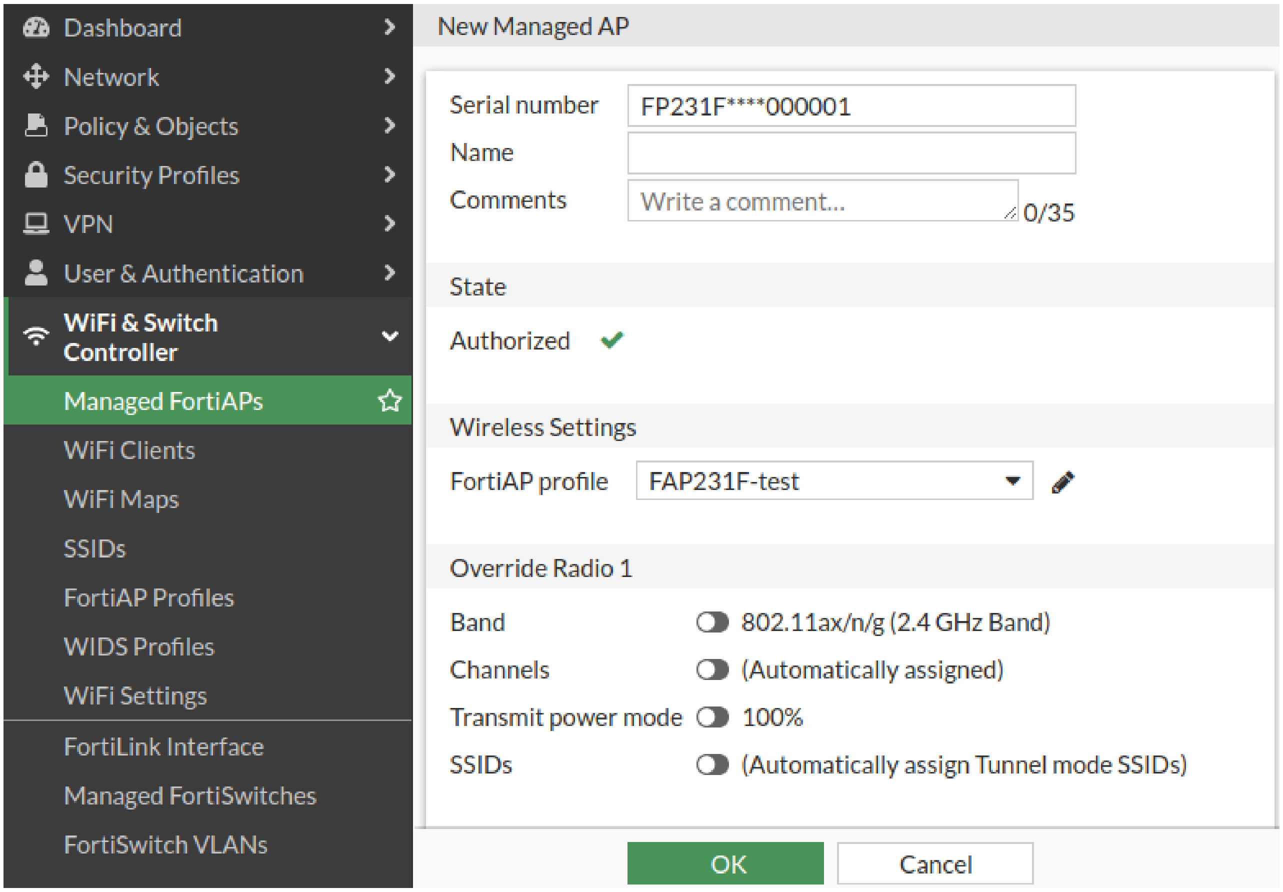
A Wildcard Serial Number consists of three parts:

- A six digit valid prefix for a FortiAP model, like "FP231F".
- Four "*" (asterisks) to indicate that the Serial Number is a Wildcard Serial Number.
- Six digits containing any valid characters. The characters do not need the match the actual Serial Number of the FortiAP you are registering.

  The last six digits enable you to create multiple profiles where each new FortiAP that registers adopt one of the wildcard SN profiles in order.

To configure a Wildcard Serial Number and pre-authorize a FortiAP - GUI:

1. Go to *WiFI & Switch Controller* > *Managed FortiAPs* and click *Create New* > *Managed AP*.
2. In *Serial number*, enter a Wildcard Serial Number (example "FP231F****000001").
3. Select a *FortiAP profile* you want to apply to the FortiAP.



New Managed AP

Serial number: FP231F****000001

Name:

Comments: Write a comment... 0/35

State

Authorized ✓

Wireless Settings

FortiAP profile: FAP231F-test

Override Radio 1

Band: 802.11ax/n/g (2.4 GHz Band)

Channels: (Automatically assigned)

Transmit power mode: 100%

SSIDs: (Automatically assign Tunnel mode SSIDs)

4. Click *OK* to save.
5. Connect the FortiAP unit to your topology.

   Once the FortiAP is discovered by FortiGate, FortiGate will try to find a matching Wildcard SN. When FortiGate finds a matching Wildcard SN, the template Serial Number is renamed to match the newly discovered physical FortiAP SN.
6. Go to *WiFI & Switch Controller* > *Managed FortiAPs* to verify that the FortiAP is pre-authorized.

To configure a Wildcard Serial Number and pre-authorize a FortiAP- CLI:

1. Pre-configure a Wildcard FortiAP SN (example "FP231F****000001").

   ```
    config wireless-controller wtp
     edit "FP231F****000001"
       set uuid 47ab50f8-5f7c-51ec-0a60-4ff00a3eba2e
       set admin enable
       set wtp-profile "FAP231F-test"
       config radio-1
       end
       config radio-2
       end
     next
   end
   ```

2. Connect the FortiAP unit to your topology.

   Once the FortiAP is discovered by FortiGate, FortiGate will try to find a matching Wildcard SN. When FortiGate finds a matching Wildcard SN, the template Serial Number is renamed to match the newly discovered physical FortiAP SN.

   ```
   FortiGate-80E-POE # diag debug enable
   FortiGate-80E-POE # diag debug cli 7
   Debug messages will be on for unlimited time.
   FortiGate-80E-POE # 0: config wireless-controller wtp
   0: rename "FP231F****000001" to "FP231FTF20026472"
   0: end
   ```

   The pre-configured template FortiAP SN is successfully renamed to match the FortiAP SN "FP231FTF20026472".

3. The new FortiAP is now pre-authorized and can be managed from the FortiGate without manual authorization. Note that the UUID does not change.

   ```
    config wireless-controller wtp
     edit "FP231FTF20026472"
       set uuid 47ab50f8-5f7c-51ec-0a60-4ff00a3eba2e
       set admin enable
       set wtp-profile "FAP231F-test"
       config radio-1
       end
       config radio-2
       end
     next
   end
   ```

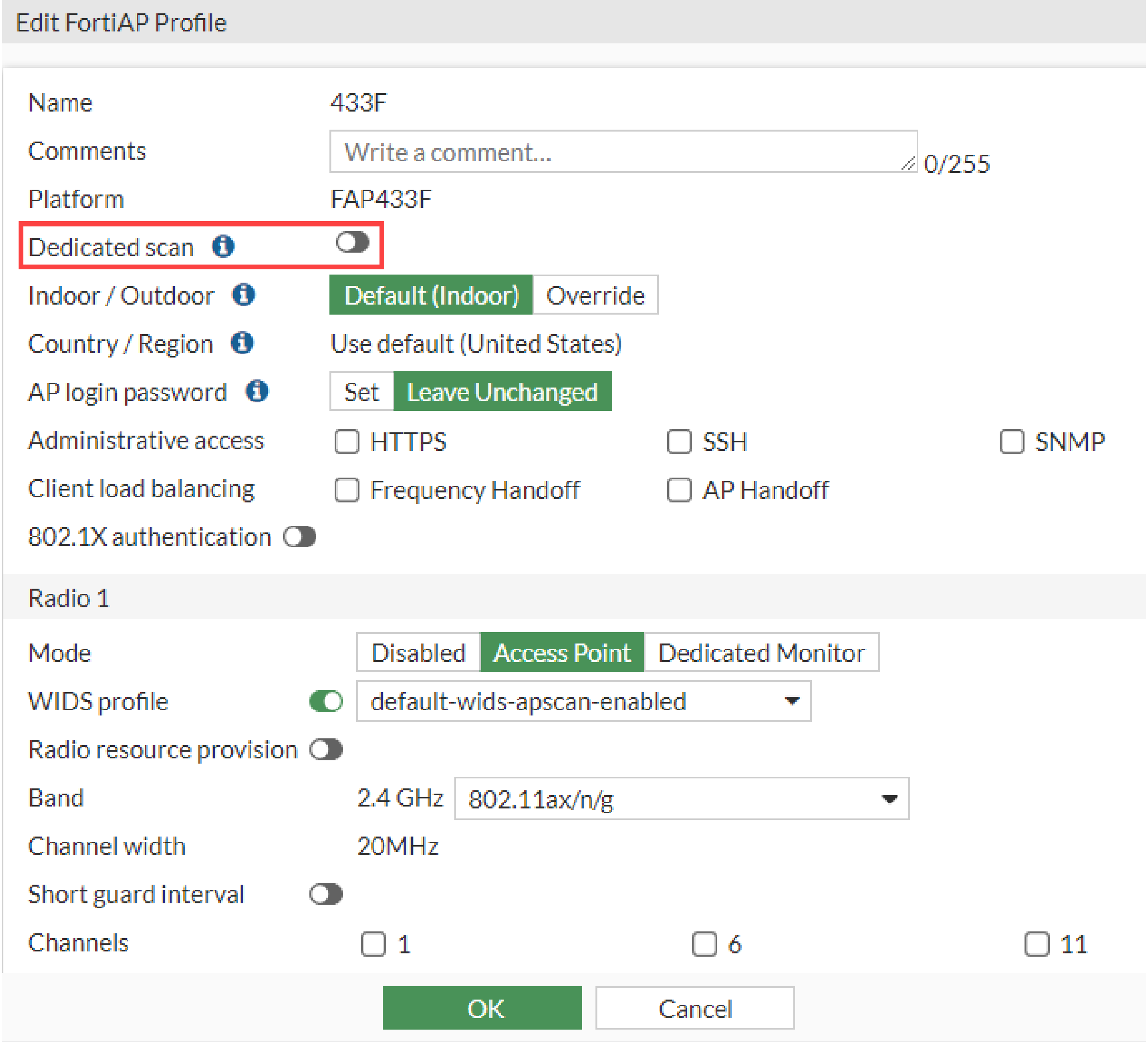
Disable dedicated scanning on FortiAP F-Series profiles

The FortiAP F-series product family supports two radios while a third radio performs dedicated scans at all times. However, due to wireless chipset limitations on the third radio, some of the data packets cannot be scanned, which may impact the detection capabilities for FortiPresence and other related solutions. You can disable dedicated scanning which then allows background scanning using WIDS profile to be enabled on Radios 1 and 2.

To disable dedicated scanning and enable background scanning - GUI:

1. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and select the FortiAP F-series profile you want to disable dedicated scanning for.

2. Disable *Dedicated scan*.



Edit FortiAP Profile

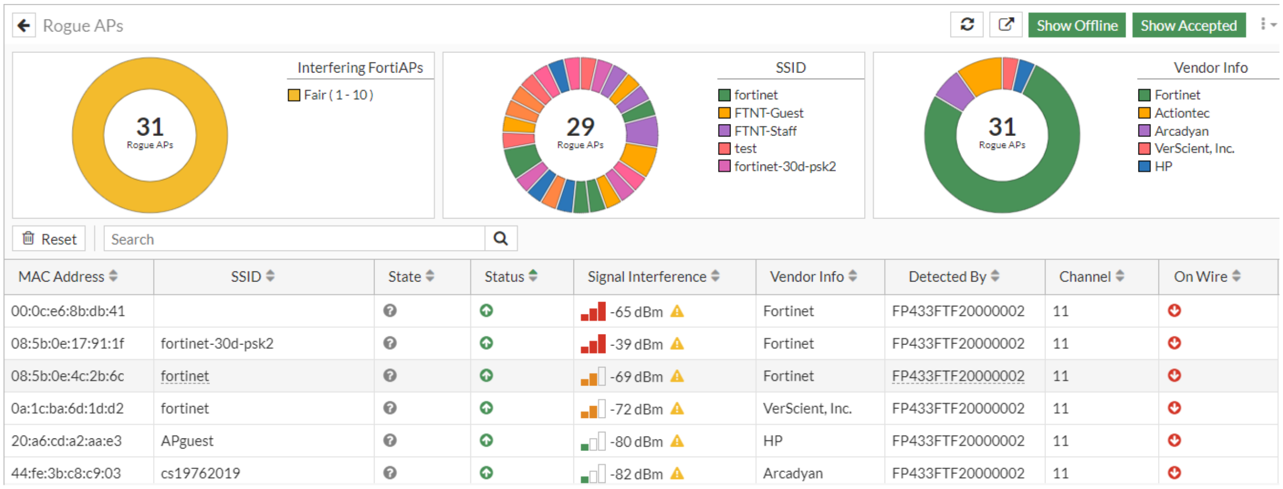
Name	433F
Comments	Write a comment... 0/255
Platform	FAP433F
Dedicated scan	○
Indoor / Outdoor	[✓ Default (Indoor)] Override
Country / Region	Use default (United States)
AP login password	Set [✓ Leave Unchanged]
Administrative access	□ HTTPS □ SSH □ SNMP
Client load balancing	□ Frequency Handoff □ AP Handoff
802.1X authentication	○

Radio 1

Mode	Disabled [✓ Access Point] Dedicated Monitor
WIDS profile	● default-wids-apscan-enabled
Radio resource provision	○
Band	2.4 GHz 802.11ax/n/g
Channel width	20MHz
Short guard interval	○
Channels	□ 1 □ 6 □ 11

After you disable *Dedicated scan*, the *WIDS profile* option becomes available under Radio 1 and Radio 2 configuration.

3. Set the *Mode* of the Radio to *Access Point*.
4. Enable *WIDS profile* and select a WIDS profile to perform background scanning.
5. Go to *Dashboard* > *WiFi* > *Rogue APs* to verify that the Rogue AP list is on the same channel as the Radio you configured.



MAC Address	SSID	State	Status	Signal Interference	Vendor Info	Detected By	Channel	On Wire
00:0c:e6:8b:db:41		?	⬆	-65 dBm ⚠	Fortinet	FP433FTF20000002	11	⬇
08:5b:0e:17:91:1f	fortinet-30d-psk2	?	⬆	-39 dBm ⚠	Fortinet	FP433FTF20000002	11	⬇
08:5b:0e:4c:2b:6c	fortinet	?	⬆	-69 dBm ⚠	Fortinet	FP433FTF20000002	11	⬇
0a:1c:ba:6d:1d:d2	fortinet	?	⬆	-72 dBm ⚠	VerScient, Inc.	FP433FTF20000002	11	⬇
20:a6:cd:a2:aa:e3	APguest	?	⬆	-80 dBm ⚠	HP	FP433FTF20000002	11	⬇
44:fe:3b:c8:c9:03	cs19762019	?	⬆	-82 dBm ⚠	Arcadyan	FP433FTF20000002	11	⬇

To disable dedicated scanning and enable background scanning - CLI:

When you create a new FortiAP F-series profile, dedicated scanning is automatically enabled.

1. Disable dedicated scanning and assign a WIDS profile:

```
config wireless-controller wtp-profile
  edit 433F
    config platform
      set type 433F
      set ddscan disable
    end
    set handoff-sta-thresh 55
    config radio-1
      set band 802.11ax,n,g-only
      set wids-profile "default-wids-apscan-enabled"
    end
    config radio-2
      set band 802.11ax-5G
      set wids-profile "default-wids-apscan-enabled"
    end
    config radio-3
      set mode disabled
    end
  next
end
```

2. Configure the WIDS profile to enable background scan:

```
config wireless-controller wids-profile
  edit "default-wids-apscan-enabled"
    set ap-scan enable
    set ap-bgscan-period 60
    set ap-bgscan-intv 1
    set ap-bgscan-duration 20
    set ap-bgscan-idle 0
  next
end
```

3. Assign the wtp-profile to a managed FortiAP:

```
config wireless-controller wtp
  edit "FP433FTF20000002"
    set uuid e3beadf4-6fdf-51ec-d2ed-cd489ee341cb
    set admin enable
    set wtp-profile "433F"
    config radio-1
    end
    config radio-2
    end
  next
end
```

4. Check managed FortiAP Channel and background scan status:

```
FortiGate-80E-POE # diag wire wlac -c wtp FP433FTF20000002
-------------------------------WTP    1----------------------------
WTP vd               : root
    vfid             : 0
    id               : FP433FTF20000002
    ...
  Radio 1            : AP
    ...
    bgscan oper    : enabled
      bgscan period  : oper 60 cfg 60
      bgscan intv    : 1
      bgscan dur     : 20
      bgscan idle    : 0
      bgscan rptintv : 30
    ...
  Radio 2            : AP
    ...
    bgscan oper    : enabled
      bgscan period  : oper 60 cfg 60
      bgscan intv    : 1
      bgscan dur     : 20
      bgscan idle    : 0
      bgscan rptintv : 30
    ...
-------------------------------Total    1 WTPs----------------------------
```

5. Check the Rogue AP list on FortiGate:

```
 FortiGate-80E-POE # diag wire wlac -c ap-rogue
CMWP AP: vf                  bssid ssid             ch  rate  sec
signal noise  age      sta mac                 wtp cnt     ici    bw sgi band

UNNN AP: 0       08:5b:0e:17:91:1f fortinet-30d-... 11  130   WPA2 Personal           -
39 -95    8        00:00:00:00:00:00       1   /1    56->0    20 0  11NGHT20

 N                FP433FTF20000002 fortinet-30d-... 11  130   WPA2 Personal           -
39 -95    8        10.43.1.18:25246-0  1
UNNN AP: 0       08:5b:0e:4c:2b:6c fortinet         11  130   WPA2 Personal           -
67 -95    18       00:00:00:00:00:00       1   /1    28->0    20 0  11NGHT20
```

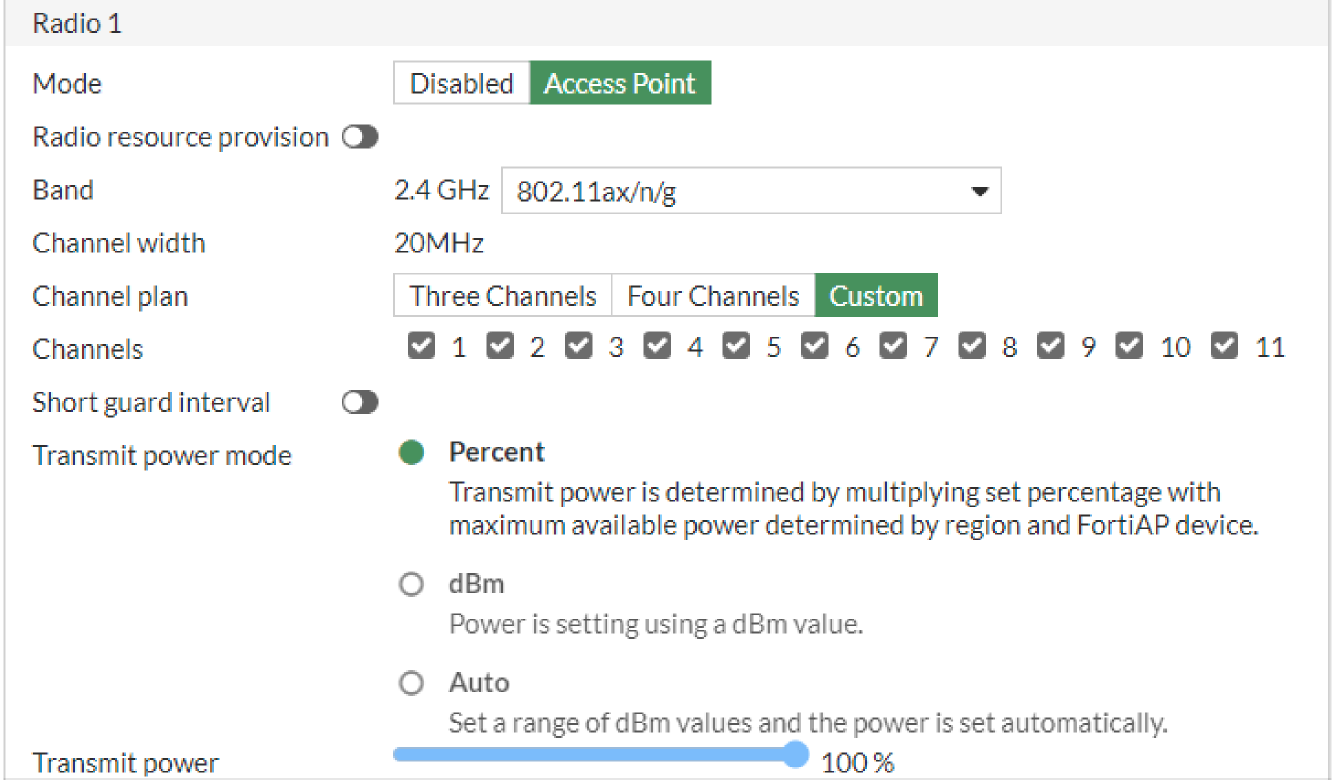
```
 N                 FP433FTF20000002 fortinet         11  130   WPA2 Personal          -
67 -95    18       10.43.1.18:25246-0  1
...
C - Configured  (G:accept, B:rogue, S:suppress, U:unconfigured)
M - AC managed  (V:vdom, C:AC, N:unmanaged)
W - On wire     (Y:yes, N:no)
P - Phishing    (F:fake, O:offending, N:no)
Total Rogue-AP:34 Rogue-AP-WTP(displayed):34 Rogue-AP-WTP(total):34
Total Entries: 34
```

Improve WiFi channel selection GUI

This GUI enhancement improves the channel selection for each of the 2.4GHz and 5GHz wireless radios. For 2.4GHz, you can select two default channel plans—Three Channels and Four Channels—to automatically configure non-overlapping channels. For 5.0GHz, a new slide-in page with improved visualization is added to help users select channels.

Selecting a channel for 2.4GHz wireless radios:

The following image shows the new *Channel Plan* field:



Radio 1

Mode: Disabled [✓ Access Point]

Radio resource provision: ○

Band: 2.4 GHz 802.11ax/n/g

Channel width: 20MHz

Channel plan: Three Channels | Four Channels | [✓ Custom]

Channels: ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11

Short guard interval: ○

Transmit power mode:
● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm
Power is setting using a dBm value.
○ Auto
Set a range of dBm values and the power is set automatically.

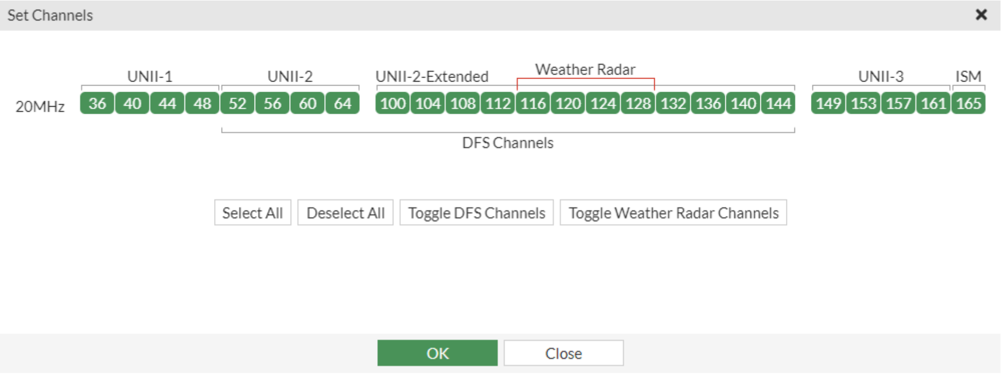
Transmit power: 100 %

You can select:

- *Three Channels* (automatically selects channel 1, 6, and 11),
- *Four Channels* (automatically selects channels 1, 4, 8, and 11), or
- *Custom* (select custom channels).

Selecting a channel for 5GHz wireless radios:

You can select channels for the 5GHz radio by clicking *Set Channels*. The following image shows the channel selector panel:



You can select individual channels or click *Toggle DFS Channels* and *Toggle Weather Radar Channels* to select/deselect those channels . The channel chart also shows channel availability for 40MHz or 80MHz channel-bonding.

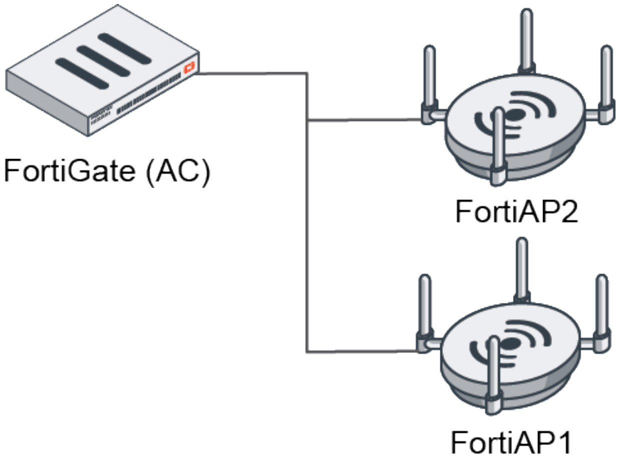
Support Layer 3 roaming for tunnel mode

This feature supports Layer 3 roaming between different VLANs and subnets on the same or different Wireless Controller. A client connected to the tunnel mode SSID on one FortiAP can roam to the same SSID on another FortiAP managed by the same or different FortiGate Wireless Controller, and continue to use the same IP. When the client idles longer than the `client-idle-rehome-timeout`, the client will rehome and receive an address on the new subnet from the new FortiAP.

Currently, this feature can only be configured using the CLI on the FortiGate Wireless Controllers.

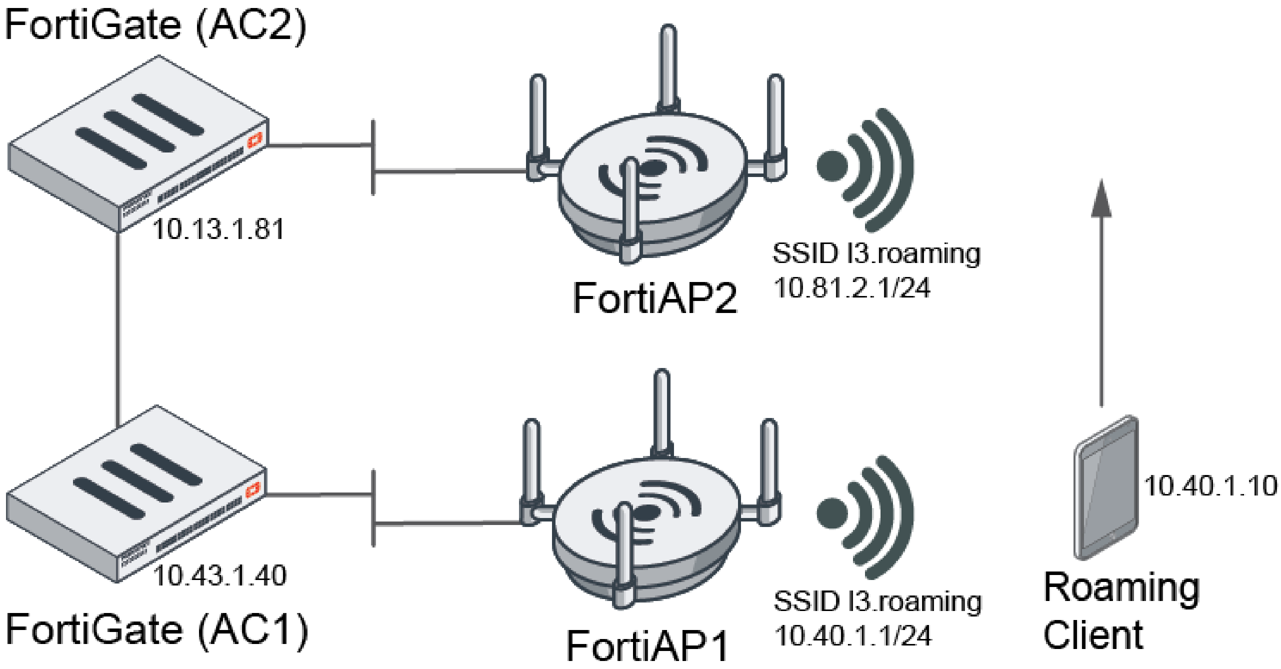
This feature supports two topologies:

- **L3 roaming intra-controller**
  In this example, there are two FortiAPs (FAP1 and FAP2) being managed by a controller. The FortiAPs are located on different floors of the same building. Each FAP is mapped to a different VLAN, but are on the same SSID. The client roams from FAP1 to FAP 2 and the L3 handoff is handled by the controller. The client maintains the same IP address.



- **L3 roaming inter-controller**

  In this example, there are two controllers (Controller1 and Controller2) each managing a FortiAP (FAP1 and FAP2) respectively. The L3 client roams from Controller1's FAP1 to Controller 2's FAP2. Both FAPs have the same SSID, and each FAP has the SSID tied to a different VLAN. The client roams between the two FAPs and the L3 handoff is handled by Controller1 and Controller2's mobility tunnel. The client maintains the same IP address.



Configuring L3 Roaming for Tunnel Mode SSIDs

To configure Intra-Controller L3 roaming - CLI:

1. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

2. configure the L3 roaming support SSID:

```
config wireless-controller vap
  edit "l3_rm1"
    set ssid "l3.roaming"
    set passphrase ENC
    set schedule "always"
    set l3-roaming enable
  next
end
config system interface
  edit "l3_rm1"
    set vdom "root"
    set ip 10.40.1.1 255.255.255.0
    set allowaccess ping
    set type vap-switch
    set role lan
    set snmp-index 18
  next
end
```

3. Assign L3 roaming VAP to FAP433F:

```
config wireless-controller wtp-profile
  edit "433F"
    config platform
      set type 433F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11ax-5G
      set power-mode dBm
      set power-value 1
      set channel "36"
      set vap-all manual
      set vaps "13_rm1"
    end
    config radio-3
      set mode monitor
    end
  next
end
config wireless-controller wtp
  edit "FP433FXX00000000"
    set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
    set admin enable
    set wtp-profile "433F"
    config radio-2
    end
  next
end
```

4. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
  edit "831F"
    config platform
      set type 831F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11ax-5G
      set channel "36" "40"
      set vap-all manual
      set vaps "13_rm1"
    end
    config radio-3
      set mode disabled
    end
  next
end
config wireless-controller wtp
  edit "FP831FXX00000000"
    set uuid 23ed4966-af92-51ec-44e8-3c1318698661
    set admin enable
    set wtp-profile "831F"
    config radio-2
    end
  next
end
```

To configure Inter-Controller L3 roaming - CLI:

This configuration requires two FortiGate units. In order to enable L3 roaming supported VAP, both FortiGate units must have the same SSID, security, and passphrase.

The following example uses:

- AC1 as FGT40F
  - FAP1 as FAP433E
- AC2 as FGT81EP
  - FAP2 as FAP831F

1. Configure the L3 roaming peer IP for AC1 (FGT-40F):

   ```
   config system interface
     edit "wan"
       set vdom "root"
       set ip 10.43.1.40 255.255.255.0
       set allowaccess ping https ssh http fabric
       set type physical
       set role wan
       set snmp-index 1
     next
   end
   config wireless-controller inter-controller
   ```

```
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.81
    next
  end
end
```

a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

   ```
   config wireless-controller timers
     set client-idle-rehome-timeout 20
   end
   ```

b. configure the L3 roaming support SSID:

   ```
   config wireless-controller vap
     edit "l3_rm1"
       set ssid "l3.roaming"
       set passphrase ENC
       set schedule "always"
       set l3-roaming enable
     next
   end
   config system interface
     edit "l3_rm1"
       set vdom "root"
       set ip 10.40.1.1 255.255.255.0
       set allowaccess ping
       set type vap-switch
       set role lan
       set snmp-index 18
     next
   end
   ```

c. Assign L3 roaming VAP to FAP433F:

   ```
   config wireless-controller wtp-profile
     edit "433F"
       config platform
         set type 433F
         set ddscan enable
       end
       set handoff-sta-thresh 55
       set allowaccess ssh
       config radio-1
         set mode disabled
       end
       config radio-2
         set band 802.11ax-5G
         set power-mode dBm
         set power-value 1
         set channel "36"
         set vap-all manual
         set vaps "13_rm1"
       end
       config radio-3
         set mode monitor
   ```

```
        end
      next
    end
    config wireless-controller wtp
      edit "FP433FXX00000000"
        set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
        set admin enable
        set wtp-profile "433F"
        config radio-2
        end
      next
    end
```

2. Configure the L3 roaming peer IP for AC2 (FGT-81EP):

```
config system interface
  edit "wan"
    set vdom "root"
    set ip 10.43.1.81 255.255.255.0
    set allowaccess ping https ssh http fabric
    set type physical
    set role wan
    set snmp-index 1
  next
end
config wireless-controller inter-controller
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.40
    next
  end
end
```

   a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

   b. configure the L3 roaming support SSID:

```
config wireless-controller vap
  edit "l3_rm1"
    set ssid "l3.roaming"
    set passphrase ENC
    set schedule "always"
    set l3-roaming enable
  next
end
config system interface
  edit "l3_rm1"
    set vdom "root"
    set 10.81.2.1 255.255.255.0
    set allowaccess ping speed-test
    set type vap-switch
    set role lan
    set snmp-index 23
  next
end
```

c. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
  edit "831F"
    config platform
      set type 831F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11ax-5G
      set channel "36" "40"
      set vap-all manual
      set vaps "l3_rm1"
    end
    config radio-3
      set mode disabled
    end
  next
end
config wireless-controller wtp
  edit "FP831FXX00000000"
    set uuid 23ed4966-af92-51ec-44e8-3c1318698661
    set admin enable
    set wtp-profile "831F"
    config radio-2
    end
  next
end
```

3. Check the peer status from AC1 (FGT-40F):

```
FortiGate-40F  # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
    peer cnt: 1
              FG81EPXX00000000 10.43.1.81:5246       UP 2
```

4. Check the peer status from AC2 (FGT-81EP):

```
FortiGate-81E-POE # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
    peer cnt: 1
              FGT40FXX00000000 10.43.1.40:5246       UP 3
```

Understanding L3 roaming events for inter-controller L3 roaming for a tunnel mode SSID

When the wireless client is connected with "l3.roaming" on AP1 in AC1, the client receives IP 10.40.1.10 from AP1 in AC1:

```
FortiGate-40F # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=2 rId=2 wlan=l3_rm1 vlan_id=0 ip=10.40.1.10 ip6=fe80::7766:7ffe:ee4d:c396
mac=a4:c3:f0:6d:69:33 vci= host=test-wifi user= group= signal=-65 noise=-95 idle=1 bw=3
use=7 chan=36 radio_type=11AC(wave2) security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no l3r=1,1 10.43.1.81:5247 -- 10.43.1.40:5247 33,0 online=yes mimo=2
```

When the client leaves AP1 and roams towards AP2, it connects with the same SSID "l3.roaming" on AP2. Wireless traffic passed from AP2 and is sent to AC2. Eventually the wireless traffic is transferred from AC2 to AC1 and traffic is maintained from AC1. The wireless client maintains the original IP of 10.40.1.10:

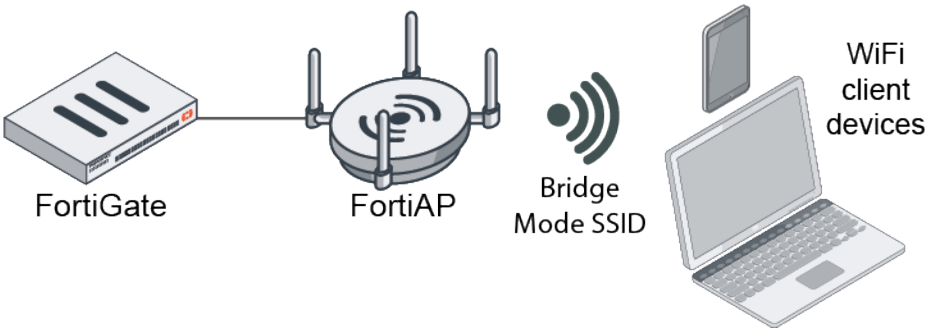
```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=3 rId=2 wlan=l3_rm1 vlan_id=0 ip=10.40.1.10 ip6=:: mac=a4:c3:f0:6d:69:33 vci=
host= user= group= signal=-66 noise=-95 idle=0 bw=2 use=7 chan=36 radio_type=11AC(wave2)
security=wpa2_only_personal mpsk= encrypt=aes cp_authed=no l3r=0,1 0.0.0.0:0 -- 0.0.0.0:0
0,0 online=yes mimo=2
```

If the wireless client idle time exceeds `client-idle-rehome-timeout`, it triggers the rehome event. The wireless client will send a DHCP request and obtain a new IP address from AC2 (10.81.2.20). Now the wireless client traffic is maintained from AC2:

```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=3 rId=2 wlan=l3_rm1 vlan_id=0 ip=10.81.2.20 ip6=:: mac=a4:c3:f0:6d:69:33 vci=
host=test-wifi user= group= signal=-65 noise=-95 idle=0 bw=0 use=6 chan=36 radio_type=11AC
(wave2) security=wpa2_only_personal mpsk= encrypt=aes cp_authed=no l3r=1,0 0.0.0.0:0 --
0.0.0.0:0 0,0 online=yes mimo=2
```

Report wireless client app usage for clients connected to bridge mode SSIDs

This feature enhances the CLI command "`diagnose wireless-controller wlac -d sta online`" to include application usage data for each wireless client connected to a bridge mode SSID. FortiGate receives the wireless client application information from FortiAPs and analyzes the traffic information on each application.



FortiAP is updated to capture application information of wireless client traffic passing through it when this feature has been configured; it requires managed FortiAPs to run firmware version 7.2.0 and later.

The following CLI commands have been added under `config wireless-controller vap`:

- `set application-detection enable | disable`: Enable or disable the reporting of wireless client application information for the bridge mode SSID that it is configured for. Application reporting is disabled by default.
- `set application-report-intv <seconds>`: Configure the time interval for the FortiAP to collect and report the application traffic information to the FortiGate. The default interval is 120 seconds.

To enable application-detection in VAP:

```
config wireless-controller vap
  edit "vap-ndpi"
    set ssid "SSID_NDPI"
    set passphrase ENC
    set local-bridging enable
    set schedule "always"
    set application-detection-engine enable
    set application-report-intv 60
  next
end
```

To check the application detection attribute from FortiAP:

```
FortiAP-231F # vcfg
-------------------------------VAP Configuration    1----------------------------
Radio Id  1 WLAN Id  0 SSID_NDPI ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown (-1)
           vlanid=0, intf=wlan10, vap=0x3db5702c, bssid=e0:23:ff:d7:74:b0
           11ax high-efficiency=enabled target-wake-time=enabled
           bss-color-partial=enabled
           mesh backhaul=disabled
           local_auth=disabled standalone=disabled nat_mode=disabled
           local_bridging=enabled split_tunnel=disabled
           intra_ssid_priv=disabled
           mcast_enhance=disabled igmp_snooping=disabled
           mac_auth=disabled fail_through_mode=disabled sta_info=1/0
           mac=local, tunnel=8023, cap=8ce0, qos=disabled
           prob_resp_suppress=disabled
           rx sop=disabled
           sticky client remove=disabled
           mu mimo=enabled           ldpc_config=rxtx
           dhcp_option43_insertion=enabled           dhcp_option82_insertion=disabled
           dhcp_enforcement=disabled
           access_control_list=disabled
           bc_suppression=dhcp dhcp-ucast arp
           auth=WPA2, PSK, AES WPA keyIdx=1, keyLen=16, keyStatus=1, gTsc=000000000000
           key=f4cf7fd6 32dbced5 6d9fb25c 8894ad9b
           pmf=disable
           okc=disabled, dynamic_vlan=disabled, extern_roaming=disabled
           voice_ent(802.11kv)=disabled, fast_bss_trans(802.11r)=disabled mbo=disabled
           port_macauth=disable
           airfairness weight: 20%
           schedules=SMTWTFS 00:00->00:00,
           ratelimit(Kbps): ul=0 dl=0 ul_user=0 dl_user=0 burst=disabled
           primary wag:
           secondary wag:
           application detection engine: enabled, report-interval=60, configured
-------------------------------Total    1 VAP Configurations----------------------------
```

To check the application detection information from FortiAP:

```
FortiAP-231F # cw_diag -d ndpi sta


Station 00:c0:ca:87:07:50 flow stats list:
-----------------------------------------------------------------------------
 AID  TX total   TX new     RX total   RX new     Application/Protocol Name
----- ---------- ---------- ---------- ---------- ---------------------------
    0      992 B        0 B   3.821 KB        0 B ukn
    7   2.056 KB        0 B   1.888 KB        0 B twitter
   12      342 B        0 B       62 B        0 B icloud
   28  68.553 KB   7.416 KB  11.400 KB   3.879 KB youtube
  139   6.281 KB        0 B   1.841 KB        0 B yahoo
  609   4.847 KB        0 B   1.734 KB        0 B new-relic
  632  20.167 KB        0 B   4.310 KB        0 B google-services
  664   6.080 KB        0 B  13.842 KB        0 B microsoft-services
  728  18.324 KB        0 B  12.785 KB        0 B amazon-services
  765   2.031 MB        0 B 345.697 KB        0 B service_amazon
  768  70.786 KB  70.497 KB   7.094 KB   7.031 KB service_google
  786   3.927 KB        0 B   1.992 KB        0 B service_microsoft
  866   5.842 KB        0 B   2.656 KB        0 B spotxchange
  889      359 B        0 B       63 B        0 B goodreads
 1032      480 B      480 B       58 B       58 B imdb
 1090  23.201 KB        0 B   7.608 KB        0 B adobeanalytics
 1141   7.160 KB        0 B   2.030 KB        0 B casale
 1218   5.226 KB        0 B   2.002 KB        0 B rubiconproject
 1397   5.411 KB   5.411 KB   1.938 KB   1.938 KB exelate
 1788  25.110 KB  25.110 KB   6.503 KB   6.503 KB bing
 1838  12.417 KB  12.417 KB   2.830 KB   2.830 KB delicious
 1861   6.106 KB   6.106 KB   2.008 KB   2.008 KB pubmatic
 1968      753 B        0 B      406 B        0 B http
 1974  11.720 KB  11.375 KB   1.826 KB   1.757 KB dns
 1979 475.727 KB        0 B  66.211 KB        0 B ssl
 2012      357 B        0 B        0 B        0 B dhcp
 2182   1.033 MB        0 B 152.760 KB        0 B quic
-----------------------------------------------------------------------------
```

To check the application detection information from FortiGate:

```
FortiGate-201E # diag wire wlac -d sta online
   vf=0 wtp=3 rId=2 wlan=vap-ndpi vlan_id=0 ip=10.132.132.11 ip6=fe80::90bf:3f23:991:c8d4
mac=00:c0:ca:87:07:50 vci=MSFT 5.0 host=DESKTOP-CJ6F7M2 user= group= signal=-42 noise=-95
idle=0 bw=4158 use=6 chan=36 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes
cp_authed=no l3r=1,0 0.0.0.0:0 -- 0.0.0.0:0 0,0 online=yes mimo=2
                ip6=*fe80::90bf:3f23:991:c8d4,57,
Id 0 App:ukn
Tx:992 Rx:2466 Age:9
Id 28 App:youtube
Tx:60614 Rx:7460 Age:9
Id 609 App:new-relic
Tx:4847 Rx:1734 Age:9
Id 632 App:google-services
Tx:8521 Rx:2404 Age:9
Id 765 App:service_amazon
Tx:4057 Rx:18035 Age:9
```

```
Id 1979 App:ssl
Tx:474313 Rx:64787 Age:9
Id 2182 App:quic
Tx:1028073 Rx:138326 Age:9
Id 1090 App:adobeanalytics
Tx:23201 Rx:7608 Age:9
Id 1141 App:casale
Tx:7160 Rx:2030 Age:9
Id 1218 App:rubiconproject
Tx:5226 Rx:2002 Age:9
```

Support enabling or disabling 802.11d - 7.2.1

This enhancement adds the ability to toggle 802.11d support for 2.4 GHz radios through a FortiAP profile. In previous versions, 802.11d was always enabled on FortiAPs. When 802.11d is enabled, the FortiAPs broadcast the country code in beacons, probe responses, and probe requests. This led to some older legacy clients failing to associate to the FortiAP. The ability to disable 802.11d prevents the broadcasting of country code settings and provides backwards compatibility with those clients.

Since IEEE 802.11d only applies to 2.4 GHz radios operating in the 802.11g band, disabling 802.11d only applies to radios configured to operate in the 802.11g band.

To disable 802.11d:

```
config wireless-controller wtp-profile
  edit FAP231F-default
    config radio-1
    set 80211d disable
  end
end
```

To verify the configuration from FortiGate:

1. From the FortiGate:

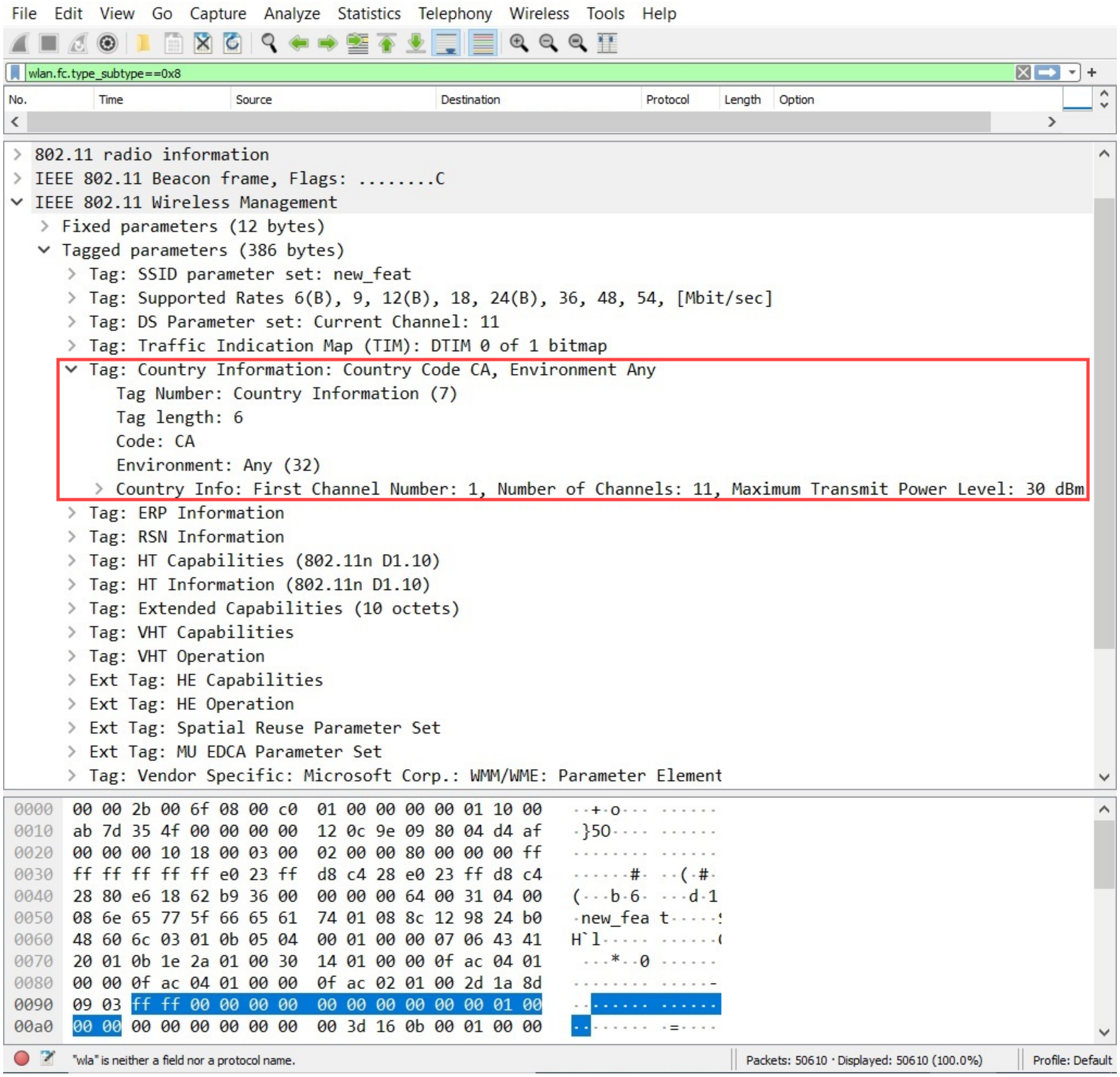
   ```
   diagnose wireless-controller wlac -c wtp FP231FTF20007509 | grep 80211d
      80211d enable : disabled
   ```

2. When the previous FortiGate setting are applied to a Managed FortiAP, the settings can be verified on the FortiAP CLI through the `rcfg` and `iwpriv` commands:

   ```
   FortiAP-231F # rcfg | grep 802
      802.11d enable : disabled
   FortiAP-231F #

   Check iwpriv

   FortiAP-231F # iwpriv wlan00 get_countryie
   wlan00 get_countryie:0 (0x0)
   FortiAP-231F #
   ```

3. Sniff the packets in the air before and after disabling the feature:

a. Before enabling the feature, use a packet analyzer to check the sample beacon packet for the *Country Information* Tag in *Tagged parameters.*

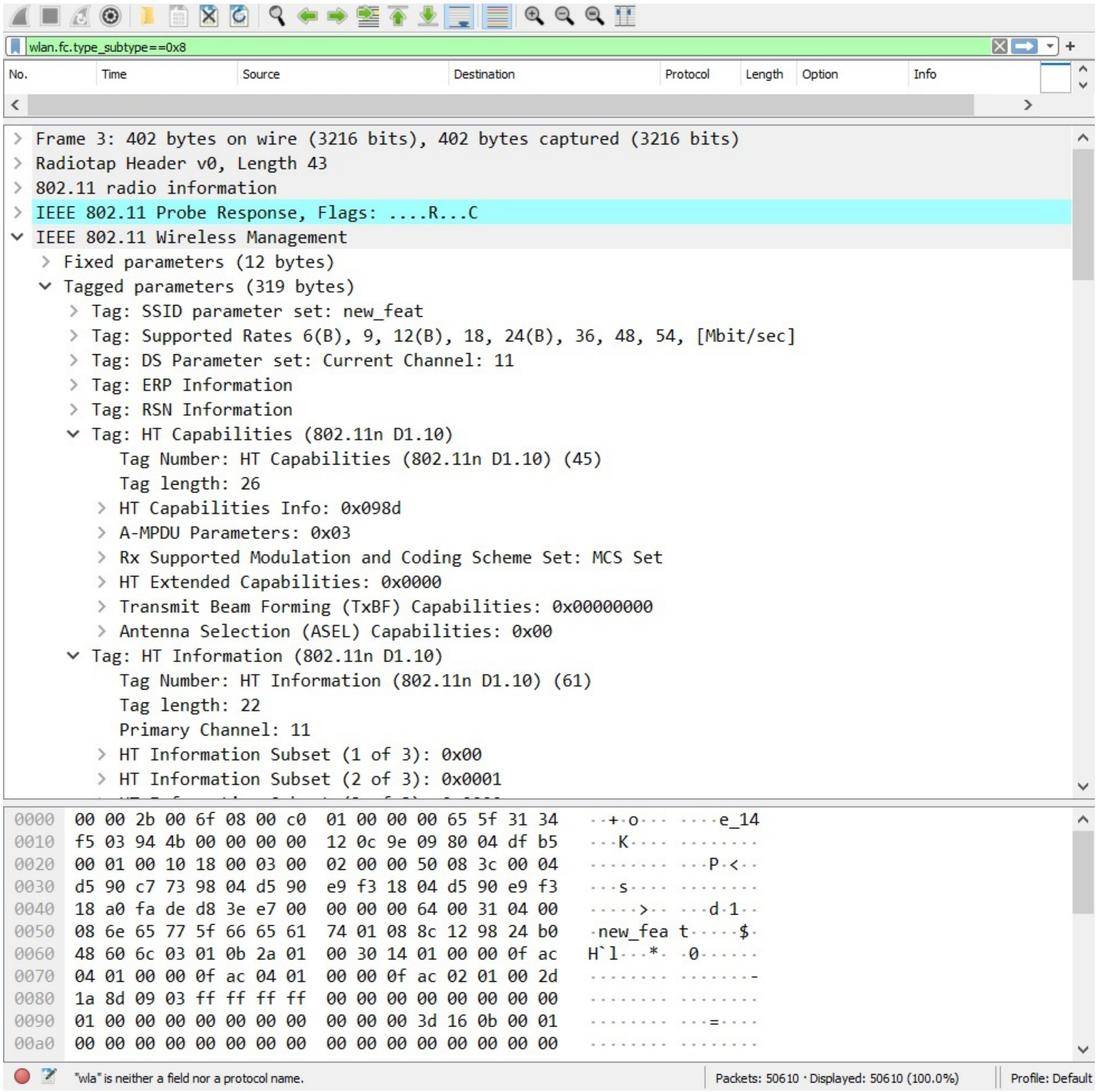

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.fc.type_subtype==0x8
No. Time Source Destination Protocol Length Option

```
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (386 bytes)
    > Tag: SSID parameter set: new_feat
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 11
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    v Tag: Country Information: Country Code CA, Environment Any
        Tag Number: Country Information (7)
        Tag length: 6
        Code: CA
        Environment: Any (32)
      > Country Info: First Channel Number: 1, Number of Channels: 11, Maximum Transmit Power Level: 30 dBm
    > Tag: ERP Information
    > Tag: RSN Information
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (10 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Ext Tag: HE Capabilities
    > Ext Tag: HE Operation
    > Ext Tag: Spatial Reuse Parameter Set
    > Ext Tag: MU EDCA Parameter Set
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

```
0000  00 00 2b 00 6f 08 00 c0  01 00 00 00 00 01 10 00   ··+·o··· ······
0010  ab 7d 35 4f 00 00 00 00  12 0c 9e 09 80 04 d4 af   ·}5O···· ······
0020  00 00 00 10 18 00 03 00  02 00 00 80 00 00 00 ff   ········ ······
0030  ff ff ff ff ff e0 23 ff  d8 c4 28 e0 23 ff d8 c4   ······#· ··(·#·
0040  28 80 e6 18 62 b9 36 00  00 00 00 64 00 31 04 00   (···b·6· ···d·1
0050  08 6e 65 77 5f 66 65 61  74 01 08 8c 12 98 24 b0   ·new_fea t·····$
0060  48 60 6c 03 01 0b 05 04  00 01 00 00 07 06 43 41   H`l····· ······C
0070  20 01 0b 1e 2a 01 00 30  14 01 00 00 0f ac 04 01    ···*··0 ······
0080  00 00 0f ac 04 01 00 00  0f ac 02 01 00 2d 1a 8d   ········ ·····-
0090  09 03 ff ff 00 00 00 00  00 00 00 00 00 00 01 00   ········ ······
00a0  00 00 00 00 00 00 00 00  00 3d 16 0b 00 01 00 00   ········ ·=····
```

"wla" is neither a field nor a protocol name. | Packets: 50610 · Displayed: 50610 (100.0%) | Profile: Default

b. After disabling the 802.11d on a 2.4Ghz radio, use a packet analyzer to check the beacon and verify that the *Country Information* Tag is no longer under in *Tagged Parameters.*



```
wlan.fc.type_subtype==0x8
```

```
> Frame 3: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits)
> Radiotap Header v0, Length 43
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: ....R...C
v IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)
    v Tagged parameters (319 bytes)
        > Tag: SSID parameter set: new_feat
        > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
        > Tag: DS Parameter set: Current Channel: 11
        > Tag: ERP Information
        > Tag: RSN Information
        v Tag: HT Capabilities (802.11n D1.10)
              Tag Number: HT Capabilities (802.11n D1.10) (45)
              Tag length: 26
            > HT Capabilities Info: 0x098d
            > A-MPDU Parameters: 0x03
            > Rx Supported Modulation and Coding Scheme Set: MCS Set
            > HT Extended Capabilities: 0x0000
            > Transmit Beam Forming (TxBF) Capabilities: 0x00000000
            > Antenna Selection (ASEL) Capabilities: 0x00
        v Tag: HT Information (802.11n D1.10)
              Tag Number: HT Information (802.11n D1.10) (61)
              Tag length: 22
              Primary Channel: 11
            > HT Information Subset (1 of 3): 0x00
            > HT Information Subset (2 of 3): 0x0001
```

```
0000  00 00 2b 00 6f 08 00 c0  01 00 00 00 65 5f 31 34   ··+·o···  ····e_14
0010  f5 03 94 4b 00 00 00 00  12 0c 9e 09 80 04 df b5   ···K····  ········
0020  00 01 00 10 18 00 03 00  02 00 00 50 08 3c 00 04   ········  ···P·<··
0030  d5 90 c7 73 98 04 d5 90  e9 f3 18 04 d5 90 e9 f3   ···s····  ········
0040  18 a0 fa de d8 3e e7 00  00 00 00 64 00 31 04 00   ·····>··  ···d·1··
0050  08 6e 65 77 5f 66 65 61  74 01 08 8c 12 98 24 b0   ·new_fea  t·····$·
0060  48 60 6c 03 01 0b 2a 01  00 30 14 01 00 00 0f ac   H`l···*·  ·0······
0070  04 01 00 00 0f ac 04 01  00 00 0f ac 02 01 00 2d   ········  ·······-
0080  1a 8d 09 03 ff ff ff ff  00 00 00 00 00 00 00 00   ········  ········
0090  01 00 00 00 00 00 00 00  00 00 00 3d 16 0b 00 01   ········  ···=····
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
```

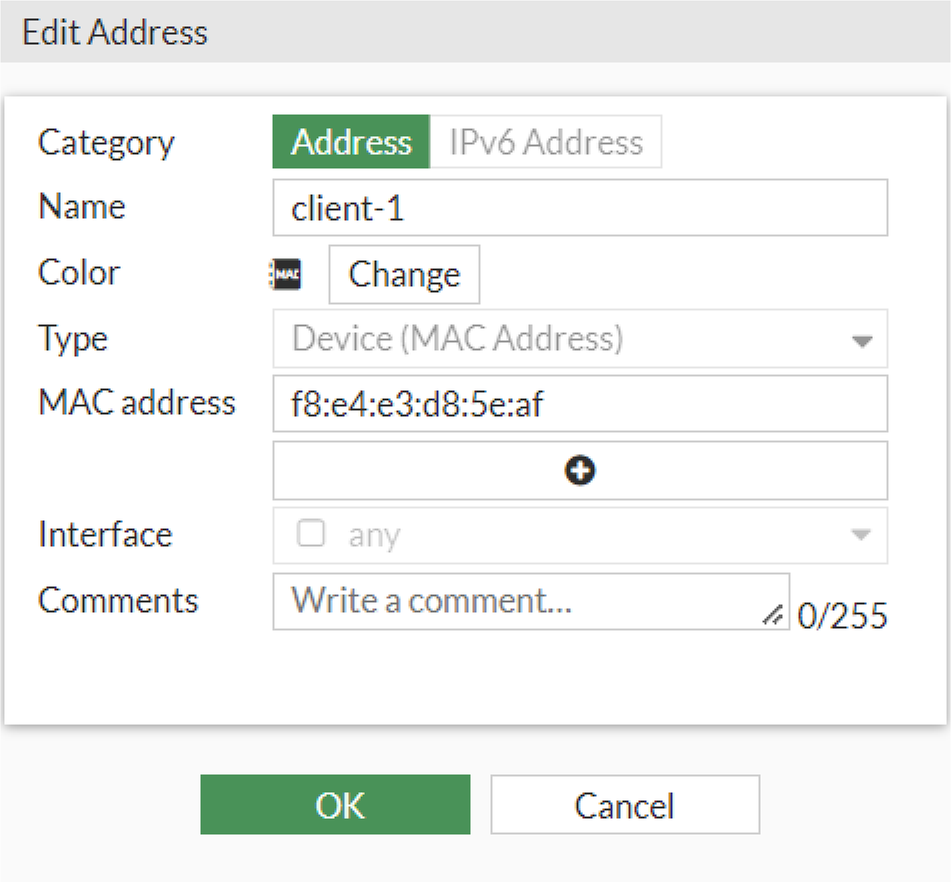
"wla" is neither a field nor a protocol name. | Packets: 50610 · Displayed: 50610 (100.0%) | Profile: Default

Improve MAC address filtering - 7.2.1

This enhancement adds GUI support for configuring MAC address filters in the *WiFi & Switch Controller* > *SSIDs* page and introduces a new `address-group-policy` command that applies MAC filters directly from the SSID. Using address groups, you can choose if you want to permit or exclude clients based on their MAC addresses.

To create and apply a MAC address filter - GUI:

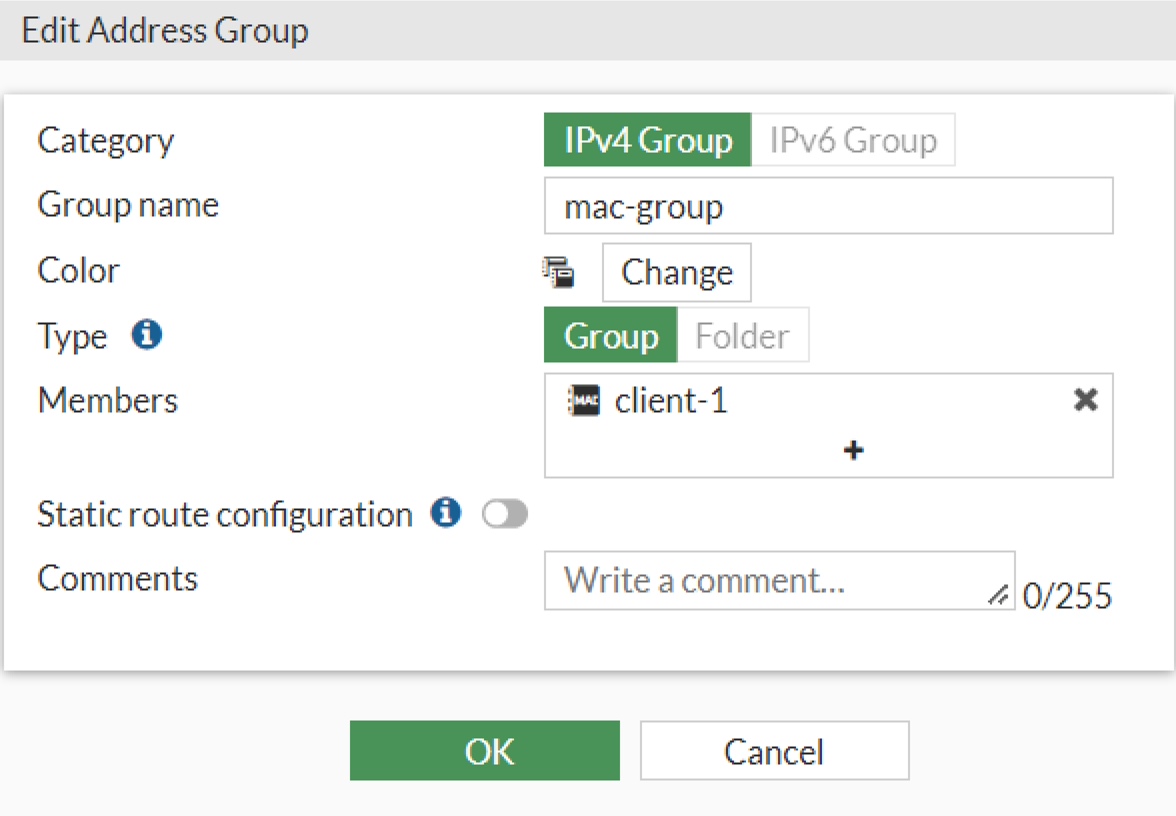
1. Go to *Policy & Objects* > *Addresses* and select *Create New* > *Address*.
2. Name the address and set the *Type* as *Device (MAC Address)*.
3. Enter the *MAC address(es)* you want to filter.



Edit Address

Category	Address | IPv6 Address
Name	client-1
Color	Change
Type	Device (MAC Address)
MAC address	f8:e4:e3:d8:5e:af
Interface	□ any
Comments	Write a comment... 0/255

4. When you are finished, click *OK*.
5. Go to *Policy & Objects* > *Addresses* and select *Create New* > *Address Group*.
6. Name the address group
7. Click *Members* and select the address you created earlier.



Edit Address Group

Category: [✓ IPv4 Group] IPv6 Group

Group name: mac-group

Color: Change

Type: [✓ Group] Folder

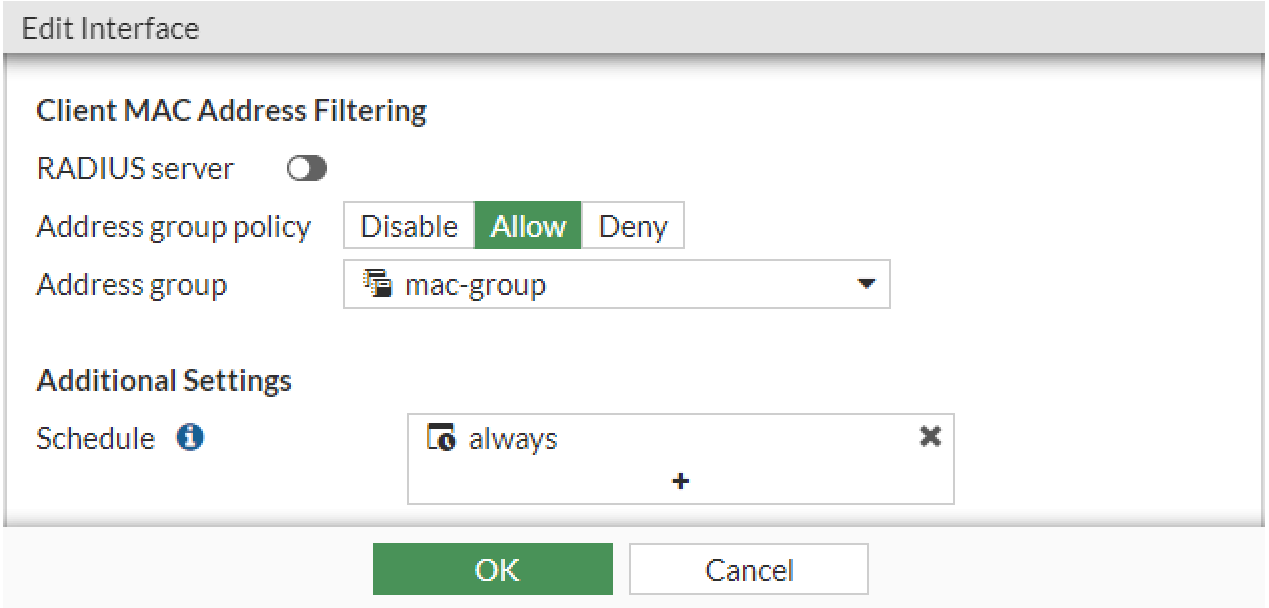
Members: client-1

Static route configuration ○

Comments: Write a comment... 0/255

OK Cancel

8. When you are finished, click *OK*.
9. Go to *WiFi & Switch Controller > SSIDs* and select the SSID you want to apply the filter to.
10. Locate *Client MAC Address Filtering* and select an *Address group policy*:
    - *Disable*: Disable MAC address filtering policy for MAC addresses that are in the address group. This is the default.
    - *Allow*: Permit clients with MAC addresses that are in the address group.
    - *Deny*: Deny clients with MAC addresses that are in the address group.
11. Select the *Address group* you created.



Edit Interface

Client MAC Address Filtering

RADIUS server ○

Address group policy: Disable [✓ Allow] Deny

Address group: mac-group

Additional Settings

Schedule: always

12. When you are finished, click *OK*.
    The SSID now accepts or denies the address group you configured.

To create and apply a MAC address filter - CLI:

1. Create the firewall address entry and set the `type` to `mac`:

```
 config firewall address
  edit "client-1"
    set uuid f35b2080-a199-51ec-7d97-00495859217e
    set type mac
    set macaddr "f8:e4:e3:d8:5e:af"
  next
end
```

2. Create a firewall address group and select the address entry you just created.

```
 config firewall addrgrp
  edit "mac-group"
    set uuid 26260750-a19a-51ec-b054-b385dab00c07
    set member "client-1"
  next
end
```

3. Under a wireless vap interface, there is a new `address-group-policy` option to help control the mac filter function.
   - To allow the connection, select the created `address-group` and set the `address-group-policy` to `allow`:

```
config wireless-controller vap
  edit "wifi.fap.01"
    set ssid "ExampleSSID"
    set passphrase ENC *
    set schedule "always"
    set address-group "mac-group"
```

```
        set address-group-policy allow
      next
    end
```

- To deny the connection, select the created `address-group` and set the `address-group-policy` to `deny`:

```
config wireless-controller vap
    edit "wifi.fap.02"
        set ssid "ExampleSSID"
        set passphrase ENC *
        set schedule "always"
        set address-group "mac-group"
        set address-group-policy deny
    next
end
```

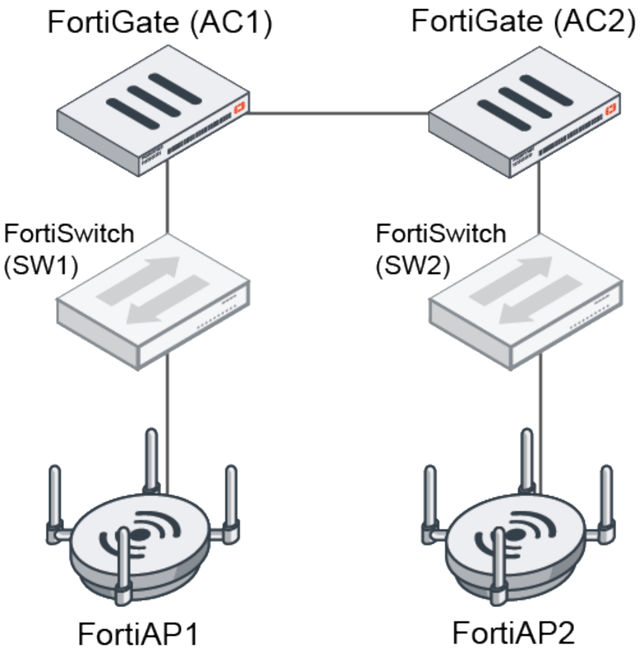
Support Layer 3 roaming for bridge mode - 7.2.1

Support for Layer 3 roaming with tunnel mode SSIDs was added in FortiOS 7.2.0. FortiOS 7.2.1 expands support to bridge mode SSIDs. For more information on Layer 3 roaming and supported topologies, see Support Layer 3 roaming for tunnel mode on page 470.

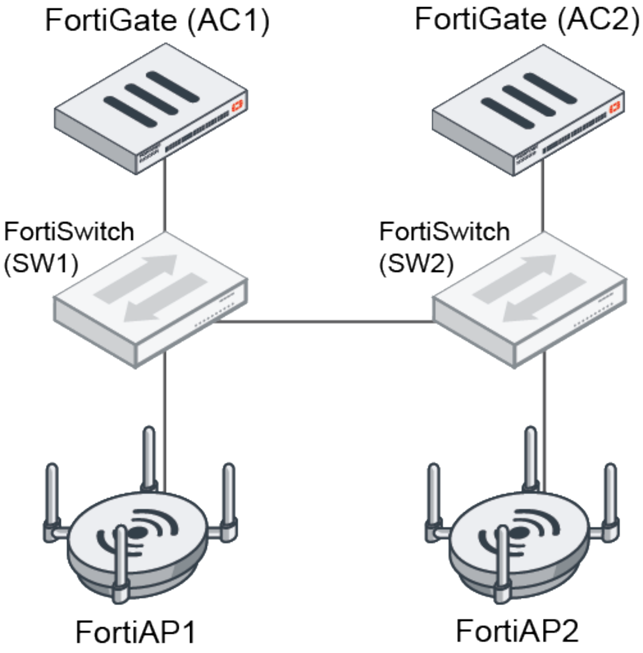
A client connected to the bridge mode SSID on one FortiAP can roam to the same SSID on another FortiAP managed by the same or different FortiGate Wireless Controller, and continue to use the same IP. When the client idles longer than the `client-idle-rehome-timeout`, then the client will rehome and receive an address on the new subnet from the new FortiAP.

For the L3 roaming inter-controller topology, bridge mode SSIDs support two Layer 3 roaming modes: indirect and direct.

- **Indirect Mode**
  In indirect mode, the L3 handoff is handled by the mobility tunnel between the FortiGate Wireless Controllers.



- **Direct Mode**
  In direct mode, the two FortiAPs must be able to reach each other with no NAT in the path and the L3 handoff occurs between the FortiAPs directly.



Note: Direct mode is preferred when feasible.

Configuring L3 Roaming for Bridge Mode SSIDs

The following configurations require dynamic user VLAN assignment by RADIUS to be configured for RADIUS users per the steps in VLAN assignment by RADIUS in the *FortiWiFi and FortiAP Configuration Guide*, specifically, configuring RADIUS user attributes that are used for the VLAN ID assignment.

To configure Intra-Controller L3 roaming for a bridge mode SSID - CLI:

1. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

2. configure the L3 roaming support bridge mode SSID and related VLAN interface:

```
 config wireless-controller vap
    edit "l3_br1"
        set ssid "L3Roaming_br1"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "wifi-radius"
        set local-bridging enable
        set schedule "always"
        set dynamic-vlan enable
        set l3-roaming enable
    next
```

```
end
config system interface
    edit "lan"
        set vdom "root"
        set ip 10.40.0.1 255.255.255.0
        set allowaccess ping https ssh http fabric
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 4
    next
end
config system interface
    edit "lan_100"
        set vdom "root"
        set ip 10.43.100.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 10
        set interface "lan"
        set vlanid 100
    next
end
```

3. Assign L3 roaming VAP to FAP433F:

```
config wireless-controller wtp-profile
    edit "433F"
        config platform
            set type 433F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ax-5G
            set vap-all manual
            set vaps "l3_br1"
            set channel "36"
        end
        config radio-3
            set mode disabled
        end
    next
end
config wireless-controller wtp
    edit "FP433FXX00000000"
        set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
        set admin enable
        set wtp-profile "433F"
        config radio-2
        end
    next
end
```

4. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
    edit "831F.1"
        config platform
            set type 831F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        set allowaccess https ssh
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ax-5G
            set power-level 99
            set vap-all manual
            set vaps "l3_br1"
            set channel "36" "40"
        end
        config radio-3
            set mode disabled
        end
    next
end
config wireless-controller wtp
    edit "FP831FXX00000000"
        set uuid b867ca7c-cbc5-51ec-d5ac-4a395282be68
        set admin enable
        set wtp-profile "831F.1"
        config radio-2
        end
    next
end
```

To configure Inter-Controller L3 roaming for a bridge mode SSID - CLI:

This configuration requires two FortiGate units. In order to enable L3 roaming supported VAP, both FortiGate units must have the same SSID, security, and passphrase.

The following example uses:

- AC1 as FGT40F
  - FAP1 as FAP433E
- AC2 as FGT81EP
  - FAP2 as FAP831F

1. Configure the L3 roaming peer IP for AC1 (FGT-40F):

```
config system interface
  edit "wan"
    set vdom "root"
    set ip 10.43.1.40 255.255.255.0
    set allowaccess ping https ssh http fabric
    set type physical
    set role wan
    set snmp-index 1
  next
end
config wireless-controller inter-controller
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.81
    next
  end
end
```

a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

b. Configure the L3 roaming support bridge mode SSID and related VLAN interface:

```
config wireless-controller vap
    edit "l3_br1"
        set ssid "L3Roaming_br1"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "wifi-radius"
        set local-bridging enable
        set schedule "always"
        set dynamic-vlan enable
        set l3-roaming enable
        set l3-roaming-mode indirect
    next
end
config system interface
    edit "lan"
        set vdom "root"
        set ip 10.40.0.1 255.255.255.0
        set allowaccess ping https ssh http fabric
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 4
    next
end
config system interface
    edit "lan_100"
        set vdom "root"
        set ip 10.43.100.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 10
        set interface "lan"
        set vlanid 100
    next
end
```

c. Assign L3 roaming VAP to FAP433F:

```
config wireless-controller wtp-profile
    edit "433F"
        config platform
            set type 433F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ax-5G
            set vap-all manual
            set vaps "l3_br1"
            set channel "36"
        end
        config radio-3
            set mode disabled
        end
    next
end
config wireless-controller wtp
    edit "FP433FXX00000000"
        set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
        set admin enable
        set wtp-profile "433F"
        config radio-2
        end
    next
end
```

2. Configure the L3 roaming peer IP for AC2 (FGT-81EP):

```
config system interface
  edit "wan1"
    set vdom "root"
    set ip 10.43.1.81 255.255.255.0
    set allowaccess ping https ssh http fabric
    set type physical
    set role wan
    set snmp-index 1
  next
end
config wireless-controller inter-controller
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.40
    next
  end
end
```

a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

b. Configure the L3 roaming support bridge mode SSID and related VLAN interface:

```
config wireless-controller vap
    edit "l3_br1"
        set ssid "L3Roaming_br1"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "wifi-radius"
        set local-bridging enable
        set schedule "always"
        set dynamic-vlan enable
        set l3-roaming enable
        set l3-roaming-mode indirect
    next
end
config system interface
    edit "lan_hw"
        set vdom "root"
        set ip 10.81.0.129 255.255.255.0
        set allowaccess ping https ssh http fabric
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 52
    next
end
config system interface
    edit "lan_100"
        set vdom "root"
        set ip 10.81.100.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 34
        set interface "lan_hw"
        set vlanid 100
    next
end
```

c. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
    edit "831F.1"
        config platform
            set type 831F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        set allowaccess https ssh
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ax-5G
```

```
                set power-level 99
                set vap-all manual
                set vaps "l3_br1"
                set channel "36" "40"
            end
            config radio-3
                set mode disabled
            end
        next
    end
    config wireless-controller wtp
        edit "FP831FXX00000000"
            set uuid b867ca7c-cbc5-51ec-d5ac-4a395282be68
            set admin enable
            set wtp-profile "831F.1"
            config radio-2
            end
        next
    end
```

3. Check the peer status from AC1 (FGT-40F):

```
FortiGate-40F  # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
    peer cnt: 1
              FG81EPXX00000000 10.43.1.81:5246       UP 0
```

4. Check the peer status from AC2 (FGT-81EP):

```
FortiGate-81E-POE # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
    peer cnt: 1
              FGT40FXX00000000 10.43.1.40:5246       UP 0
```

Understanding L3 roaming events for inter-controller L3 roaming for a bridge mode SSID

When the wireless client is connected with "L3Roaming_br1" on AP1 in AC1, the client receives IP 10.43.100.2 from AP1 in AC1, bridged to “lan_100” VLAN interface:

```
FortiGate-40F # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=2 rId=2 wlan=l3_br1 vlan_id=100 ip=10.43.100.2 ip6=fe80::c84:737e:2ba0:7ae2
mac=22:cf:0e:1a:7f:d2 vci= host= user=vlan0100 group=wifi-radius signal=-67 noise=-95 idle=6
bw=0 use=6 chan=36 radio_type=11AC security=wpa2_only_enterprise mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

When the client leaves AP1 and roams towards AP2, it connects with the same SSID "L3Roaming_br1" on AP2. Wireless traffic passes from AP2 and is sent to AC2. Eventually the wireless traffic is transferred from AC2 to AC1 and traffic is maintained from AC1. The wireless client maintains the original IP of 10.43.100.2:

```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=10 rId=2 wlan=l3_br1 vlan_id=0 ip=10.43.100.2 ip6=:: mac=22:cf:0e:1a:7f:d2 vci=
host= user=vlan0100 group=wifi-radius signal=-58 noise=-95 idle=1 bw=5 use=7 chan=36 radio_
```

```
type=11AC security=wpa2_only_enterprise mpsk= encrypt=aes cp_authed=no l3r=0,1
G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

If the wireless client idle time exceeds `client-idle-rehome-timeout`, it triggers the rehome event. The wireless client will send a DHCP request and obtain a new IP address from AC2 (10.81.100.2). Now the wireless client traffic is maintained from AC2:

```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   L vf=0 wtp=10 rId=2 wlan=l3_br1 vlan_id=100 ip=10.81.100.2 ip6=fe80::c84:737e:2ba0:7ae2
mac=22:cf:0e:1a:7f:d2 vci= host= user=vlan0100 group=wifi-radius signal=-55 noise=-95 idle=3
bw=0 use=6 chan=36 radio_type=11AC security=wpa2_only_enterprise mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

Redesign rate control CLI - 7.2.1

This implementation redesigns wireless controller VAP CLI commands to support allowed data rates based on the 802.11ac operating band and ax standards. This update provides flexibility to disable any spatial streams from the setting and options to set rate control on the VAP level based on the number of spatial streams. You can configure data rates on up to 8 spatial streams under the newer VHT (802.11ac) and HE (802.11ax) standards, an upgrade from the previous syntax that only allowed up to 4 spatial streams. This redesign also supports 8x8 AP models.

This following old CLI commands are removed from `config wireless-controller vap` and replaced with new commands to configure 802.11ac and 802.11ax Modulation and Coding Scheme (MCS) rates:

Removed commands	New commands
`set rates-11ac-ss12` Allowed data rates for 802.11ac with 1 or 2 spatial streams.	`set rates-11ac-mcs-map` Comma separated list of max supported VHT MCS for spatial streams 1 through 8, max supported mcs option: - spatial streams not supported. 7 support for VHT-MCS 0-7 for n spatial streams. 8 support for VHT-MCS 0-8 for n spatial streams. 9 support for VHT-MCS 0-9 for n spatial streams. 11 support for VHT-MCS 0-11 for n spatial streams.
`set rates-11ac-ss34` Allowed data rates for 802.11ac with 3 or 4 spatial streams.	`set rates-11ax-mcs-map` Comma separated list of max supported HE MCS for spatial streams 1 through 8, max supported mcs option: - spatial streams not supported. 7 support for HE-MCS 0-7 for n spatial streams. 9 support for HE-MCS 0-9 for n spatial streams. 11 support for HE-MCS 0-11 for n spatial

Removed commands	New commands
	streams.
set rates-11ax-ss12 Allowed data rates for 802.11ax with 1 or 2 spatial streams.	
set rates-11ax-ss34 Allowed data rates for 802.11ax with 3 or 4 spatial streams.	

- Enabling MCS data rate with MCS index 9 will automatically enable data rate with MCS index 8.
- For 8x8 FortiAPs, users can set 8 values for 8 streams separated by commas.
- If the values `rates-11ax-mcs-map` and `rates-11ac-mcs-map` are not set, the maximum data rate setting is set by default

To set data rates in VAP:

The following example configuration on a 4x4 AP shows how to set data rates for four streams where stream 5-8 are not supported. The numbers used in this example are separated by commas that correspond to MCS values in the 802.11ax and 802.11ac WiFi standards.

1. Set data rates in the wireless controller VAP.

```
config wireless-controller vap
  edit "new_rate_test"
    set ssid "newratetest"
    set security wpa-personal
    set passphrase ENC ******
    set rates-11ac-mcs-map "7,8,9,8"
    set rates-11ax-mcs-map "7,9,11,7"
  next
end
```

2. Apply the SSID to the wtp-profile.

```
config wireless-controller wtp-profile
  edit "431F_rate"
    config platform
      set type 431F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess https ssh snmp
    config radio-1
      set band 802.11ax,n,g-only
      set vap-all manual
      set vaps "new_rate_test"
    end
    config radio-2
      set band 802.11ax-5G
      set vap-all manual
      set vaps "new_rate_test"
      set channel "108"
    end
    config radio-3
      set mode monitor
    end
  next
end
```

3. Once the FortiGate settings are applied to a manged FortiAP, you can verify the configurations from the FortiAP CLI.

   Note: The maximum rates in 802.11ac and 802.11ax streams 1-4 under the `rates control configuration` output are bolded to show how the configurations directly correspond to `set rates-11ac-mcs-map "7,8,9,8"` and `set rates-11ax-mcs-map "7,9,11,7"`, configured in Step 1.

```
FortiAP-431F # vcfg
-------------------------------VAP Configuration    1----------------------------
Radio Id  0 WLAN Id  0 newratetest ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
           vlanid=0, intf=wlan00, vap=0x37e7e02c, bssid=04:d5:90:e9:f3:18
           11ax high-efficiency=enabled target-wake-time=enabled
           ...
           rates control configuration:
               11ac_ss12: mcs0/1 mcs1/1 mcs2/1 mcs3/1 mcs4/1 mcs5/1 mcs6/1 mcs7/1 mcs0/2
mcs1/2 mcs2/2 mcs3/2 mcs4/2 mcs5/2 mcs6/2 mcs7/2 mcs8/2
               11ac_ss34: mcs0/3 mcs1/3 mcs2/3 mcs3/3 mcs4/3 mcs5/3 mcs6/3 mcs7/3 mcs8/3
mcs9/3 mcs0/4 mcs1/4 mcs2/4 mcs3/4 mcs4/4 mcs5/4 mcs6/4 mcs7/4 mcs8/4
               11ac_ss56: mcs0/5 mcs1/5 mcs2/5 mcs3/5 mcs4/5 mcs5/5 mcs6/5 mcs7/5 mcs8/5
mcs9/5 mcs10/5 mcs11/5 mcs0/6 mcs1/6 mcs2/6 mcs3/6 mcs4/6 mcs5/6 mcs6/6 mcs7/6 mcs8/6
mcs9/6 mcs10/6 mcs11/6
               11ac_ss78: mcs0/7 mcs1/7 mcs2/7 mcs3/7 mcs4/7 mcs5/7 mcs6/7 mcs7/7 mcs8/7
mcs9/7 mcs10/7 mcs11/7 mcs0/8 mcs1/8 mcs2/8 mcs3/8 mcs4/8 mcs5/8 mcs6/8 mcs7/8 mcs8/8
mcs9/8 mcs10/8 mcs11/8
               11ax_ss12: mcs0/1 mcs1/1 mcs2/1 mcs3/1 mcs4/1 mcs5/1 mcs6/1 mcs7/1 mcs0/2
mcs1/2 mcs2/2 mcs3/2 mcs4/2 mcs5/2 mcs6/2 mcs7/2 mcs8/2 mcs9/2
               11ax_ss34: mcs0/3 mcs1/3 mcs2/3 mcs3/3 mcs4/3 mcs5/3 mcs6/3 mcs7/3 mcs8/3
mcs9/3 mcs10/3 mcs11/3 mcs0/4 mcs1/4 mcs2/4 mcs3/4 mcs4/4 mcs5/4 mcs6/4 mcs7/4
               11ax_ss56: mcs0/5 mcs1/5 mcs2/5 mcs3/5 mcs4/5 mcs5/5 mcs6/5 mcs7/5 mcs8/5
mcs9/5 mcs10/5 mcs11/5 mcs0/6 mcs1/6 mcs2/6 mcs3/6 mcs4/6 mcs5/6 mcs6/6 mcs7/6 mcs8/6
mcs9/6 mcs10/6 mcs11/6
               11ax_ss78: mcs0/7 mcs1/7 mcs2/7 mcs3/7 mcs4/7 mcs5/7 mcs6/7 mcs7/7 mcs8/7
mcs9/7 mcs10/7 mcs11/7 mcs0/8 mcs1/8 mcs2/8 mcs3/8 mcs4/8 mcs5/8 mcs6/8 mcs7/8 mcs8/8
mcs9/8 mcs10/8 mcs11/8
           application detection engine: disabled
-------------------------------VAP Configuration    2----------------------------
Radio Id  1 WLAN Id  0 newratetest ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
           vlanid=0, intf=wlan10, vap=0x37e7e8b1, bssid=04:d5:90:e9:f3:20
           11ax high-efficiency=enabled target-wake-time=enabled
           ...
           rates control configuration:
               11ac_ss12: mcs0/1 mcs1/1 mcs2/1 mcs3/1 mcs4/1 mcs5/1 mcs6/1 mcs7/1 mcs0/2
mcs1/2 mcs2/2 mcs3/2 mcs4/2 mcs5/2 mcs6/2 mcs7/2 mcs8/2
               11ac_ss34: mcs0/3 mcs1/3 mcs2/3 mcs3/3 mcs4/3 mcs5/3 mcs6/3 mcs7/3 mcs8/3
mcs9/3 mcs0/4 mcs1/4 mcs2/4 mcs3/4 mcs4/4 mcs5/4 mcs6/4 mcs7/4 mcs8/4
               11ac_ss56: mcs0/5 mcs1/5 mcs2/5 mcs3/5 mcs4/5 mcs5/5 mcs6/5 mcs7/5 mcs8/5
```

```
mcs9/5 mcs10/5 mcs11/5 mcs0/6 mcs1/6 mcs2/6 mcs3/6 mcs4/6 mcs5/6 mcs6/6 mcs7/6 mcs8/6
mcs9/6 mcs10/6 mcs11/6
               11ac_ss78: mcs0/7 mcs1/7 mcs2/7 mcs3/7 mcs4/7 mcs5/7 mcs6/7 mcs7/7 mcs8/7
mcs9/7 mcs10/7 mcs11/7 mcs0/8 mcs1/8 mcs2/8 mcs3/8 mcs4/8 mcs5/8 mcs6/8 mcs7/8 mcs8/8
mcs9/8 mcs10/8 mcs11/8
               11ax_ss12: mcs0/1 mcs1/1 mcs2/1 mcs3/1 mcs4/1 mcs5/1 mcs6/1 mcs7/1 mcs0/2
mcs1/2 mcs2/2 mcs3/2 mcs4/2 mcs5/2 mcs6/2 mcs7/2 mcs8/2 mcs9/2
               11ax_ss34: mcs0/3 mcs1/3 mcs2/3 mcs3/3 mcs4/3 mcs5/3 mcs6/3 mcs7/3 mcs8/3
mcs9/3 mcs10/3 mcs11/3 mcs0/4 mcs1/4 mcs2/4 mcs3/4 mcs4/4 mcs5/4 mcs6/4 mcs7/4
               11ax_ss56: mcs0/5 mcs1/5 mcs2/5 mcs3/5 mcs4/5 mcs5/5 mcs6/5 mcs7/5 mcs8/5
mcs9/5 mcs10/5 mcs11/5 mcs0/6 mcs1/6 mcs2/6 mcs3/6 mcs4/6 mcs5/6 mcs6/6 mcs7/6 mcs8/6
mcs9/6 mcs10/6 mcs11/6
               11ax_ss78: mcs0/7 mcs1/7 mcs2/7 mcs3/7 mcs4/7 mcs5/7 mcs6/7 mcs7/7 mcs8/7
mcs9/7 mcs10/7 mcs11/7 mcs0/8 mcs1/8 mcs2/8 mcs3/8 mcs4/8 mcs5/8 mcs6/8 mcs7/8 mcs8/8
mcs9/8 mcs10/8 mcs11/8
           application detection engine: disabled
-------------------------------Total    2 VAP Configurations----------------------------
```

Data rate conversion support

Previously configured rate control values are converted to the new data rate values when you upgrade to FOS 7.2.1. The following example shows how an old value would be converted:

Old rate control value	Converted rate control value in FOS 7.2.1

config wireless-controller vap
  edit "upgrade"
    set ssid "upgrade"
    set security wpa-personal
    set passphrase ENC ******
    set rates-11ac-ss12 mcs5/1 mcs7/2
    set rates-11ac-ss34 mcs7/3 mcs9/4
    set rates-11ax-ss12 mcs7/1 mcs8/2
    set rates-11ax-ss34 mcs9/3 mcs11/4
  next
end
	config wireless-controller vap
	  edit "upgrade"
	    set ssid "upgrade"
	    set security wpa-personal
	    set passphrase ENC ******
	    set rates-11ac-mcs-map "7,7,7,9,"
	    set rates-11ax-mcs-map "7,9,9,11,"
	  next
	end

Conversion of old syntax settings to upgraded new syntax settings is based on the following points:

- In the old syntax, **mcsX/n** means **MCS index value X** for **n spatial streams**. For example, **mcs5/1** means **MCS index value 5** for **1 spatial stream**.
- Enabling MCS data rate with MCS index 9 will automatically enable data rate with MCS index 8.
- rates-11ac-mcs-map syntax:

  7 support for VHT-MCS 0-7 for n spatial streams.

  8 support for VHT-MCS 0-8 for n spatial streams.

  9 support for VHT-MCS 0-9 for n spatial streams.

  11 support for VHT-MCS 0-11 for n spatial streams.

  For example, mcs5/1 is converted to 7 to represent VHT-MCS 0-7 for n spatial streams.
- rates-11ax-mcs-map syntax:

  7 support for HE-MCS 0-7 for n spatial streams.

  9 support for HE-MCS 0-9 for n spatial streams.

11 support for HE-MCS 0-11 for n spatial streams.

For example, mcs8/2 is converted to 9 to represent HE-MCS 0-9 for n spatial streams.

Add GUI visibility for Advanced Wireless Features - 7.2.1

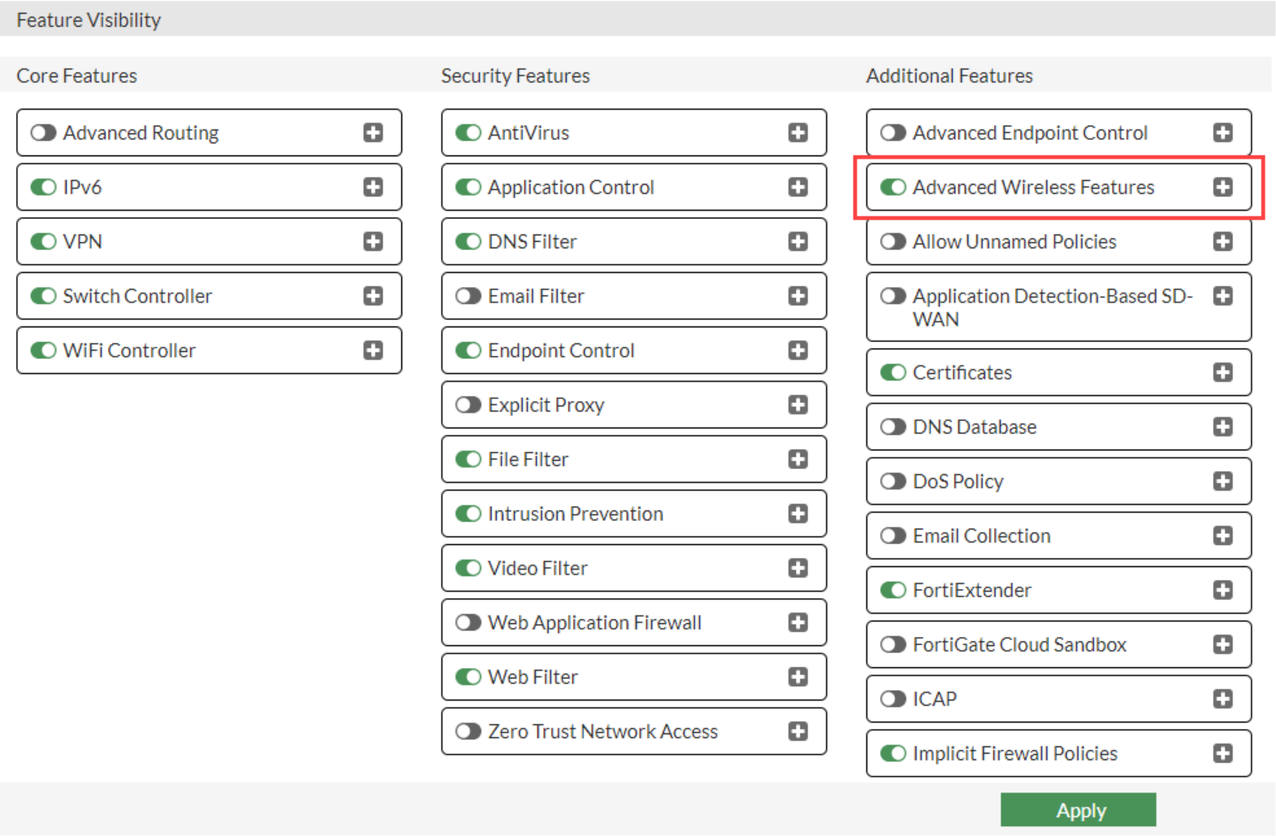
This enhancement adds visibility for configuring advanced options for wireless features in the FortiGate GUI. You can go to *Feature Visibility* and enable *Advanced Wireless Features* to access the following:

- New navigation entries under *WiFi & Switch Controller*.
  - Operation Profiles: FortiAP, QoS, and FortiAP Configuration.
  - Connectivity Profiles: MPSK and Bonjour.
  - Protection Profiles: WIDS and L3 Firewall (also known as L3 Access Control List configurations for FortiAPs).
- Additional advanced options for wireless features under the *SSIDs* and *WiFi Settings* entries.
  - *SSIDs > Edit Interface*: Voice-Enterprise, Multiband operation, Fast BSS transition, Probe response suppression, Sticky client removal, multicast enhancement, IGMP snooping, Radio sensitivity, Airtime weight, QoS profile, and L3 firewall profile.
  - *WiFi Settings*: Duplicate SSID, DARRP, Phishing SSID detection, and SNMP settings.

A new CLI command is added under system settings to enable the advanced WiFi features on GUI.

To enable Advanced Wireless Features - GUI:

1. From the FortiOS GUI, go to *System > Feature Visibility*.
2. Under the *Additional Features* column, locate and enable *Advanced Wireless Features*.



Feature Visibility

Core Features	Security Features	Additional Features
☐ Advanced Routing	☑ AntiVirus	☐ Advanced Endpoint Control
☑ IPv6	☑ Application Control	☑ Advanced Wireless Features
☑ VPN	☑ DNS Filter	☐ Allow Unnamed Policies
☑ Switch Controller	☐ Email Filter	☐ Application Detection-Based SD-WAN
☑ WiFi Controller	☑ Endpoint Control	☑ Certificates
	☐ Explicit Proxy	☐ DNS Database
	☑ File Filter	☐ DoS Policy
	☑ Intrusion Prevention	☐ Email Collection
	☑ Video Filter	☑ FortiExtender
	☐ Web Application Firewall	☐ FortiGate Cloud Sandbox
	☑ Web Filter	☐ ICAP
	☐ Zero Trust Network Access	☑ Implicit Firewall Policies

3. Click *Apply*.

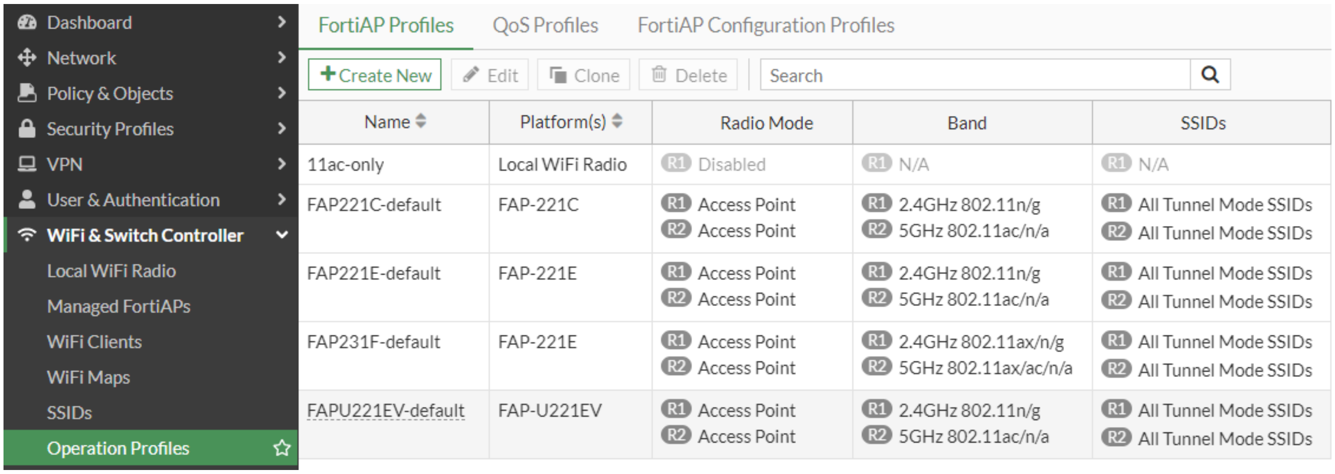
   The Navigation bar reloads with the new features visible.

To enable Advanced Wireless Features - CLI:

```
config system settings
    set gui-advanced-wireless-features enable
end
```

Operations Profiles Entry

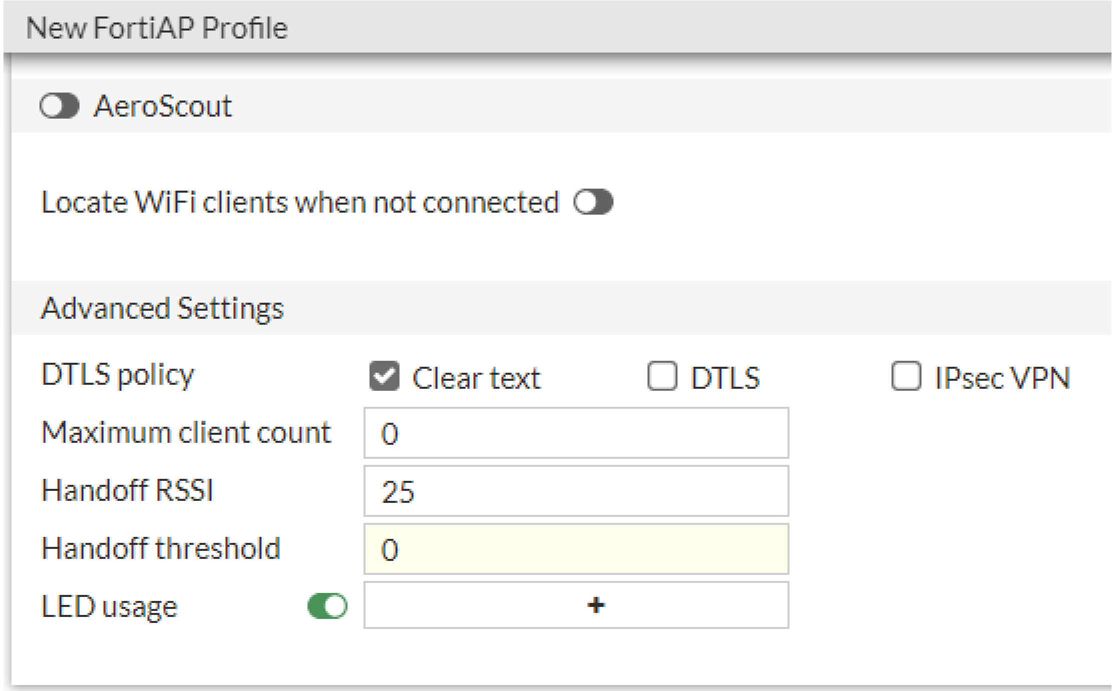
When you enable Advanced Wireless Features, FortiAP Profiles is renamed to Operation Profiles and contains additional tabs that enable you to manage QoS and FortiAP Configuration profiles.



Name	Platform(s)	Radio Mode	Band	SSIDs
11ac-only	Local WiFi Radio	R1 Disabled	R1 N/A	R1 N/A
FAP221C-default	FAP-221C	R1 Access Point R2 Access Point	R1 2.4GHz 802.11n/g R2 5GHz 802.11ac/n/a	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs
FAP221E-default	FAP-221E	R1 Access Point R2 Access Point	R1 2.4GHz 802.11n/g R2 5GHz 802.11ac/n/a	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs
FAP231F-default	FAP-221E	R1 Access Point R2 Access Point	R1 2.4GHz 802.11ax/n/g R2 5GHz 802.11ax/ac/n/a	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs
FAPU221EV-default	FAP-U221EV	R1 Access Point R2 Access Point	R1 2.4GHz 802.11n/g R2 5GHz 802.11ac/n/a	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs

FortiAP Profile Advanced Settings

When you create or edit a FortiAP profile, you can configure additional advanced settings.



New FortiAP Profile

AeroScout

Locate WiFi clients when not connected

Advanced Settings

DTLS policy ☑ Clear text □ DTLS □ IPsec VPN

Maximum client count: 0

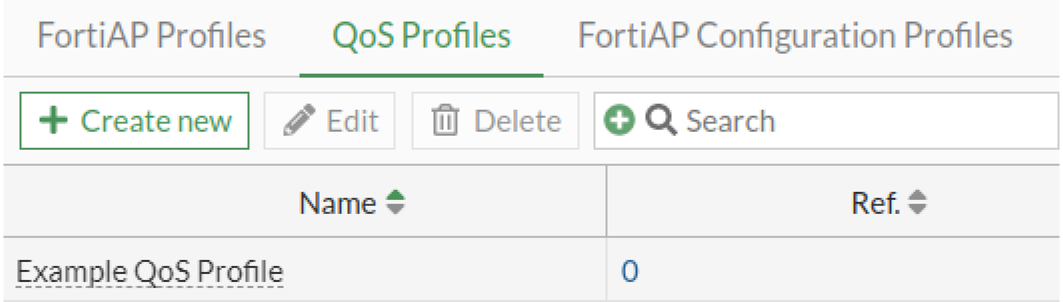
Handoff RSSI: 25

Handoff threshold: 0

LED usage: ● +

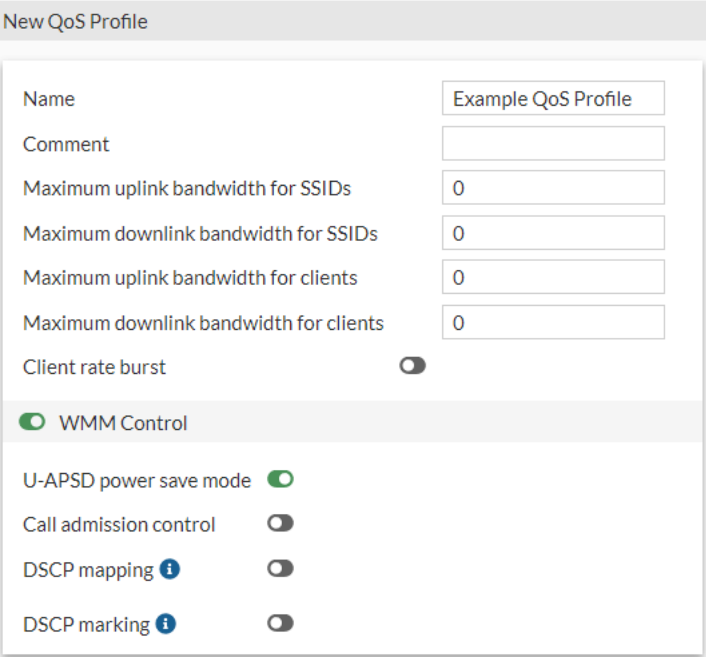
QoS Profiles

You can create or edit Quality of Service (QoS) profiles by clicking the *QoS Profiles* tab.



Name	Ref.
Example QoS Profile	0

Click *Create new* to create a QoS profile.



New QoS Profile

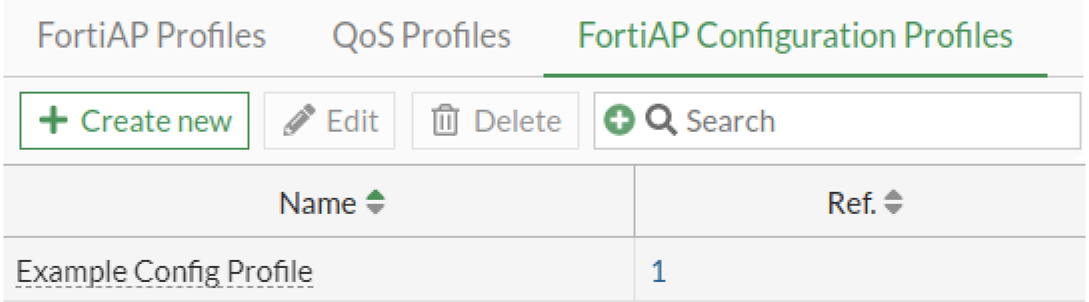
Name	Example QoS Profile
Comment	
Maximum uplink bandwidth for SSIDs	0
Maximum downlink bandwidth for SSIDs	0
Maximum uplink bandwidth for clients	0
Maximum downlink bandwidth for clients	0
Client rate burst	○

● WMM Control

U-APSD power save mode	●
Call admission control	○
DSCP mapping	○
DSCP marking	○

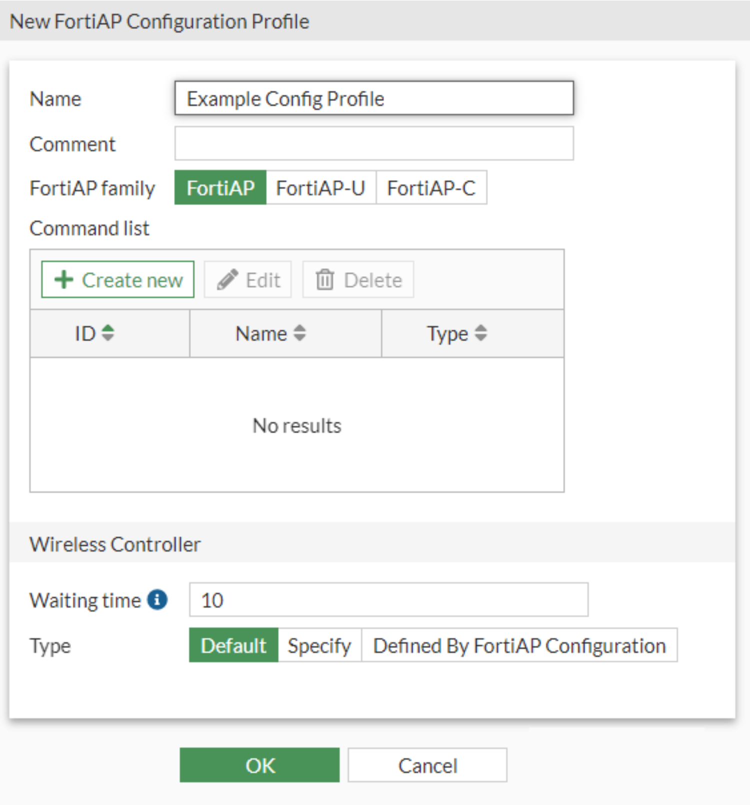
FortiAP Configuration Profiles

You can create or edit FortiAP Configuration Profile for managing local FortiAP configuration by clicking the *FortiAP Configuration Profiles* tab.



Name	Ref.
Example Config Profile	1

Click *Create new* to create a FortiAP Configuration profile.



New FortiAP Configuration Profile

Name: Example Config Profile

Comment:

FortiAP family: FortiAP | FortiAP-U | FortiAP-C

Command list

ID	Name	Type
No results		

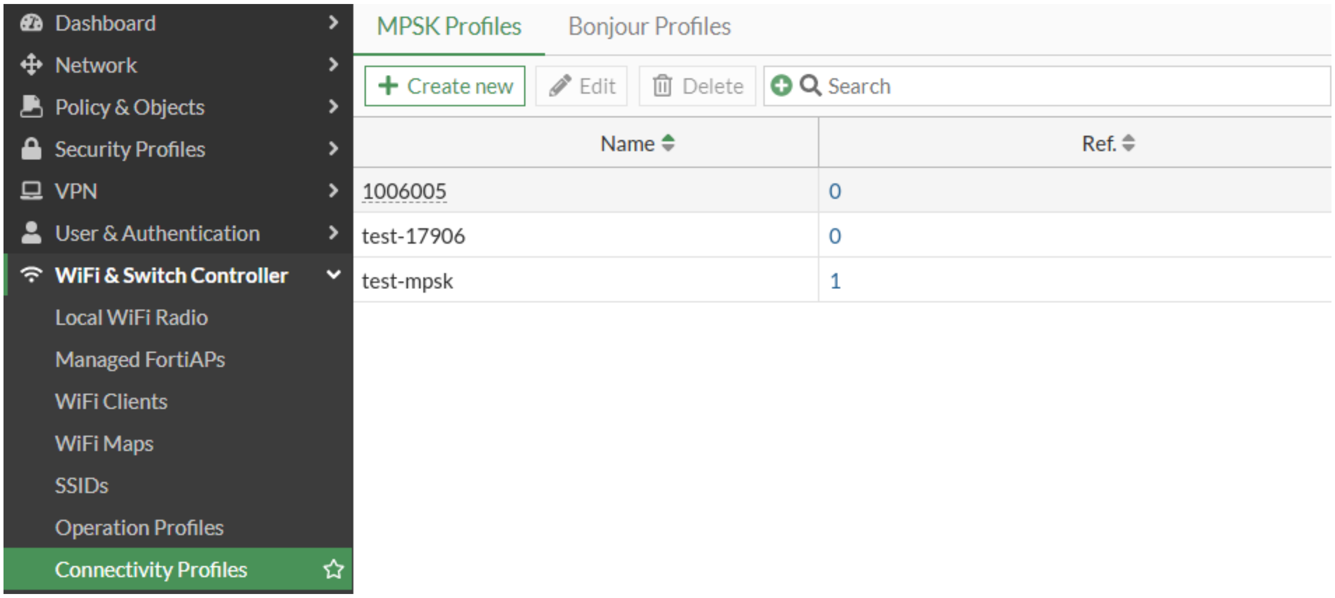
Wireless Controller

Waiting time: 10

Type: Default | Specify | Defined By FortiAP Configuration

Connectivity Profiles Entry

You can access Connectivity Profiles to manage your MPSK and Bonjour profiles.

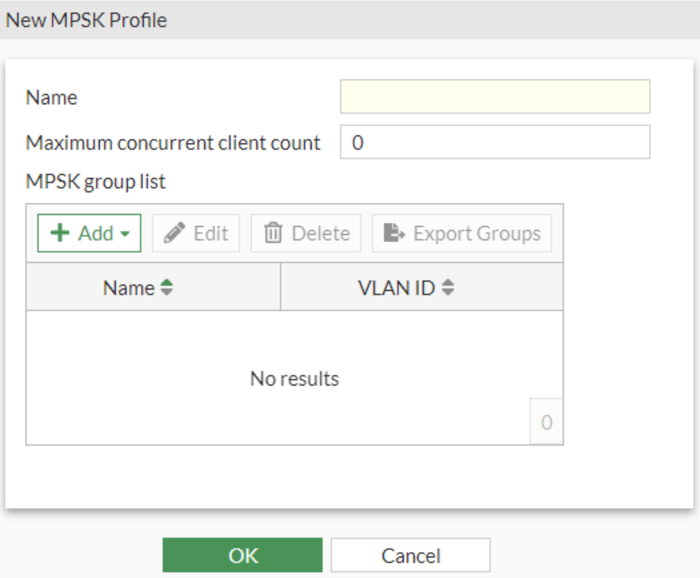


Name	Ref.
1006005	0
test-17906	0
test-mpsk	1

MPSK Profiles

After you click *Connectivity Profile*, the *MPSK Profiles* tab loads by default. From there you can create or edit MPSK profiles to manage multiple pre-shared keys.

Click *Create new* to create an MPSK profile.



New MPSK Profile

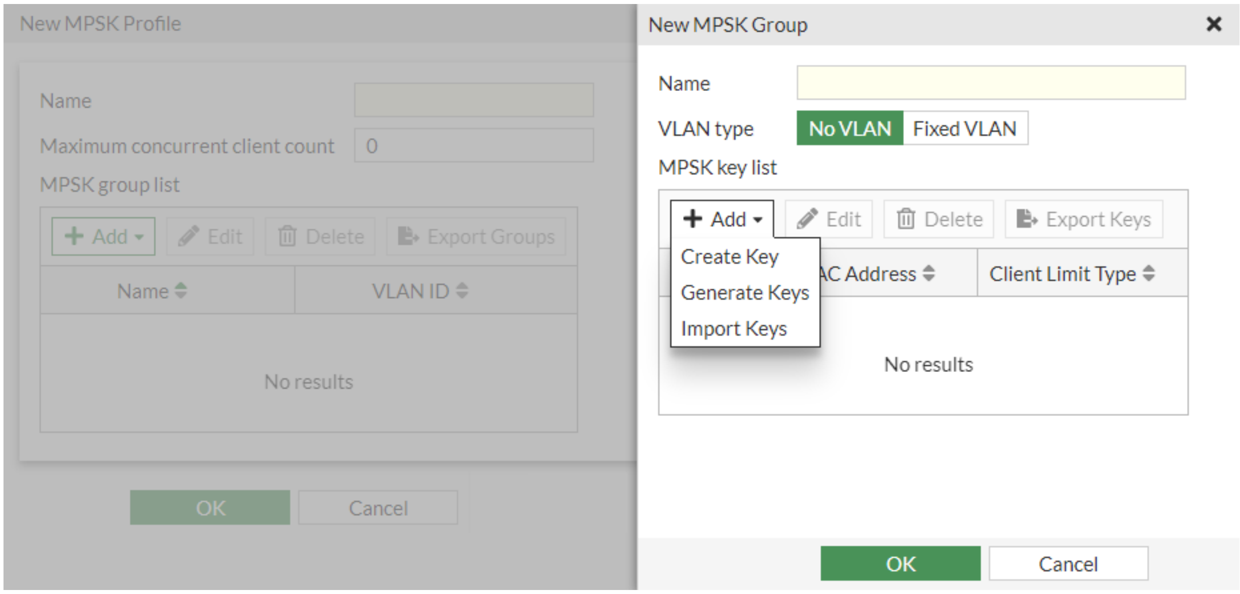
Name

Maximum concurrent client count: 0

MPSK group list

Name	VLAN ID
No results	

From there you can create and add MPSK groups and determine how you want to add your MPSK keys.



New MPSK Group

Name

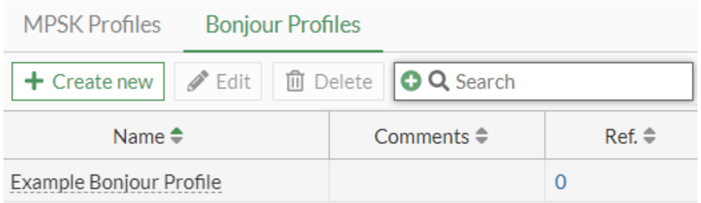
VLAN type: No VLAN (selected) | Fixed VLAN

MPSK key list

...	AC Address	Client Limit Type
No results		

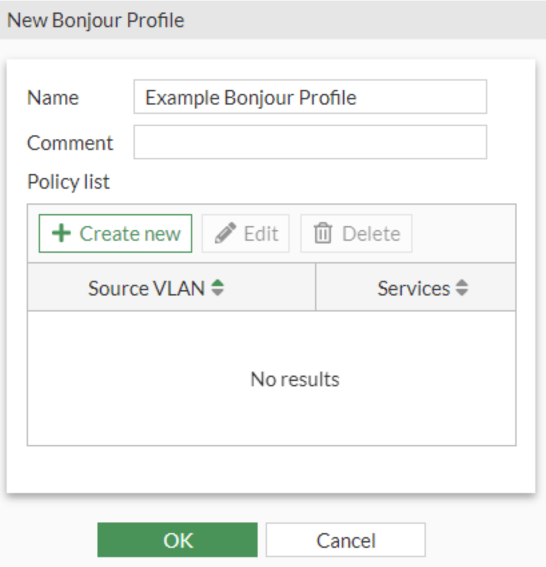
Bonjour Profiles

Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour. You can create or edit Bonjour profiles by clicking the *Bonjour Profiles* tab.



Name	Comments	Ref.
Example Bonjour Profile		0

Click *Create new* to create a Bonjour profile.



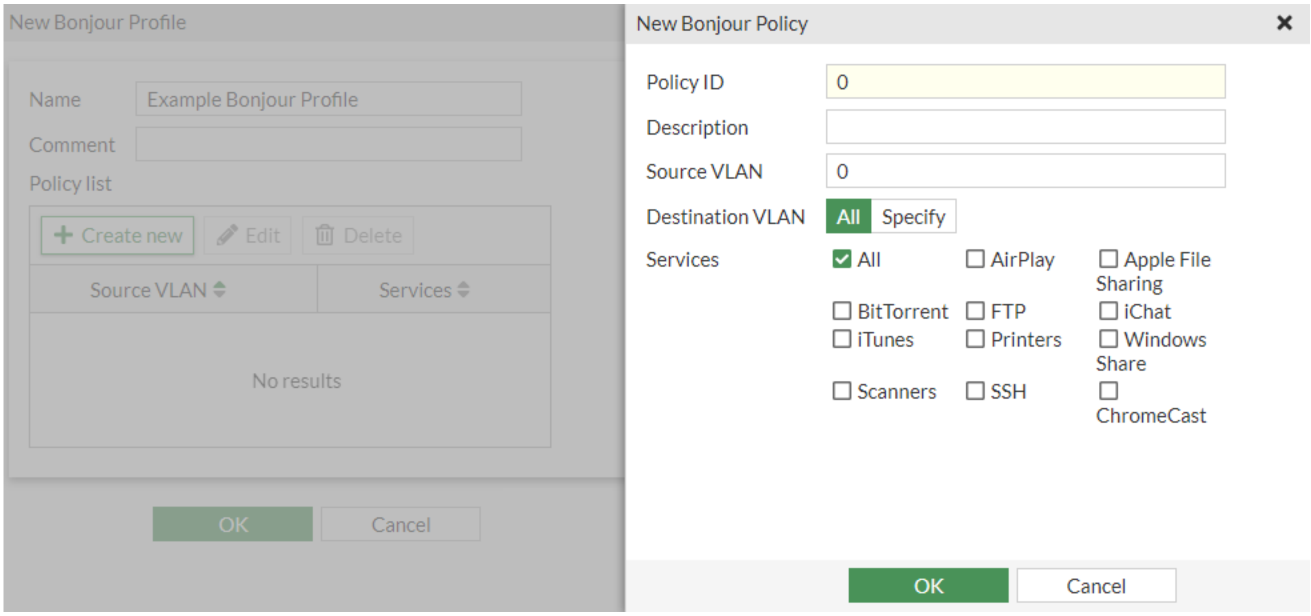
Name: Example Bonjour Profile

Comment:

Policy list

Source VLAN	Services
No results	

From there you can create and add policies that determine which services you want to advertise across the network.



Policy ID: 0

Description:

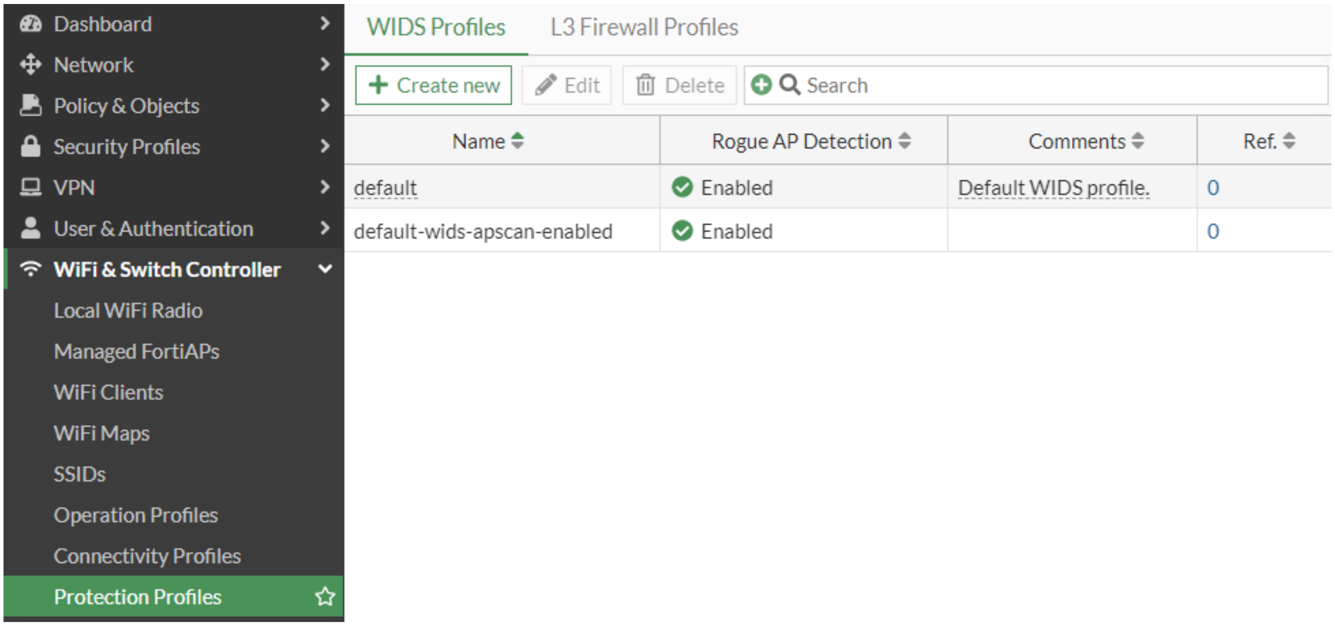
Source VLAN: 0

Destination VLAN: All | Specify

Services: ☑ All ☐ AirPlay ☐ Apple File Sharing ☐ BitTorrent ☐ FTP ☐ iChat ☐ iTunes ☐ Printers ☐ Windows Share ☐ Scanners ☐ SSH ☐ ChromeCast

Protection Profiles Entry

When you enable Advanced Wireless Features, WIDS Profiles is renamed to Protection Profiles and contains additional tabs that enable you to manage L3 Firewall Profiles.



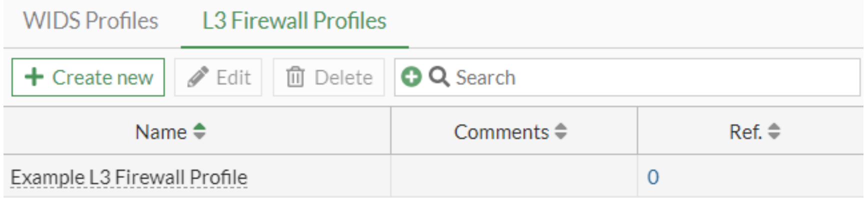
Name	Rogue AP Detection	Comments	Ref.
default	✓ Enabled	Default WIDS profile.	0
default-wids-apscan-enabled	✓ Enabled		0

WIDS Profiles

After you click *Protection Profiles*, the *WIDS Profiles* tab loads by default. From there you can create or edit WIDS profiles to configure the type of security threats you want to monitor.

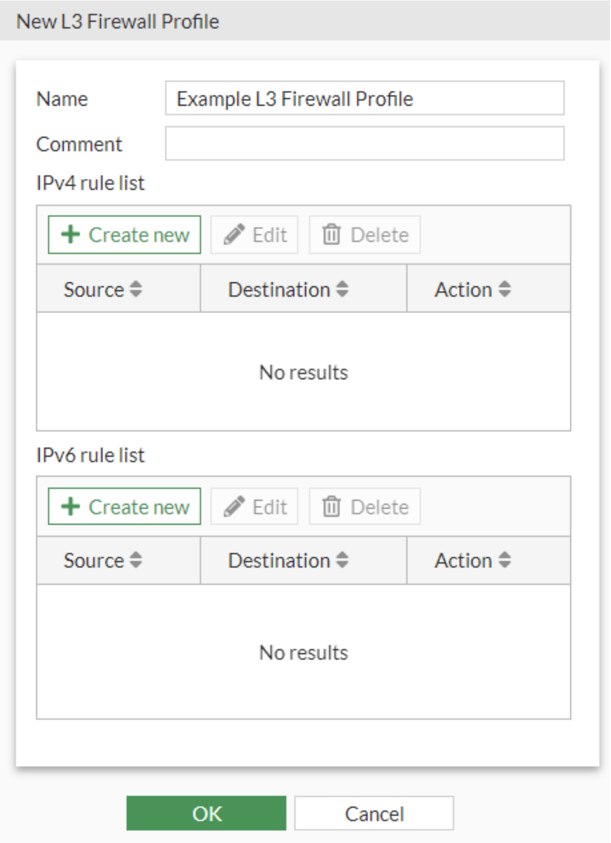
L3 Firewall Profile

You can create or edit L3 Firewall Profiles to configure the WiFi bridge access control list by clicking the *L3 Firewall Profiles* tab.



Name	Comments	Ref.
Example L3 Firewall Profile		0

Click *Create new* to create a L3 Firewall profile.



New L3 Firewall Profile

Name	Example L3 Firewall Profile
Comment	

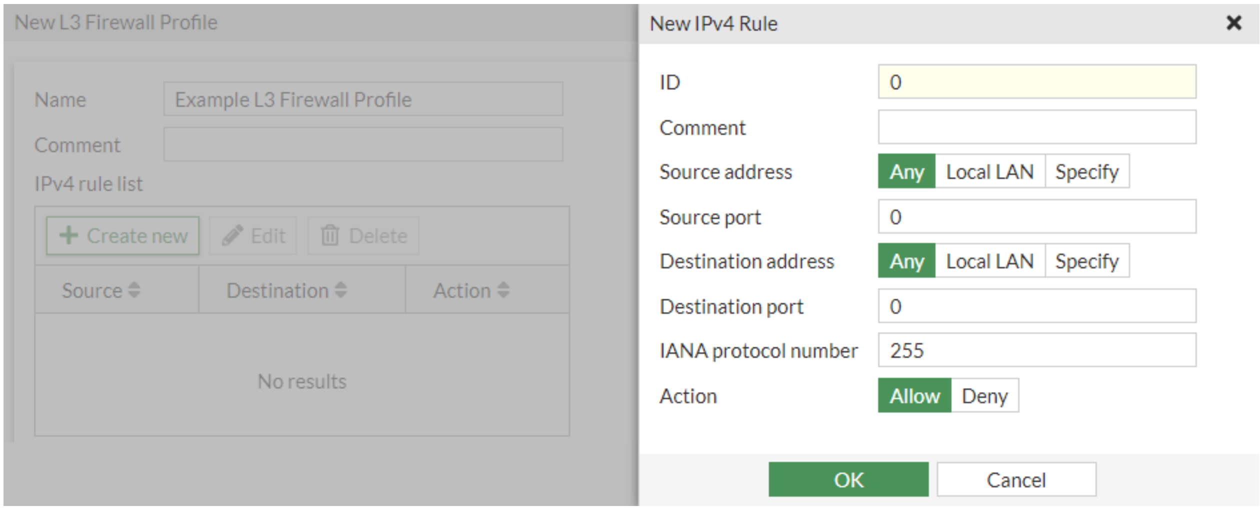
IPv4 rule list

Source	Destination	Action
No results		

IPv6 rule list

Source	Destination	Action
No results		

From there, you can create IPv4 or IPv6 rule lists to allow or deny traffic that matches the configured policy.

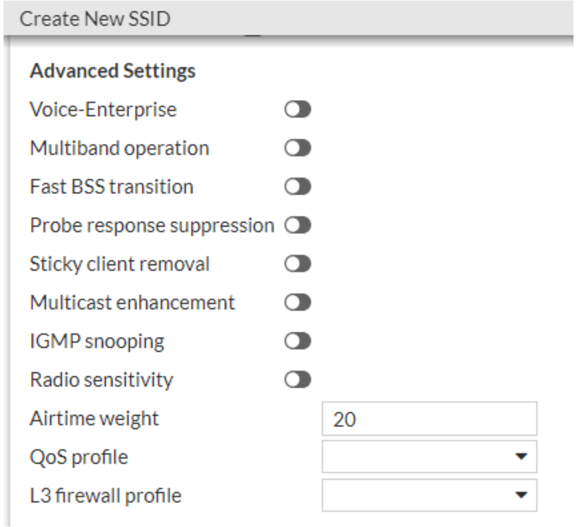


New IPv4 Rule

ID	0
Comment	
Source address	[✓ Any] Local LAN Specify
Source port	0
Destination address	[✓ Any] Local LAN Specify
Destination port	0
IANA protocol number	255
Action	[✓ Allow] Deny

Advanced SSID options

When you create or edit an SSID, you can configure additional advanced settings.



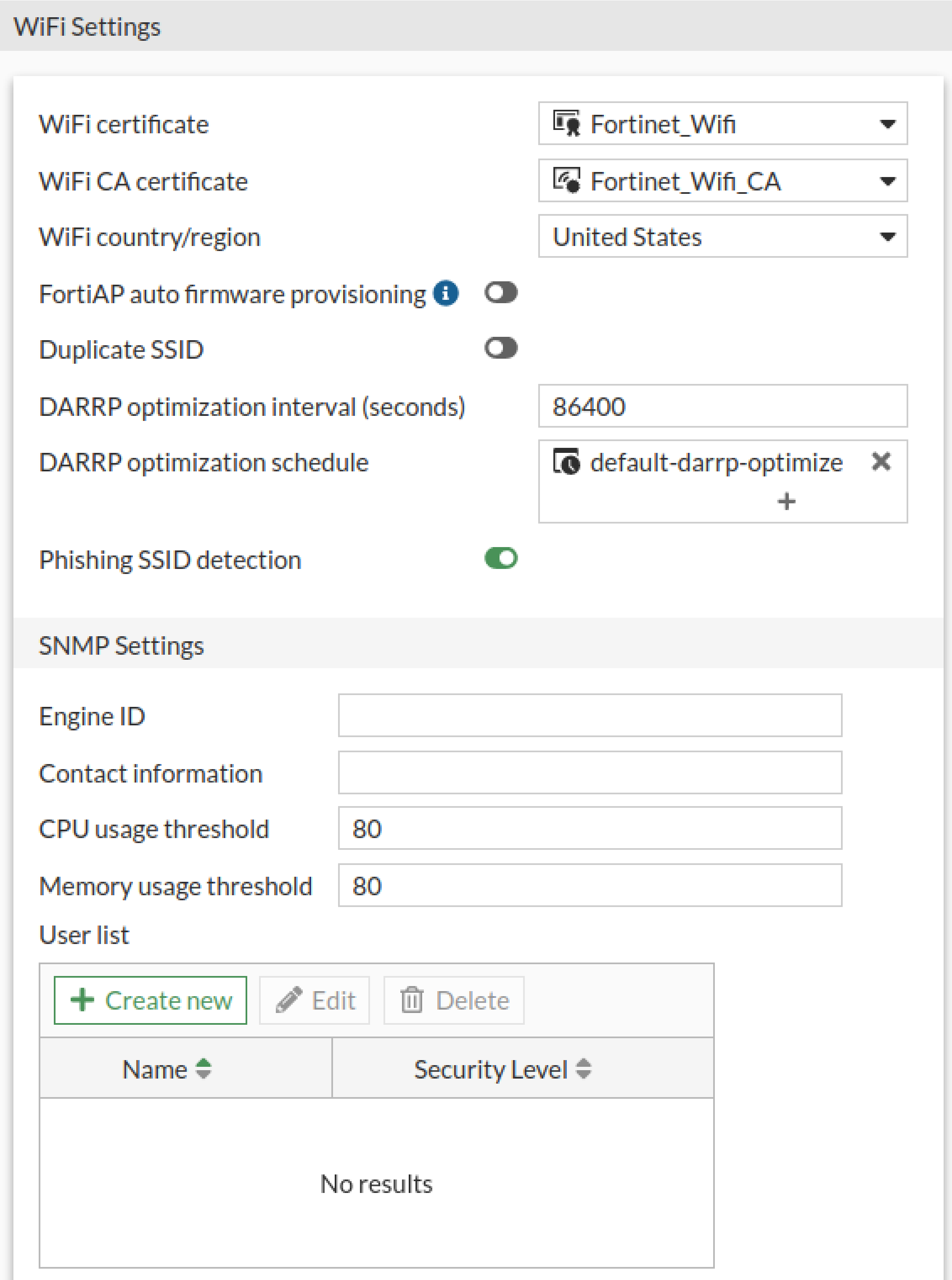
Create New SSID

Advanced Settings

Voice-Enterprise	○
Multiband operation	○
Fast BSS transition	○
Probe response suppression	○
Sticky client removal	○
Multicast enhancement	○
IGMP snooping	○
Radio sensitivity	○
Airtime weight	20
QoS profile	▾
L3 firewall profile	▾

Advanced WiFi Settings options

More options are exposed on WiFi Settings page, including Duplicate SSID, DARRP related settings, Phishing SSID detection setting, and SNMP settings.



WiFi Settings

WiFi certificate	Fortinet_Wifi
WiFi CA certificate	Fortinet_Wifi_CA
WiFi country/region	United States
FortiAP auto firmware provisioning	off
Duplicate SSID	off
DARRP optimization interval (seconds)	86400
DARRP optimization schedule	default-darrp-optimize
Phishing SSID detection	on

SNMP Settings

Engine ID	
Contact information	
CPU usage threshold	80
Memory usage threshold	80

User list

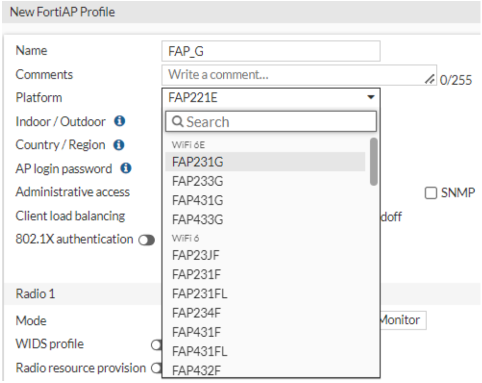
Name	Security Level
No results	

Add profile support for FortiAP G-series models supporting WiFi 6E Tri-band and Dual 5 GHz modes - 7.2.1

WTP profiles are supported for FortiAP G series access points (FAP-231G, FAP-233G, FAP-431G, FAP-433G). The G series models support Wi-Fi 6E IEEE 802.11ax Tri-band 2.4 GHz/5 GHz/6 GHz mode and dual 5 GHz mode.

To configure a FortiAP G series profile - GUI:

1. From the FortiGate GUI, navigate to *WiFi & Switch Controller > FortiAP Profiles* and click *Create New*.
2. In *Platform*, you can select a FortiAP G series model that supports WiFi 6E.



New FortiAP Profile

Name FAP_G

Comments Write a comment... 0/255

Platform FAP221E

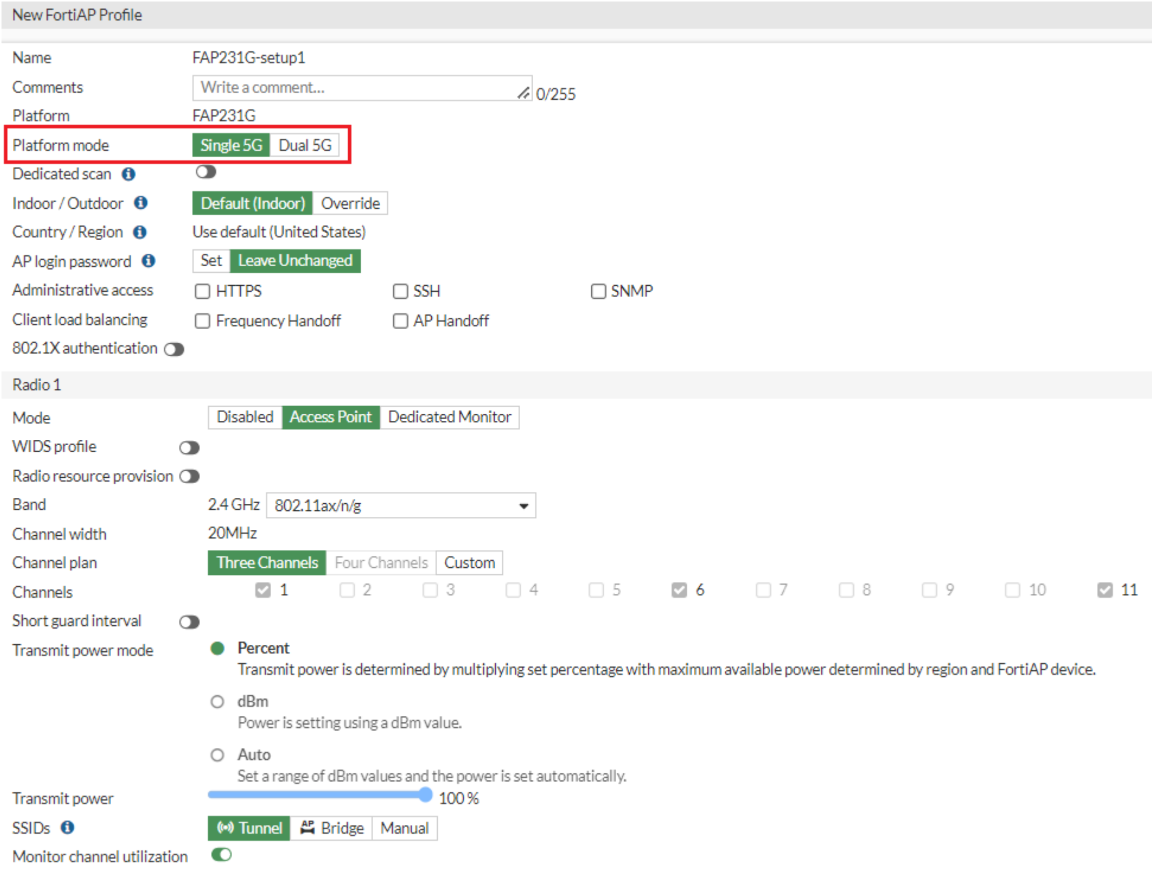
Once you select a platform type, you can begin to configure the profile.

FortiAP G series models support three different radio configuration setups:

- **Tri-band mode: Single 5G, with Dedicated scan disabled**

  This is the default setup when creating a new FortiAP G series profile.

  In this setup, Radio 1 works on the 2.4GHz 802.11ax/n/g bands, Radio 2 works on the 5GHz 802.11ax/ac/n/a bands, and Radio 3 works on the Wi-Fi 6E 6GHz 802.11ax bands.

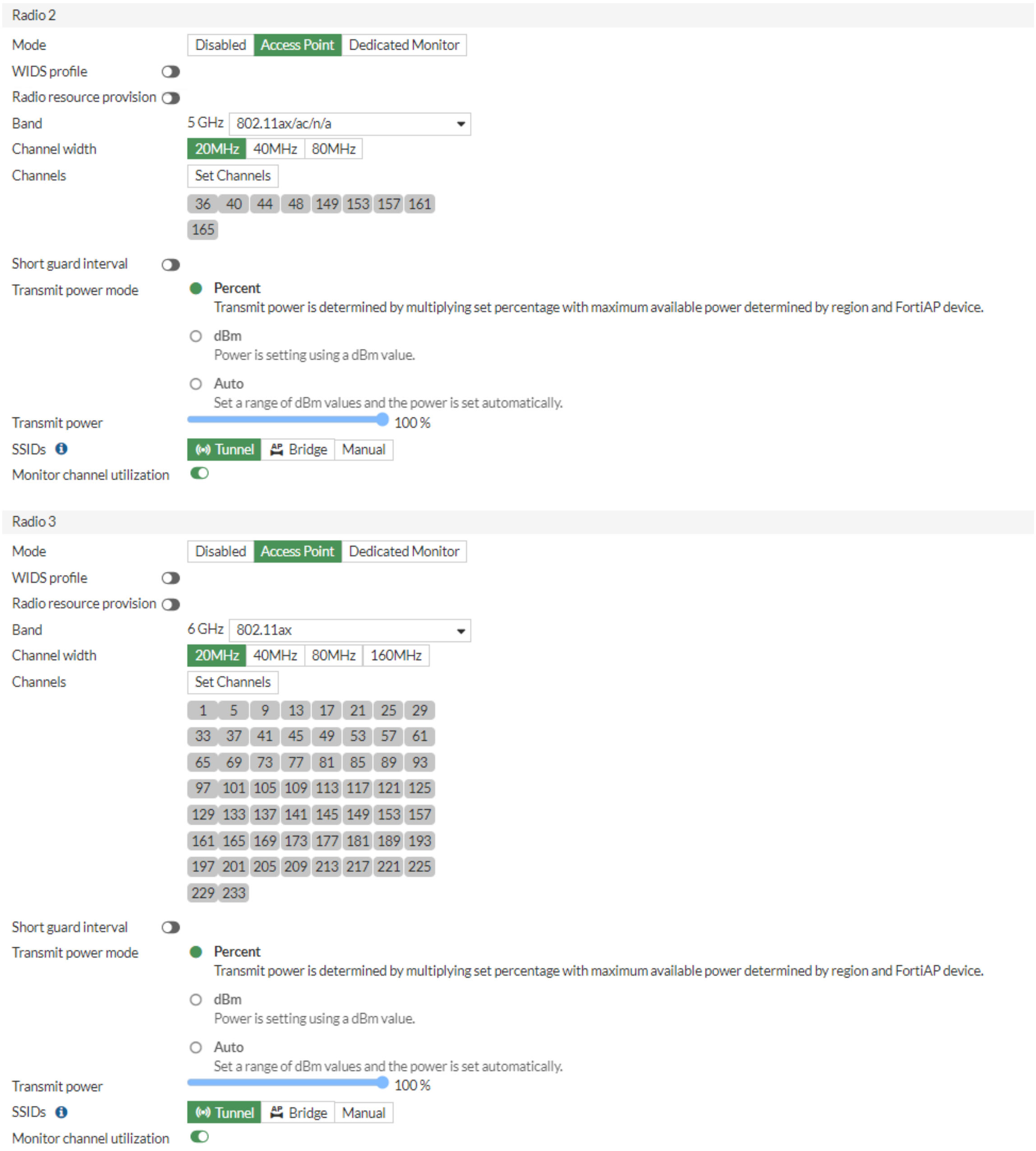


New FortiAP Profile

Name	FAP231G-setup1
Comments	Write a comment... 0/255
Platform	FAP231G
Platform mode	[✓ Single 5G] Dual 5G
Dedicated scan	○
Indoor / Outdoor	[✓ Default (Indoor)] Override
Country / Region	Use default (United States)
AP login password	Set [✓ Leave Unchanged]
Administrative access	□ HTTPS □ SSH □ SNMP
Client load balancing	□ Frequency Handoff □ AP Handoff
802.1X authentication	○

Radio 1

Mode	Disabled [✓ Access Point] Dedicated Monitor
WIDS profile	○
Radio resource provision	○
Band	2.4 GHz 802.11ax/n/g
Channel width	20MHz
Channel plan	[✓ Three Channels] Four Channels Custom
Channels	☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 □ 7 □ 8 □ 9 □ 10 ☑ 11
Short guard interval	○
Transmit power mode	● Percent Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device. ○ dBm Power is setting using a dBm value. ○ Auto Set a range of dBm values and the power is set automatically.
Transmit power	100 %
SSIDs	[✓ Tunnel] Bridge Manual
Monitor channel utilization	●



Radio 2

Mode: Disabled [✓ Access Point] Dedicated Monitor

WIDS profile

Radio resource provision

Band: 5 GHz 802.11ax/ac/n/a

Channel width: [✓ 20MHz] 40MHz 80MHz

Channels: Set Channels

36 40 44 48 149 153 157 161 165

Short guard interval

Transmit power mode:

● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

○ dBm
Power is setting using a dBm value.

○ Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 100 %

SSIDs: [✓ Tunnel] Bridge Manual

Monitor channel utilization

Radio 3

Mode: Disabled [✓ Access Point] Dedicated Monitor

WIDS profile

Radio resource provision

Band: 6 GHz 802.11ax

Channel width: [✓ 20MHz] 40MHz 80MHz 160MHz

Channels: Set Channels

1 5 9 13 17 21 25 29
33 37 41 45 49 53 57 61
65 69 73 77 81 85 89 93
97 101 105 109 113 117 121 125
129 133 137 141 145 149 153 157
161 165 169 173 177 181 189 193
197 201 205 209 213 217 221 225
229 233

Short guard interval

Transmit power mode:

● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

○ dBm
Power is setting using a dBm value.

○ Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 100 %

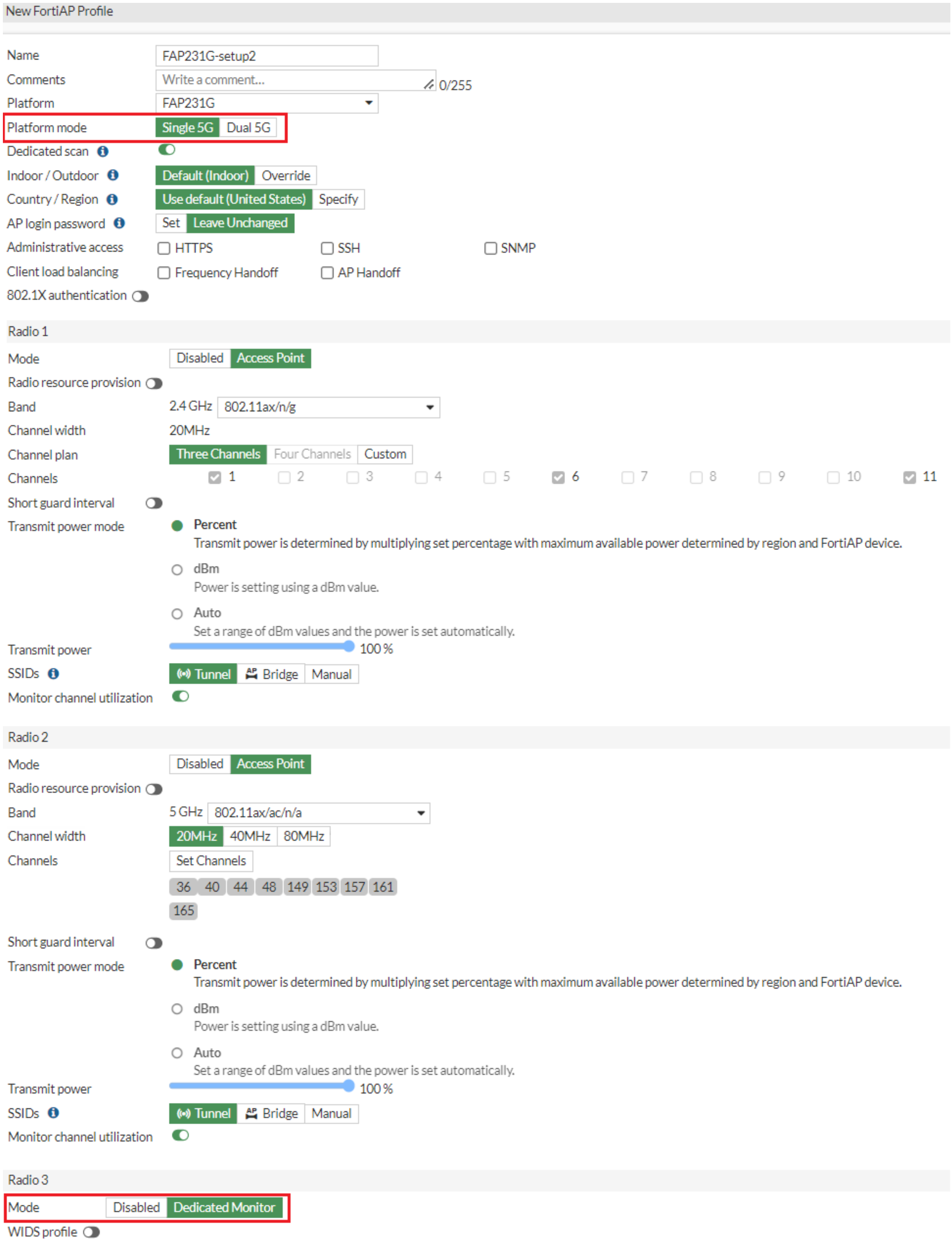
SSIDs: [✓ Tunnel] Bridge Manual

Monitor channel utilization

- **Platform mode: Single 5G, with Dedicated scan enabled**

  In the setup, Radio 1 works on the 2.4GHz 802.11ax/n/g bands, Radio 2 works on the 5GHz 802.11ax/ac/n/a bands, and Radio 3 works in monitor mode only.

  Note: When *Dedicated scan* is enabled, Radio 1 and Radio 2 will not spend any resources on scanning-related functions (for example, rogue AP detection, interfering SSID detection, and etc.). Radio 3 will be scanning all the time for all 2.4GHz, 5GHz, and 6GHz bands.



New FortiAP Profile

Name	FAP231G-setup2
Comments	Write a comment... 0/255
Platform	FAP231G
Platform mode	[✓ Single 5G] Dual 5G
Dedicated scan	●
Indoor / Outdoor	[✓ Default (Indoor)] Override
Country / Region	[✓ Use default (United States)] Specify
AP login password	Set [✓ Leave Unchanged]
Administrative access	□ HTTPS □ SSH □ SNMP
Client load balancing	□ Frequency Handoff □ AP Handoff
802.1X authentication	○

Radio 1

Mode	Disabled [✓ Access Point]
Radio resource provision	○
Band	2.4 GHz 802.11ax/n/g
Channel width	20MHz
Channel plan	[✓ Three Channels] Four Channels Custom
Channels	☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 □ 7 □ 8 □ 9 □ 10 ☑ 11
Short guard interval	○
Transmit power mode	● Percent Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device. ○ dBm Power is setting using a dBm value. ○ Auto Set a range of dBm values and the power is set automatically.
Transmit power	100 %
SSIDs	[✓ Tunnel] Bridge Manual
Monitor channel utilization	●

Radio 2

Mode	Disabled [✓ Access Point]
Radio resource provision	○
Band	5 GHz 802.11ax/ac/n/a
Channel width	[✓ 20MHz] 40MHz 80MHz
Channels	Set Channels 36 40 44 48 149 153 157 161 165
Short guard interval	○
Transmit power mode	● Percent Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device. ○ dBm Power is setting using a dBm value. ○ Auto Set a range of dBm values and the power is set automatically.
Transmit power	100 %
SSIDs	[✓ Tunnel] Bridge Manual
Monitor channel utilization	●

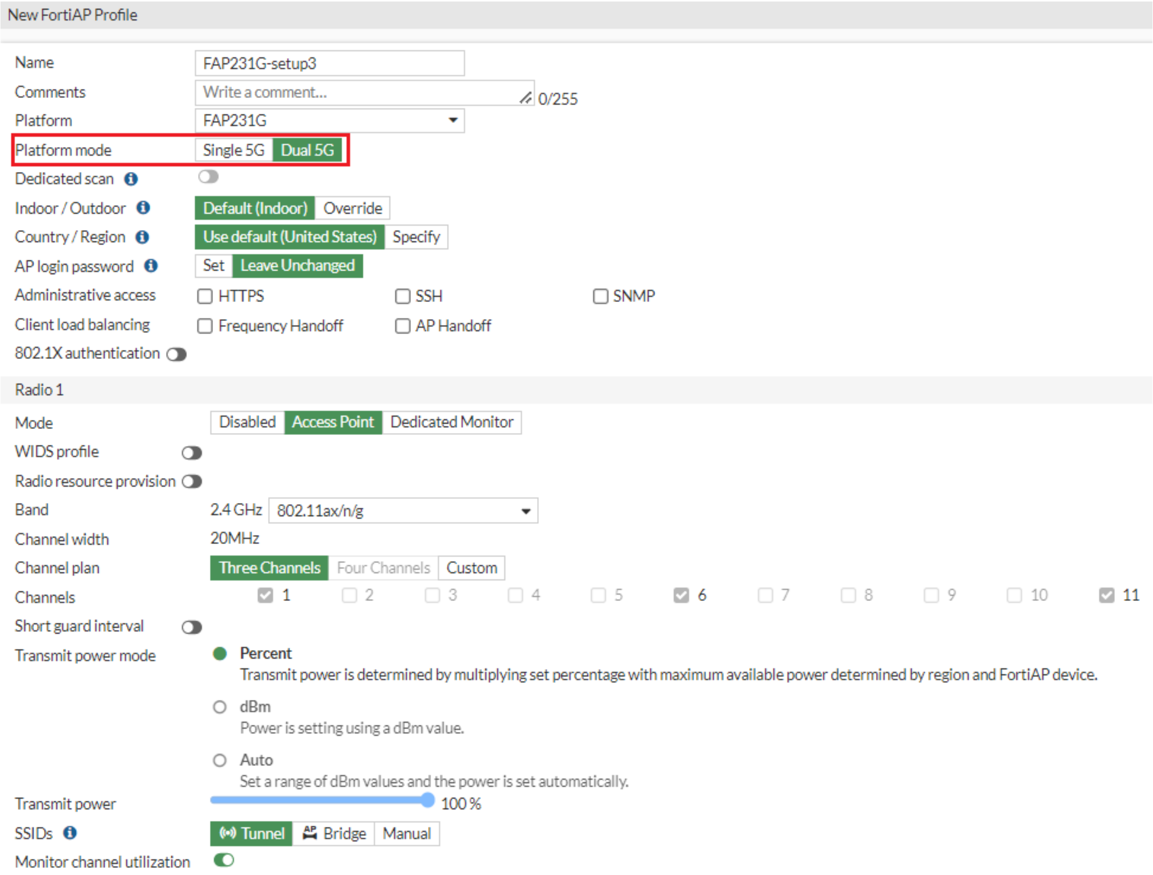
Radio 3

Mode	Disabled [✓ Dedicated Monitor]
WIDS profile	○

- **Platform mode: Dual 5G**

  In the setup, Radio 1 works on the 2.4GHz 802.11ax/n/g bands, Radio 2 works on the 5GHz 802.11ax/ac/n/a bands but is limited to lower 5GHz channels, and Radio 3 works on the 5GHz 802.11ax/ac/n/a bands but with higher 5GHz channels.

  Note: Dedicated scan is always disabled in Dual 5G mode.



New FortiAP Profile

Name: FAP231G-setup3

Comments: Write a comment... 0/255

Platform: FAP231G

Platform mode: Single 5G [✓ Dual 5G]

Dedicated scan

Indoor / Outdoor: [✓ Default (Indoor)] Override

Country / Region: [✓ Use default (United States)] Specify

AP login password: Set [✓ Leave Unchanged]

Administrative access: ☐ HTTPS ☐ SSH ☐ SNMP

Client load balancing: ☐ Frequency Handoff ☐ AP Handoff

802.1X authentication

Radio 1

Mode: Disabled [✓ Access Point] Dedicated Monitor

WIDS profile

Radio resource provision

Band: 2.4 GHz 802.11ax/n/g

Channel width: 20MHz

Channel plan: [✓ Three Channels] Four Channels Custom

Channels: ☑ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☑ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☑ 11

Short guard interval

Transmit power mode:

● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

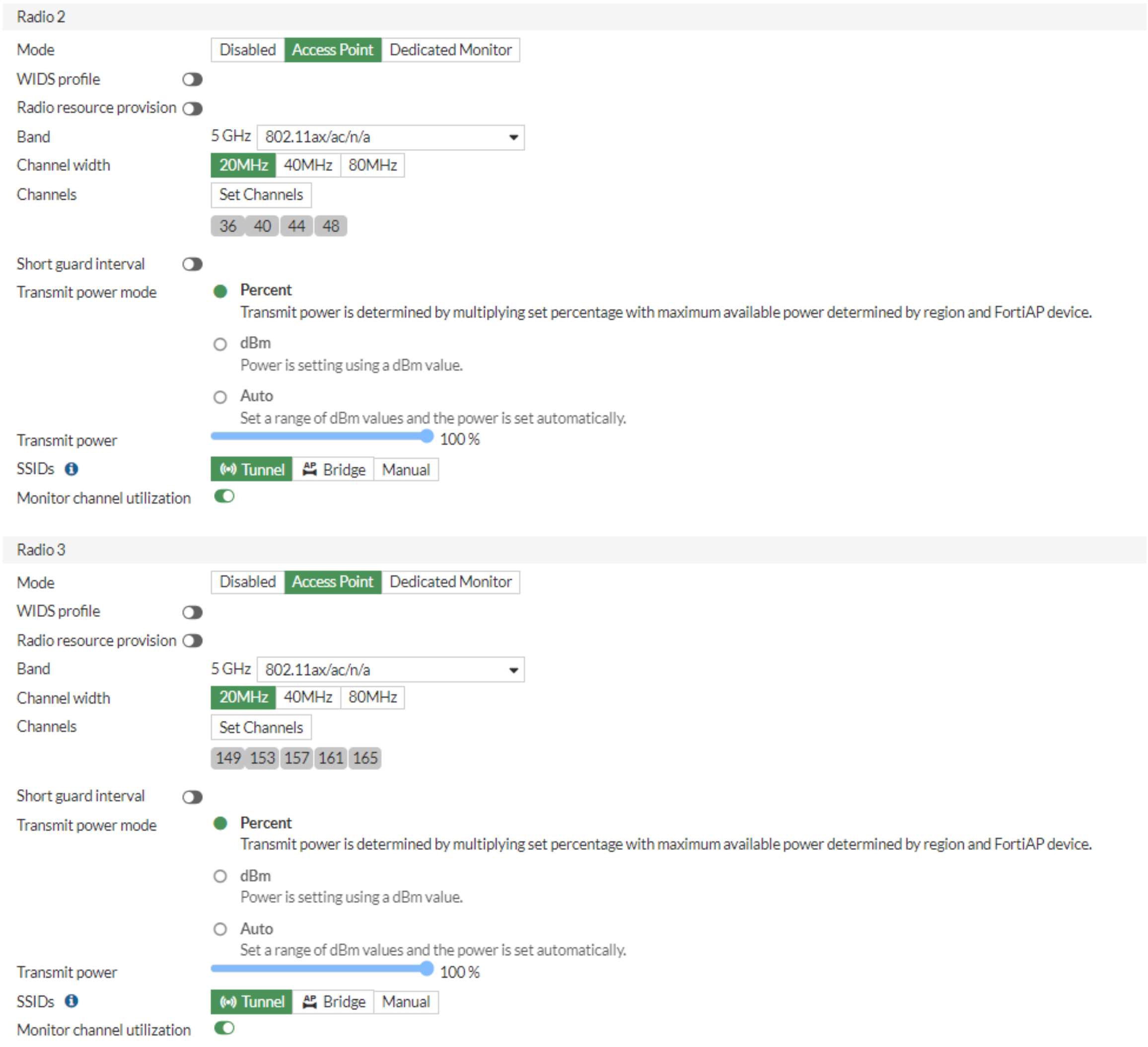
○ dBm
Power is setting using a dBm value.

○ Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 100 %

SSIDs: [✓ Tunnel] Bridge Manual

Monitor channel utilization



Radio 2

Mode: Disabled [✓ Access Point] Dedicated Monitor

WIDS profile ○

Radio resource provision ○

Band: 5 GHz 802.11ax/ac/n/a

Channel width: [✓ 20MHz] 40MHz 80MHz

Channels: Set Channels

36 40 44 48

Short guard interval ○

Transmit power mode:

● **Percent**
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

○ dBm
Power is setting using a dBm value.

○ Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 100 %

SSIDs: [✓ Tunnel] Bridge Manual

Monitor channel utilization ●

Radio 3

Mode: Disabled [✓ Access Point] Dedicated Monitor

WIDS profile ○

Radio resource provision ○

Band: 5 GHz 802.11ax/ac/n/a

Channel width: [✓ 20MHz] 40MHz 80MHz

Channels: Set Channels

149 153 157 161 165

Short guard interval ○

Transmit power mode:

● **Percent**
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

○ dBm
Power is setting using a dBm value.

○ Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 100 %

SSIDs: [✓ Tunnel] Bridge Manual

Monitor channel utilization ●

To configure a FortiAP G series profile - CLI:

FortiAP G series models support three different radio configuration setups:

- **Tri-band mode: Single 5G, Dedicated scan disabled**

```
config wireless-controller wtp-profile
  edit "FAP231G-setup1"
    config platform
      set type 231G
    end
    set handoff-sta-thresh 55
    config radio-1
      set band 802.11ax,n,g-only
      set channel "1" "6" "11"
    end
    config radio-2
      set band 802.11ax-5G
        set channel "36" "40" "44" "48" "149" "153" "157" "161" "165"
      end
```

```
   config radio-3
    set band 802.11ax-6G
    set channel "1" "5" "9" "13" "17" "21" "25" "29" "33" "37" "41" "45" "49" "53"
"57" "61" "65" "69" "73" "77" "81" "85" "89" "93" "97" "101" "105" "109" "113" "117"
"121" "125" "129" "133" "137" "141" "145" "149" "153" "157" "161" "165" "169" "173"
"177" "181" "189" "193" "197" "201" "205" "209" "213" "217" "221" "225" "229" "233"
  end
 next
end
```

Note: The default value of platform mode is `single-5G`, and the default value of `ddscan` is disabled, so they are not shown in CLI.

Note: For FortiAP G series models, 6GHz radio-3 as access point requires that VAPs must select one security mode from pure OWE, WPA3-SAE (`sae-h2e-only` must be enabled), WPA3-Enterprise, and WPA3-only-Enterprise.

- **Platform mode: Single 5G, Dedicated scan enabled**

  When `ddscan` is enabled, `radio-3` works only in `monitor` mode.

```
config wireless-controller wtp-profile
 edit "FAP231G-setup2"
  config platform
   set type 231G
   set ddscan enable
  end
  set handoff-sta-thresh 55
  config radio-1
   set band 802.11ax,n,g-only
   set channel "1" "6" "11"
  end
  config radio-2
   set band 802.11ax-5G
   set channel "36" "40" "44" "48" "149" "153" "157" "161" "165"
  end
  config radio-3
   set mode monitor
  end
 next
end
```

- **Platform mode: Dual 5G**

  When platform mode is set to `dual-5g`, `ddscan` is always disabled and `radio-3` 6GHz operation becomes unavailable.

```
config wireless-controller wtp-profile
 edit "FAP231G-setup3"
  config platform
   set type 231G
   set mode dual-5G
  end
  set handoff-sta-thresh 55
  config radio-1
   set band 802.11ax,n,g-only
   set channel "1" "6" "11"
  end
  config radio-2
```

```
          set band 802.11ax-5G
          set band-5g-type 5g-low
          set channel "36" "40" "44" "48"
        end
        config radio-3
          set band 802.11ax-5G
          set band-5g-type 5g-high
          set channel "149" "153" "157" "161" "165"
        end
      next
    end
```

WPA3 enhancements to support H2E only and SAE-PK - 7.2.1

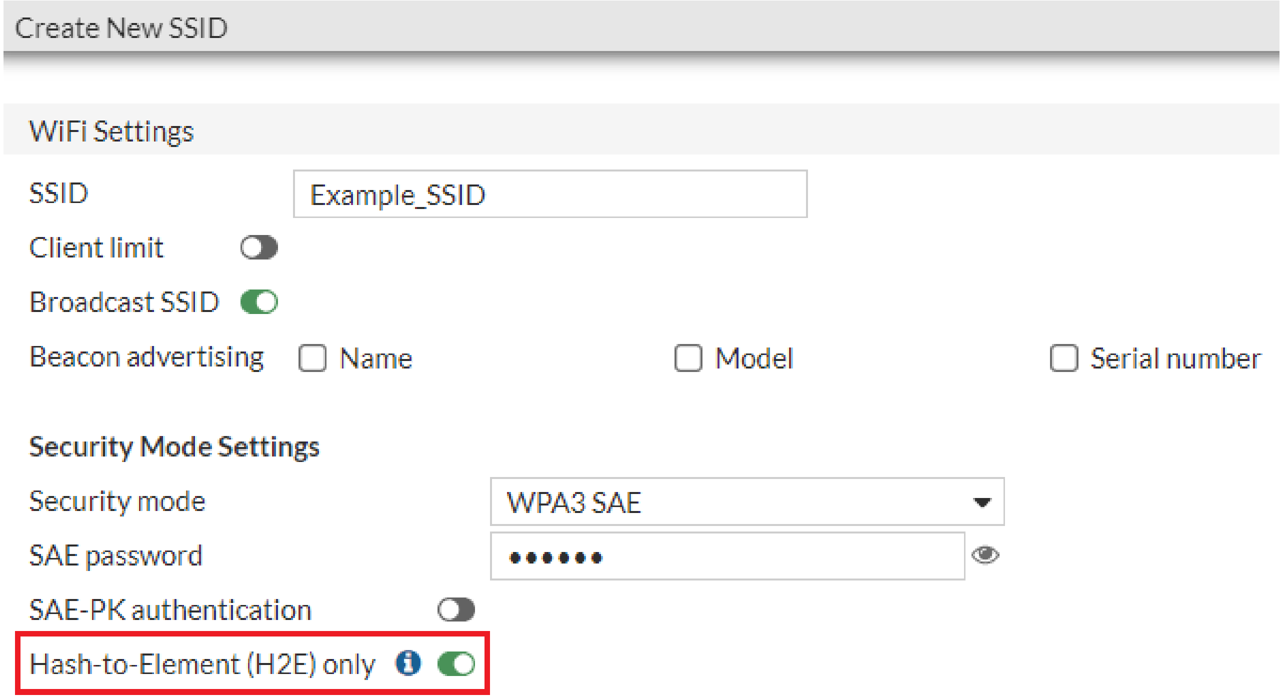
This release supports WiFi 6 Release 2 security enhancements by adding support for Hash-to-Element (H2E) only and Simultaneous Authentication of Equals Public Key (SAE-PK) for FortiAP models that support WPA3-SAE security modes.

When the security mode is set to WPA3-SAE or WPA3-SAE-Transition, the following options are available:

- **Hash-to-Element (H2E) only**: Use hash-to-element-only mechanism for PWE derivation.
- **Simultaneous Authentication of Equals Public Key (SAE-PK)**: Enable or disable WPA3 SAE-PK.
    - When SAE-PK authentication is enabled, you are required to set an SAE-PK private-key.

To enable H2E only - GUI:

1. From the FortiGate GUI, navigate to *WiFi & Switch Controller* > *SSIDs* and click *Create New* > *SSID*.
2. In *Security mode*, select either *WPA3-SAE* or *WPA3-SAE-Transition*.
3. In *SAE password*, enter a password.
4. Enable *Hash-to-Element (H2E) only*.



Create New SSID

WiFi Settings

SSID: Example_SSID

Client limit: ○

Broadcast SSID: ●

Beacon advertising: □ Name □ Model □ Serial number

Security Mode Settings

Security mode: WPA3 SAE

SAE password: ••••••

SAE-PK authentication: ○

Hash-to-Element (H2E) only: ●

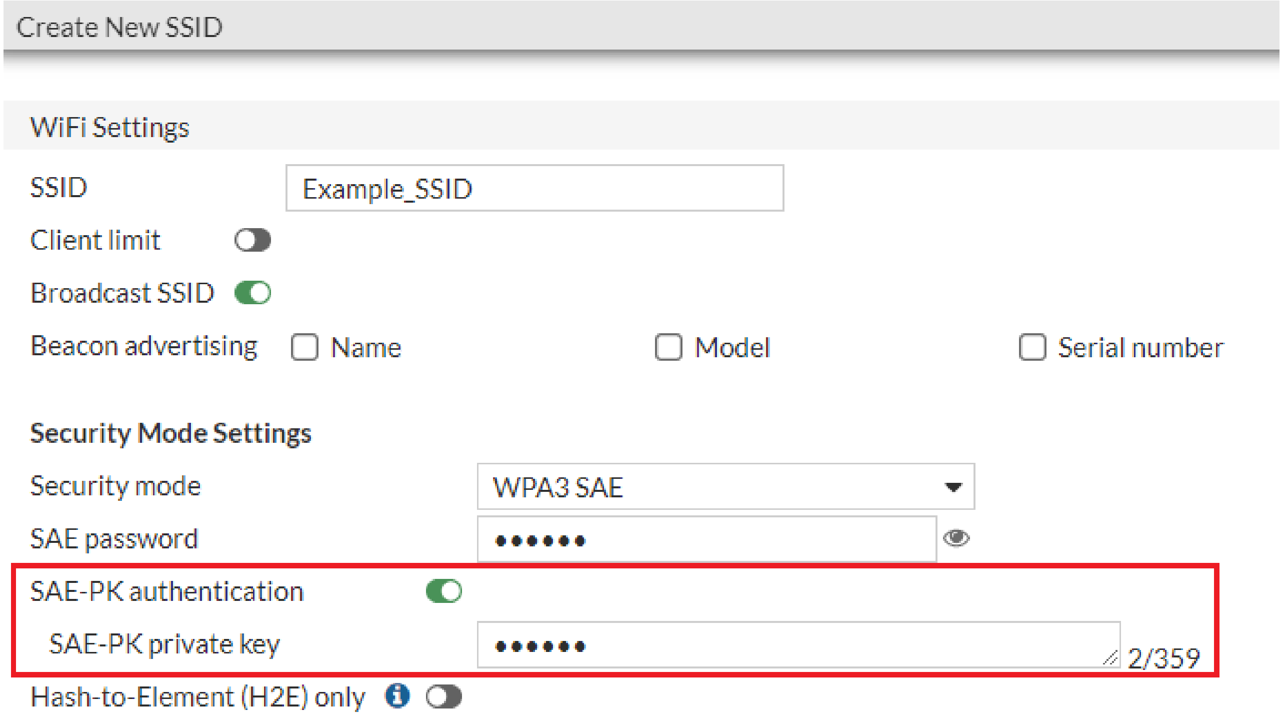
5. When you are finished, click *OK*.

To enable SAE-PK - GUI:

1. From the FortiGate GUI, navigate to *WiFi & Switch Controller* > *SSIDs* and click *Create New* > *SSID*.
2. In *Security mode*, select either *WPA3-SAE* or *WPA3-SAE-Transition*.
3. In *SAE password*, enter a password.
4. Enable *SAE-PK authentication*.

   When SAE-PK authentication option is enabled, the SAE-PK private key is mandatory.
5. In *SAE-PK private key*, enter a private key.

   The private key can be generated by a third-party tool (for example, sae_pk_gen in wpa_supplicant v2.10) to meet the encryption requirement. FortiOS will verify the private key and reject invalid input.



Create New SSID

WiFi Settings

SSID: Example_SSID

Client limit: ○

Broadcast SSID: ●

Beacon advertising: □ Name □ Model □ Serial number

Security Mode Settings

Security mode: WPA3 SAE

SAE password: ••••••

SAE-PK authentication: ●

SAE-PK private key: •••••• 2/359

Hash-to-Element (H2E) only: ○

6. When you are finished, click *OK*.

To enable H2E only - CLI:

```
config wireless-controller vap
  edit "wifi"
    set ssid "Example_SSID"
    set security wpa3-sae
    set pmf enable
    set sae-h2e-only enable
    set schedule "always"
    set sae-password ENC *
  next
end
```

To enable SAE-PK - CLI:

```
config wireless-controller vap
  edit "wifi"
    set ssid "Example_SSID"
    set security wpa3-sae
    set pmf enable
    set sae-pk enable
    set sae-private-key "******"
    set schedule "always"
    set sae-password ENC *
  next
end
```

Note: When SAE-PK authentication option is enabled, the sae-private-key is mandatory. The sae-private-key can be generated by a third-party tool (for example, sae_pk_gen in wpa_supplicant v2.10) to meet the encryption requirement. FortiOS will verify the private key and reject invalid input.

Implement multi-processing for wireless daemon for large-scale FortiAP management - 7.2.4

This information is also available in the FortiWiFi and FortiAP 7.2 Configuration Guide:

- How to implement multi-processing for large-scale FortiAP management

This release adds the ability to configure multiple processors for the wireless daemon (cw_acd) by leveraging multi-core CPU to scale large numbers of FortiAP per FortiGate Controller.

The new `acd-process-count` option allows users to specify the number of cw_acd processes to manage FortiAPs. For FortiGate managed APs, it splits the total number of FortiAPs into smaller groups where each cw_acd process manages a group. The cw_acd process won't be as overloaded, and if one cw_acd has an issue, it only affects that group of FortiAPs instead of all the FortiAPs managed by the FortiGate.

The maximum value you can specify in `acd-process-count` varies according to the `wireless-controller.wtp` in table size from different platforms.

wireless-controller.wtp	Maximum acd-process-count
8192	32
4096	16
512-1024	8
128-256	4
16-64	2

To configure multiple cw_acd processes:

In this example, there are about 1300 FortiAPs managed by a FortiGate with 16 cw_acd processes to handle all the FortiAPs.

1. Set the `acd-process-count` to `0` in `wireless-controller global`:

```
config wireless-controller global
  set acd-process-count 16
end
```

2. Verify the number of FortiAPs managed per cw_acd:

```
# diagnose wireless wlac -c mpmt
acd main  process pid     : 321
acd child process count   : 16
      idx=01 pid= 321 sl=N/A                  sm=/tmp/cwAcSock_mpmt_mngr sh=
      idx=02 pid= 376 sl=/tmp/cwCwAcSocket_data sm=/tmp/cwAcSock_mpmt_data sh=

    * idx=03 pid= 377 sl=/tmp/cwCwAcSocket    sm=/tmp/cwAcSock_mpmt    sh=
                    ws_cnt=1305 1283(RUN)   86(cfg) 1189(oper)
      idx=04 pid= 401 sl=/tmp/cwCwAcSocket_1  sm=/tmp/cwAcSock_mpmt_1  sh=/tmp/hasync_
to_cw_acd_unix_sock_1  ws_cnt=80     77(RUN)    4(cfg)   70(oper)
      idx=05 pid= 402 sl=/tmp/cwCwAcSocket_2  sm=/tmp/cwAcSock_mpmt_2  sh=/tmp/hasync_
to_cw_acd_unix_sock_2  ws_cnt=78     77(RUN)    5(cfg)   72(oper)
      idx=06 pid= 403 sl=/tmp/cwCwAcSocket_3  sm=/tmp/cwAcSock_mpmt_3  sh=/tmp/hasync_
to_cw_acd_unix_sock_3  ws_cnt=91     89(RUN)    6(cfg)   83(oper)
      idx=07 pid= 404 sl=/tmp/cwCwAcSocket_4  sm=/tmp/cwAcSock_mpmt_4  sh=/tmp/hasync_
to_cw_acd_unix_sock_4  ws_cnt=93     92(RUN)    6(cfg)   84(oper)
      idx=08 pid= 405 sl=/tmp/cwCwAcSocket_5  sm=/tmp/cwAcSock_mpmt_5  sh=/tmp/hasync_
to_cw_acd_unix_sock_5  ws_cnt=92     91(RUN)    7(cfg)   84(oper)
      idx=09 pid= 406 sl=/tmp/cwCwAcSocket_6  sm=/tmp/cwAcSock_mpmt_6  sh=/tmp/hasync_
to_cw_acd_unix_sock_6  ws_cnt=92     91(RUN)   10(cfg)   81(oper)
      idx=10 pid= 407 sl=/tmp/cwCwAcSocket_7  sm=/tmp/cwAcSock_mpmt_7  sh=/tmp/hasync_
to_cw_acd_unix_sock_7  ws_cnt=78     77(RUN)    4(cfg)   73(oper)
      idx=11 pid= 408 sl=/tmp/cwCwAcSocket_8  sm=/tmp/cwAcSock_mpmt_8  sh=/tmp/hasync_
to_cw_acd_unix_sock_8  ws_cnt=76     74(RUN)    5(cfg)   69(oper)
      idx=12 pid= 409 sl=/tmp/cwCwAcSocket_9  sm=/tmp/cwAcSock_mpmt_9  sh=/tmp/hasync_
to_cw_acd_unix_sock_9  ws_cnt=82     79(RUN)    9(cfg)   70(oper)
      idx=13 pid= 410 sl=/tmp/cwCwAcSocket_10 sm=/tmp/cwAcSock_mpmt_10 sh=/tmp/hasync_
to_cw_acd_unix_sock_10 ws_cnt=76     74(RUN)    4(cfg)   70(oper)
      idx=14 pid= 411 sl=/tmp/cwCwAcSocket_11 sm=/tmp/cwAcSock_mpmt_11 sh=/tmp/hasync_
to_cw_acd_unix_sock_11 ws_cnt=80     77(RUN)    6(cfg)   70(oper)
      idx=15 pid= 412 sl=/tmp/cwCwAcSocket_12 sm=/tmp/cwAcSock_mpmt_12 sh=/tmp/hasync_
to_cw_acd_unix_sock_12 ws_cnt=78     78(RUN)    5(cfg)   72(oper)
      idx=16 pid= 413 sl=/tmp/cwCwAcSocket_13 sm=/tmp/cwAcSock_mpmt_13 sh=/tmp/hasync_
to_cw_acd_unix_sock_13 ws_cnt=76     76(RUN)    5(cfg)   71(oper)
      idx=17 pid= 414 sl=/tmp/cwCwAcSocket_14 sm=/tmp/cwAcSock_mpmt_14 sh=/tmp/hasync_
to_cw_acd_unix_sock_14 ws_cnt=78     78(RUN)    5(cfg)   73(oper)
      idx=18 pid= 415 sl=/tmp/cwCwAcSocket_15 sm=/tmp/cwAcSock_mpmt_15 sh=/tmp/hasync_
to_cw_acd_unix_sock_15 ws_cnt=76     75(RUN)    1(cfg)   74(oper)
      idx=19 pid= 416 sl=/tmp/cwCwAcSocket_16 sm=/tmp/cwAcSock_mpmt_16 sh=/tmp/hasync_
to_cw_acd_unix_sock_16 ws_cnt=79     78(RUN)    4(cfg)   73(oper)
Curr Time: 683
```

Each cw_acd process handles a small number of FortiAPs, about 90.

3. Verify the CPU used by cw_acd:

```
# diagnose system top 5 30
Run Time:  0 days, 0 hours and 11 minutes
5U, 0N, 4S, 91I, 0WA, 0HI, 0SI, 0ST; 16063T, 8236F
            csfd      340      R      87.5     1.3    8
          cw_acd      377      S      12.9     6.5    6
          flpold      336      S       1.9     0.0    1
          cu_acd      325      S       1.4     0.1    0
          cw_acd      402      S       0.9     0.9    6
          cw_acd      401      S       0.9     0.9    2
          cw_acd      412      S       0.4     1.2    8
          cw_acd      404      S       0.4     1.0    10
          cw_acd      405      S       0.4     1.0    4
          cw_acd      403      S       0.4     1.0    2
          cw_acd      409      S       0.4     0.9    4
          cw_acd      408      S       0.4     0.9    6
          cw_acd      414      S       0.4     0.9    2
          cw_acd      413      S       0.4     0.9    8
            node      275      S       0.4     0.3    4
         miglogd      295      S       0.4     0.3    10
             cid      345      S       0.4     0.2    6
         miglogd      391      S       0.4     0.2    6
         miglogd      389      S       0.4     0.2    8
       forticron      282      S       0.4     0.1    6
          flcfgd      326      S       0.4     0.1    9
      fortilinkd      324      S       0.4     0.0    0
          cw_acd      376      S       0.0     2.8    3
          cw_acd      406      S       0.0     1.0    6
          cw_acd      411      S       0.0     0.9    10
          cw_acd      416      S       0.0     0.9    8
          cw_acd      407      S       0.0     0.9    2
          cw_acd      415      S       0.0     0.9    0
          cw_acd      410      S       0.0     0.8    4
         cmdbsvr      237      S       0.0     0.7    0

# get system performance status
CPU states: 5% user 3% system 0% nice 92% idle 0% iowait 0% irq 0% softirq
CPU0 states: 6% user 4% system 0% nice 90% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 5% system 0% nice 95% idle 0% iowait 0% irq 0% softirq
CPU2 states: 2% user 2% system 0% nice 96% idle 0% iowait 0% irq 0% softirq
CPU3 states: 0% user 2% system 0% nice 98% idle 0% iowait 0% irq 0% softirq
CPU4 states: 1% user 6% system 0% nice 93% idle 0% iowait 0% irq 0% softirq
CPU5 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU6 states: 37% user 2% system 0% nice 61% idle 0% iowait 0% irq 0% softirq
CPU7 states: 1% user 0% system 0% nice 99% idle 0% iowait 0% irq 0% softirq
CPU8 states: 9% user 13% system 0% nice 78% idle 0% iowait 0% irq 0% softirq
CPU9 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU10 states: 1% user 2% system 0% nice 97% idle 0% iowait 0% irq 0% softirq
CPU11 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 16448692k total, 7867592k used (47.8%), 8208572k free (49.9%), 372528k freeable
(2.3%)
Average network usage: 1710 / 942 kbps in 1 minute, 18999 / 19647 kbps in 10 minutes,
15826 / 16285 kbps in 30 minutes
Maximal network usage: 2804 / 1473 kbps in 1 minute, 27949 / 27754 kbps in 10 minutes,
31749 / 32829 kbps in 30 minutes
Average sessions: 2864 sessions in 1 minute, 2262 sessions in 10 minutes, 1995 sessions
in 30 minutes
Maximal sessions: 2941 sessions in 1 minute, 2945 sessions in 10 minutes, 2945 sessions
in 30 minutes
Average session setup rate: 1 sessions per second in last 1 minute, 5 sessions per
second in last 10 minutes, 7 sessions per second in last 30 minutes
Maximal session setup rate: 20 sessions per second in last 1 minute, 214 sessions per
second in last 10 minutes, 278 sessions per second in last 30 minutes
Average NPU sessions: 48 sessions in last 1 minute, 45 sessions in last 10 minutes, 40
sessions in last 30 minutes
Maximal NPU sessions: 52 sessions in last 1 minute, 59 sessions in last 10 minutes, 94
sessions in last 30 minutes
Average nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
Maximal nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
```

```
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days,  0 hours,  12 minutes
```

Each cw_acd uses about 1% of the CPU.

Allow custom RADIUS NAS-ID - 7.2.4

This information is also available in the FortiWiFi and FortiAP 7.2 Configuration Guide:

- Custom RADIUS NAS-ID

This enhancement allows users to configure the RADIUS NAS-ID as a custom ID or the hostname. When deploying a wireless network with WPA-Enterprise and RADIUS authentication, or using the RADIUS MAC authentication feature, FortiGate can use the custom NAS-ID in its Access-Request.

New CLI:

```
config user radius
  edit < server >
    set nas-id-type { legacy | custom | hostname }
    set nas-id < custom ID >
  next
end
```

You can configure `nas-id-type` with the following three options:

`legacy`	NAS-ID value is the value previously used by each daemon. This is the default setting.
`custom`	NAS-ID value is customized. Set `nas-id` to enter the custom ID.
`hostname`	NAS-ID value is the FortiGate hostname or HA group name if applicable.

To create an SSID with WPA2-Enterprise security mode using RADIUS authentication - CLI:

1. Configure the SSID:

```
config wireless-controller vap
 edit "wifi7"
   set ssid "80F_ent_radius"
   set security wpa2-only-enterprise
   set voice-enterprise disable
   set auth radius
   set radius-server "server-55"
   set schedule "always"
 next
end
```

2. Configure the RADIUS server:

```
 config user radius
  edit "server-55"
    set server "172.18.56.104"
    set secret ENC *
    set acct-interim-interval 60
    set radius-coa enable
    config accounting-server
      edit 1
        set status enable
        set server "172.18.56.104"
        set secret ENC *
      next
    end
  next
end
```

3. Set the `nas-id-type`:

```
config user radius
  edit server-55
    set nas-id-type hostname
 next
end

config system global
  set hostname "FortiWiFi-80F-2R"
end
```

4. After the station connects to the SSID, check the radius packets to confirm the NAS-Identifier value matches the hostname FortiWiFi-80F-2R:

```
(64) Received Access-Request Id 35 from 172.16.200.254:63111 to 172.16.200.55:1812
length 367
(64)   User-Name = "tester"
(64)   NAS-IP-Address = 0.0.0.0
(64)   NAS-Identifier = "FortiWiFi-80F-2R"
```

To create a WPA2-Personal SSID using RADIUS MAC authentication - CLI:

1. Configure the SSID:

```
config wireless-controller vap
  edit "wifi2"
    set ssid "80F_psk"
    set voice-enterprise disable
    set radius-mac-auth enable
    set radius-mac-auth-server "server-55"
    set passphrase ENC *
    set schedule "always"
  next
end
```

2. Set the `nas-id-type`:

```
config user radius
  edit server-55
    set nas-id-type custom
    set nas-id FWF-80F-LR
  next
end
```

3. After the station connects to the SSID, check the radius packets to confirm the NAS-Identifier value matches the custom value you configured, "FWF-80F-LR":

```
(87) Received Access-Request Id 3 from 172.16.200.254:62884 to 172.16.200.55:1812 length
228
(87)   User-Name = "F1-A4-23-75-9F-B1"
(87)   User-Password = "F1-A4-23-75-9F-B1"
(87)   Calling-Station-Id = "F1-A4-23-75-9F-B1"
(87)   NAS-IP-Address = 0.0.0.0
(87)   NAS-Identifier = "FWF-80F-LR"
```

Support wireless client mode on FortiWiFi 80F series models - 7.2.4

This information is also available in the FortiWiFi and FortiAP 7.2 Configuration Guide:

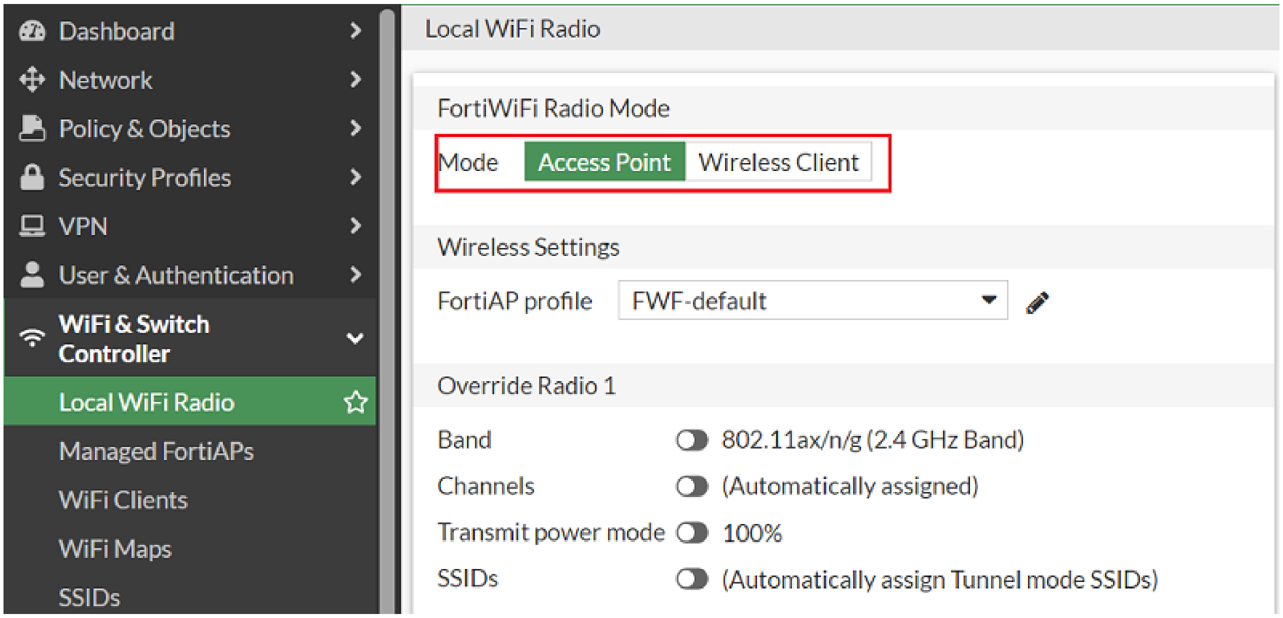
- FortiWiFi unit as a wireless client
- Configuring a FortiWiFi unit as a wireless client

This release supports wireless client mode on FortiWiFi 80F series models. When wireless client mode is successfully configured, a default static route to the "aplink" interface is automatically created. To allow outgoing traffic to use this wireless client connection, you must configure a firewall policy from the wired internal/LAN interface as the source interface to the "aplink" interface as the destination interface.

Before setting up the FortiWiFi unit as a wireless client using the steps described below, make sure to remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and software switch members using the CLI or GUI.

To configure wireless client mode - GUI:

1. Go to *WiFi and Switch Controller > Local WiFi Radio* and change the *Mode* to *Wireless Client*.



Mode: Access Point | Wireless Client

FortiAP profile: FWF-default

Band: 802.11ax/n/g (2.4 GHz Band)

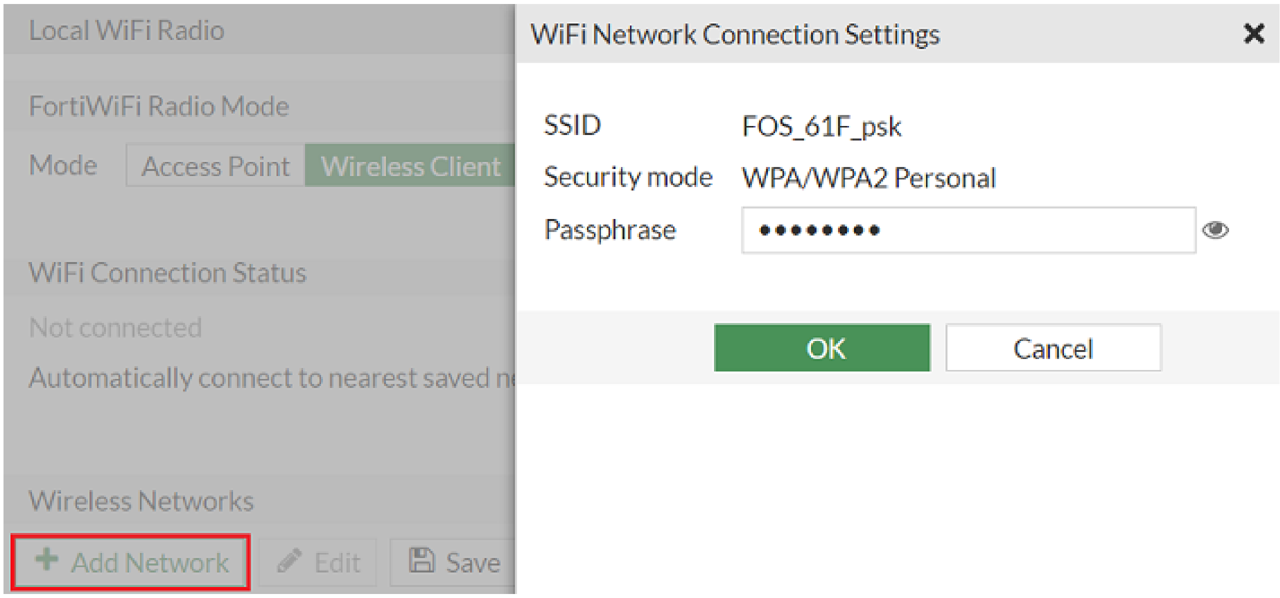
Channels: (Automatically assigned)

Transmit power mode: 100%

SSIDs: (Automatically assign Tunnel mode SSIDs)

Note: You must remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and software switch members before you can change the mode to Wireless Client. Once you select Wireless Client, the FortiWiFi unit will reboot.

2. Click *Add Network* and select an SSID to set up the WiFi connection.

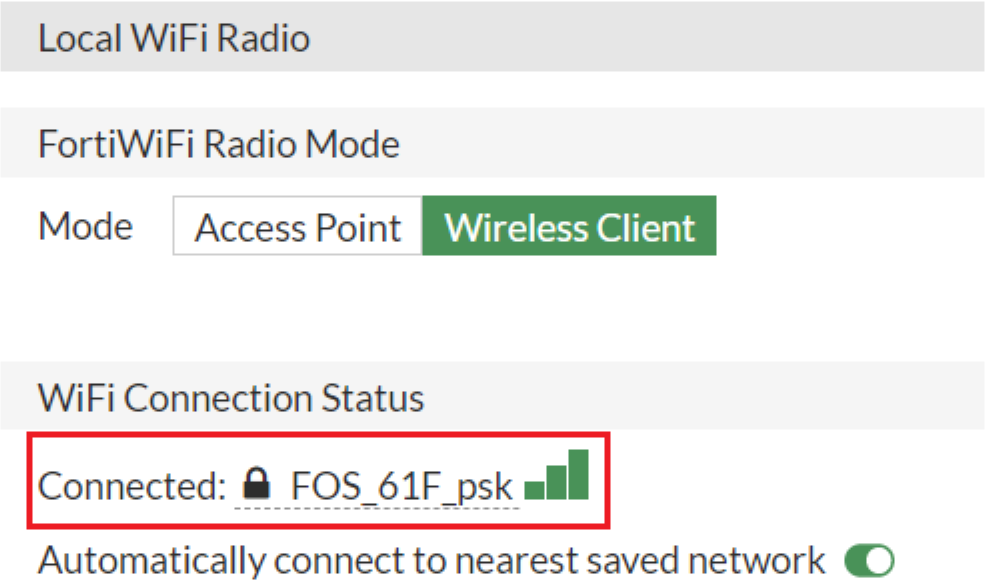


SSID: FOS_61F_psk

Security mode: WPA/WPA2 Personal

Passphrase: ••••••••

3. Click *OK* to save the WiFi Network Connection Setting.
4. From the Local WiFi Radio page, verify that the WiFi network is connected.



Local WiFi Radio

FortiWiFi Radio Mode

Mode: Access Point | Wireless Client (selected)

WiFi Connection Status

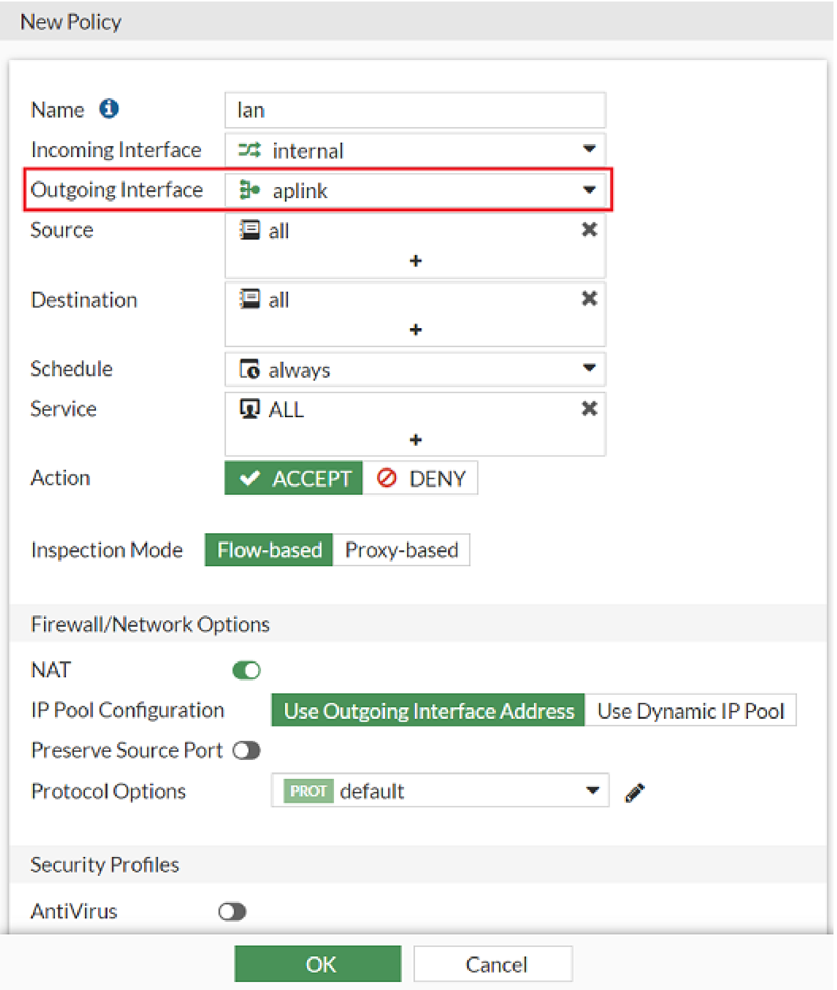
Connected: 🔒 FOS_61F_psk

Automatically connect to nearest saved network: on

5. Go to *Policy & Object* > *Firewall Policy* and click *Create New* to create a firewall policy.
6. Enter the following policy information:

Incoming Interface	*internal*
Outgoing Interface	*aplink*

For FortiWiFi 80F series models, you *must* select "aplink" as the destination interface in the firewall policy. Older FortiWiFi models must select "wifi" as the destination interface.



New Policy

Name: lan
Incoming Interface: internal
Outgoing Interface: aplink
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ACCEPT | DENY
Inspection Mode: Flow-based | Proxy-based

Firewall/Network Options

NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

Security Profiles

AntiVirus: ○

7. Configure remaining fields as needed, when you are finished, click *OK*.
8. Connect a wired station to the internal ports of the FortiWiFi to verify that it can pass traffic to the Internet.

To configure wireless client mode - CLI:

1. Change the wireless mode to client.

```
config system global
  set wireless-mode client
end
```

Note: You must remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and software switch members before you can change the mode to Wireless Client. Once you select Wireless Client, the FortiWiFi unit will reboot.

2. 2. Set up a wifi-network entry under interface "wifi".

```
config system interface
  edit "wifi"
    config wifi-networks
      edit 1
        set wifi-ssid "FOS_61F_psk"
        set wifi-passphrase *
      next
    end
  next
end
```

3. Verify that the network connection is connected.

```
FortiWiFi-80F-2R # diagnose wireless-controller wlsta cfg
STA intf        name: wlan17
              status: up
                  ip: 10.10.80.4
                 mac: d5:73:a0:7d:49:27
        auto connect: yes
           auto save: no
             ap band: any
    wifi network cnt: 1
                   1: FOS_61F_psk, 8, 1
           connected: FOS_61F_psk
```

4. Once you verify the connection, confirm that the default routing to "aplink" is added as static entry.

```
config router static
  edit 1
    set gateway 192.168.80.2
    set device "aplink"
  next
end
FortiWiFi-80F-2R # get router info routing-table details
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 192.168.80.2, aplink, [1/0]
```

5. Create a firewall policy from "internal" to "aplink".

For FortiWiFi 80F series models, you *must* select "aplink" as the destination interface in the firewall policy. Older FortiWiFi models must select "wifi" as the destination interface.

```
config firewall policy
  edit 1
    set name "lan"
    set srcintf "internal"
    set dstintf "aplink"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

6. Connect a wired station to the internal ports of the FortiWiFi to verify that it can pass traffic to the Internet.

Support displaying details about wired clients connected to the FortiAP LAN port - 7.2.4

This information is also available in the FortiWiFi and FortiAP 7.2.4 Configuration Guide:

- LAN port options

This enhancement enables the FortiGate to display details about wired clients when they are connected to a FortiAP LAN port and both the FortiGate and FortiAP have WAN-LAN operation and LAN Port Mode options configured. The wired clients must be connected to FortiAP via the following:

- Connected to the LAN port on FortiAP models with LAN and WAN ports.
- Connected to the LAN2 port on FortiAP models with dual LAN1 and LAN2 ports.

  By default, LAN1 and LAN2 are direct pass-through ports and must be re-configured for WAN-LAN operation. See Configuring a port to WAN-LAN operation mode for more information.

Important information such as the client's mode of connection, Tx/Rx rate, authentication status, OS details are pushed from the FortiAP to the FortiGate. The information is displayed in the FortiGate CLI using `diagnose wireless-controller wlac -c lan-sta` and in the FortiAP CLI using `cw_diag -c k-lan-host`.

To see client application usage over bridge mode SSIDs, see Report wireless client app usage for clients connected to bridge mode SSIDs on page 477.

To configure FortiAP models with dual LAN ports for WAN-LAN operation:

1. Create a FortiAP profile on the FortiGate.

```
config wireless-controller wtp-profile
  edit "231F-lann"
    config platform
      set type 231F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    config radio-1
      set band 802.11ax,n,g-only
    end
    config radio-2
      set band 802.11ax-5G
    end
    config radio-3
      set mode monitor
    end
  next
end
```

2. Create an SSID for the FortiAP profile. You can create either a tunnel or bridge SSID.

```
config wireless-controller vap
  edit "Example_SSID"
    set ssid "Example_SSID"
    set passphrase ENC *
    set schedule "always"
    set quarantine disable
  next
end
```

3. In the FortiAP profile you created, configure WAN-LAN mode and then select a port mode option.

   Note: This example uses bridge-to-ssid as the port mode, but you can use other port modes such as nat-to-wan or bridge-to-wan for collecting wired client details.

```
config wireless-controller wtp-profile
  edit "231F-lann"
    set wan-port-mode wan-lan
    config lan
      set port-mode bridge-to-ssid
      set port-ssid "Example_SSID"
    end
  next
end
```

4. Apply the FortiAP profile to the FortiAP unit.

```
 config wireless-controller wtp
  edit "FP231FTF20007509"
    set admin enable
    set wtp-profile "231F-lann"
  next
end
```

5. From the FortiAP CLI, execute the following commands to enable LAN-WAN mode.

```
FortiAP-231F # cfg -a WANLAN_MODE=WAN-LAN
FortiAP-231F # cfg -c
```

To display details about connected wired clients:

Once the FortiGate and FortiAP have WAN-LAN operation and LAN Port Mode options configured, you can collect data about the connected wired clients.

1. Connect a wired client to the FortiAP and connect the FortiAP to the FortiGate.

   The FortiAP LAN1 port must be connected to the FortiGate.

   The FortiAP LAN2 port must be connected to the wired clients, either directly to the LAN2 port or through a switch connected to LAN2.

2. On the FortiAP CLI, run command `cw_diag -c k-lan-host` (or) `lsta` to verify collected wired client information.

```
FortiAP-231F # lsta
WTP Kernel LAN Hosts:
Idle timeout: 300
index= 0/ 1 pId= 0 mac=00:24:9b:79:df:48 vlanid=0 auth=No
       host_info=VAN-301127-PC1 vci=MSFT 5.0 os_info=Windows
       ip=95.1.1.2 ip_proto=arp ip_age=36
```

```
        ip6=fe80::ddaa:41b0:4633:30dd ip6_proto=arp ip6_age=4846 ip6_rx_pkts=666
        rx_bytes=7218797 rx_rate=64.00bps rx_pkts=33620 last_rx_age=21
        tx_bytes=15441777 tx_rate=48.00bps tx_pkts=29080 last_tx_age=11

Total LAN Hosts: 1
```

3. Confirm that FortiGate has received the wired client details from the AP by running the diagnostic command `diagnose wireless-controller wlac -c lan-sta`.

```
FortiGate-81E-POE (root) # diagnose wireless-controller wlac -c lan-sta
-------------------------------LAN STA    1----------------------------
LAN STA mac     : 00:24:9b:79:df:48 (0-1.1.1.2:5246)
    pId         : 0  BR-TO-TUN-SSID Example_SSID
    vlan        : 0
    macauth     : No
    ip          : 95.1.1.2  ARP  48 seconds
    ip6         : fe80::ddaa:41b0:4633:30dd  ARP  4945 seconds  666 pkts
    host info   : VAN-301127-PC1
    vci info    : MSFT 5.0
    os info     : Windows
    uplink      : 226.00bps 33637 pkts 7221244 bytes 9 seconds
    downlink    : 31.00bps 29085 pkts 15442358 bytes 9 seconds
-------------------------------Total    1 LAN STAs----------------------------
```

Simplify BLE iBeacon provisioning for RTLS deployments - 7.2.5

This information is also available in the FortiWiFi and FortiAP 7.2.5 Configuration Guide:

- Bluetooth Low Energy scan

This enhancement simplifies Bluetooth Low Energy (BLE) iBeacon provisioning for the BLE major and minor IDs with the following changes:

- The BLE major ID can be set in WTP settings and WTP group settings as well as in the BLE profile settings.
  - The BLE major ID set in the WTP settings overrides the ID set in the WTP group and the BLE profile.
  - The BLE major ID set in the WTP group settings overrides the ID set in the BLE profile.
- The BLE minor ID can be set in WTP settings and in the BLE profile settings.
  - The BLE minor ID set in the WTP settings overrides the ID set in the BLE profile.

To set BLE major and minor IDs from the WTP settings:

```
config wireless-controller wtp
  edit < FortiAP-serial-number >
    set ble-major-id < ID >
    set ble-minor-id < ID >
  next
end
```

To set BLE major IDs from the WTP group settings:

```
config wireless-controller wtp-group
  edit < FortiAP-group-name >
```

```
    set ble-major-id < ID >
    set wtps < FortiAP-serial-number-1 > < FortiAP-serial-number-2 > ...
  next
end
```

To override BLE major and minor IDs:

1. Create a BLE profile:

   ```
   config wireless-controller ble-profile
       edit "ble"
           set advertising ibeacon eddystone-uid eddystone-url
           set major-id 3456
           set minor-id 1234
           set txpower 8
           set ble-scanning enable
       next
   end
   ```

2. From a WTP profile, enable the BLE profile.

   ```
   config wireless-controller wtp-profile
     edit "FAP431F-default"
       config platform
         set type 431F
         set ddscan enable
       end
       set ble-profile "ble"
       set handoff-sta-thresh 55
       config radio-1
         set band 802.11ax,n,g-only
       end
       config radio-2
         set band 802.11ax-5G
       end
       config radio-3
         set mode monitor
       end
     next
   end
   ```

3. Override the `ble-major-id` and `ble-minor-id` setting.

   ```
   config wireless-controller wtp
     edit FP431FTF00000001
       set ble-major-id 10013
       set ble-minor-id 1008
     next
   end
   ```

4. Verify that the BLE IDs have been changed from the FortiAP CLI.

   ```
   FortiAP-431F # cw_diag -c ble-config

   WTP Bluetooth Low Energy Configuration:
           ble scan report interval : 30
           advertising : ibeacon eddystone-uid eddystone-url
           ibeacon_uuid : 005ea314-cbd1-11e5-9956-625672870761
   ```

```
        major ID : 10013
        minor ID : 1008
        eddystone namespace ID : 0102030405
        eddystone instance ID : abcdef
        eddystone URL : http://www.fortinet.com
        txpower : 8
        beacon interval : 100
        ble scanning : enabled

BLE address: 04:d5:90:e9:f3:17
```

5. You can also override the `ble-major-id` from the WTP group.

```
config wireless-controller wtp-group
  edit "FP-GROUP"
    set ble-major-id 45666
    set wtps "FP431FTF00000001"
  next
end
```

Switch controller

This section includes information about switch-controller-related new features:

- Automatic updating of the port list when switch split ports are changed on page 534
- Use wildcard serial numbers to pre-authorize FortiSwitch units on page 534
- Allow multiple managed FortiSwitch VLANs to be used in a software switch on page 535
- Allow a LAG on a FortiLink-enabled software switch on page 536
- Configure MAB reauthentication globally or locally on page 537
- Enhanced FortiSwitch Topology view on page 538
- Support dynamic discovery in FortiLink mode over a layer-3 network on page 540
- Configure flap guard through the switch controller on page 541
- Allow FortiSwitch console port login to be disabled on page 542
- Configure multiple flow-export collectors on page 543
- Enhanced FortiSwitch Ports page and Diagnostics and Tools pane on page 544
- Manage FortiSwitch units on VXLAN interfaces on page 544
- Add new FortiSwitch Clients page on page 547
- Automatic revision backup upon FortiSwitch logout or firmware upgrade 7.2.1 on page 550
- Configure the frequency of IGMP queries 7.2.1 on page 550
- Add FortiView Internal Hubs monitor 7.2.4 on page 551
- Configure DHCP-snooping static entries 7.2.4 on page 554
- Track device traffic statistics when NAC is enabled 7.2.4 on page 555
- Enhance switch PoE port settings 7.2.4 on page 557
- Increase the number of NAC devices supported 7.2.4 on page 557

Automatic updating of the port list when switch split ports are changed

In previous releases, changing FortiSwitch split ports and then restarting the managed FortiSwitch unit caused the FortiGate device to have to rediscover and re-authorize the FortiSwitch unit. Now, the FortiGate device automatically updates the port list after split ports are changed and the FortiSwitch unit restarts. When split ports are added or removed, the changes are logged.

If there are any configuration errors with the split ports, you can use one of the following commands to check the errors and fix them:

- `execute switch-controller get-sync-status all`
- `execute switch-controller get-sync-status switch-id <FortiSwitch_serial_number>`

Use wildcard serial numbers to pre-authorize FortiSwitch units

You can now use asterisks as a wildcard character when you pre-authorize FortiSwitch units. Using a FortiSwitch template, you can name the managed switch and configure the ports. When the FortiSwitch unit is turned on and discovered by the FortiGate device, the wildcard serial number is replaced by the actual serial number and the settings in the FortiSwitch template are applied to the discovered FortiSwitch unit.

When you create the FortiSwitch template, use the following format for the wildcard serial number:

```
PREFIX****nnnnnn
```

PREFIX	The first six digits of a valid FortiSwitch serial number, such as S248EP, S124EN, S548DF, and S524DF.
****	Asterisks are the only wildcard characters allowed. You can have any number of asterisks, as long as ****nnnnnn is no longer than 10 characters.
nnnnnn	You can have any number of valid alphanumeric characters, as long as ****nnnnnn is no longer than 10 characters.

To pre-authorize FortiSwitch units using a FortiSwitch template:

1. Create a FortiSwitch template.

```
config switch-controller managed-switch
   edit <PREFIX****nnnnnn>
      ...
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S248EP****000000"
      set name "fortilink-FSW248EP1"
      set fsw-wan1-peer "fortilink"
      .......
      config ports
         edit "port1"
            set vlan "onboarding"
            set allowed-vlans "quarantine" "nac_segment"
            set untagged-vlans "quarantine" "nac_segment"
            set access-mode nac
```

```
                set export-to "root"
             next
             edit "port2"
                set vlan "_default"
                set allowed-vlans "quarantine"
                set untagged-vlans "quarantine"
                set access-mode dynamic
                set port-policy "aggr1"
                set export-to "root"
             next
          end
       next
    end
```

2. Turn on the FortiSwitch unit so that the FortiGate device will discover it.

   The FortiSwitch unit is matched with the FortiSwitch template using the order of entries in the CMDB table from top to bottom. The settings in the FortiSwitch template are applied to the discovered FortiSwitch unit. Once a match is made for a wildcard entry, that particular entry is consumed.

Allow multiple managed FortiSwitch VLANs to be used in a software switch

You can now add multiple managed FortiSwitch VLANs to a software switch using the GUI or CLI. In previous releases, you could add only one managed FortiSwitch VLAN per FortiGate device to a software switch.

Traffic between two VLANs is controlled by the `intra-switch-policy` setting under the `config system switch-interface` command. By default, `intra-switch-policy` is set to `implicit`, which allows traffic between software switch members.

The FortiSwitch VLANs must be configured without IP addresses.

Using the GUI

1. Go to *Network* > *Interfaces*.
2. Create or edit a software switch interface
3. In *Interface members*, select multiple FortiSwitch VLANs.
4. Click *OK*.

Using the CLI

In the following example, you create two managed FortiSwitch VLANs and then add them to a software switch.

```
config system interface
   edit "vlan1"
      set vdom "root"
      set device-identification enable
      set role lan
      set snmp-index 46
      set interface "fortilink"
      set vlanid 3501
   next
   edit "vlan2"
```

```
      set vdom "root"
      set device-identification enable
      set role lan
      set snmp-index 47
      set interface "fortilink"
      set vlanid 3502
   next
end

config system switch-interface
   edit "softwareswitch"
      set vdom "root"
      set member "vlan1" "vlan2"
   next
end
```

Allow a LAG on a FortiLink-enabled software switch

You can now configure a link-aggregation group (LAG) as a member of a software switch that is being used for FortiLink. Previously, you could not add a LAG to a software switch that was being used for FortiLink.

- You must set `fortilink-neighbor-detect` to `lldp`.
- Aggregate interfaces do not automatically form an inter-switch link (ISL) within a FortiGate software switch. You must create the aggregate interfaces and add them to the software switch.
- The FortiSwitch unit will automatically form an ISL with correctly configured FortiGate aggregate interfaces.

In the following example, aggregate1 and aggregate2 are FortiGate aggregate interfaces. The third interface, switch3, is a software switch with FortiLink enabled. The three interfaces are configured, and then aggregate1 and aggregate2 are added to the software switch interface.

```
config system interface
   edit "aggregate1"
      set vdom "root"
      set type aggregate
      set member "port11"
      set device-identification enable
      set role lan
      set snmp-index 25
   next
   edit "aggregate2"
      set vdom "root"
      set type aggregate
      set member "port7"
      set device-identification enable
      set role lan
      set snmp-index 34
   next
   edit "switch3"
      set vdom "root"
      set fortilink enable
      set ip 10.255.1.1 255.255.255.0
      set allowaccess ping fabric
      set type switch
      set lldp-reception enable
      set lldp-transmission enable
      set snmp-index 26
      set fortilink-neighbor-detect lldp
      set swc-first-create 64
      config ipv6
         set ip6-send-adv enable
         set ip6-other-flag enable
      end
   next
end

config system switch-interface
   edit "switch3"
      set vdom "root"
      set member "aggregate1" "aggregate2"
   next
end
```

Configure MAB reauthentication globally or locally

You can enable the MAC Authentication Bypass (MAB) option for devices (such as network printers) that cannot respond to the 802.1x authentication request. With MAB enabled on the port, the system will use the device MAC address as the user name and password for authentication. If a link goes down, you can select whether the impacted devices must reauthenticate. By default, reauthentication is disabled. You can use the FortiOS CLI to enable MAB reauthentication globally or locally:

- On the global level, use the new `set mab-reauth` command to enable or disable MAB reauthentication.
- On the local level, you can override the 802.1x settings for a specific managed switch and then use the new `set mab-reauth` command to enable or disable MAB reauthentication.

To control MAB reauthentication on the global level:

```
config switch-controller 802-1X-settings
   set mab-reauth {enable | disable}
end
```

To enable MAB reauthentication on the global level:

```
config switch-controller 802-1X-settings
   set mab-reauth enable
end
```

To control MAB reauthentication on the local level:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config 802-1X-settings
         set local-override enable
         set mab-reauth {enable | disable}
      next
   end
end
```

To enable MAB reauthentication on the local level:

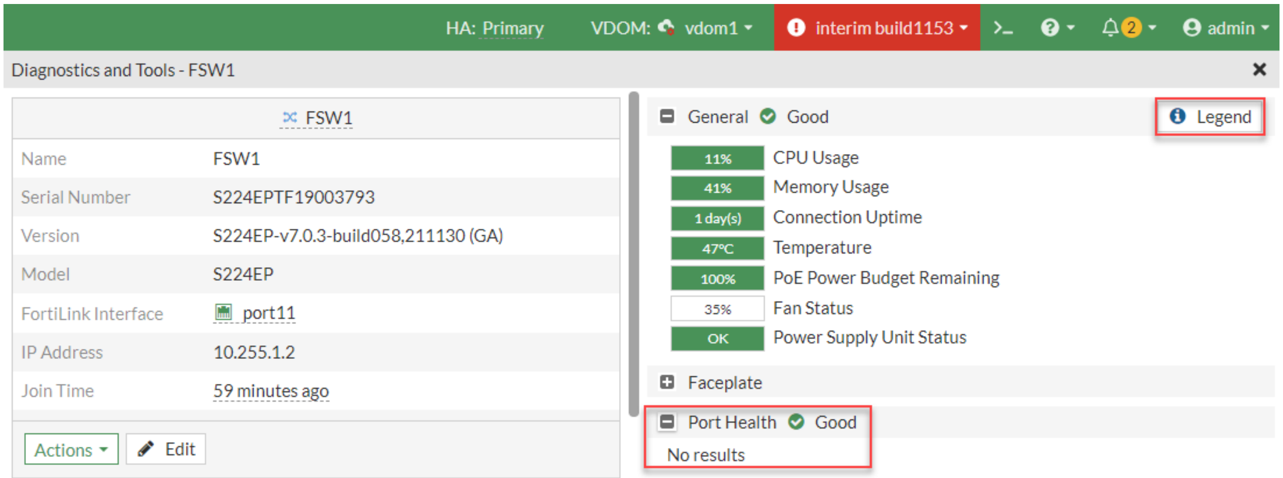
```
config switch-controller managed-switch
   edit S548DF5018000776
      config 802-1X-settings
         set local-override enable
         set mab-reauth enable
      next
   end
end
```

Enhanced FortiSwitch Topology view

There are three enhancements in the GUI for managed FortiSwitch units:

- The port health is now reported on the *Diagnostics and Tools* pane.

  Go to *WiFi & Switch Controller > Managed FortiSwitches*, right-click a FortiSwitch unit in Topology view or List view, and select *Diagnostics and Tools*. When there are error frames, the port health is shown as *Poor*. When there are no error frames, the port health is shown as *Good*.



Diagnostics and Tools - FSW1

FSW1	
Name	FSW1
Serial Number	S224EPTF19003793
Version	S224EP-v7.0.3-build058,211130 (GA)
Model	S224EP
FortiLink Interface	port11
IP Address	10.255.1.2
Join Time	59 minutes ago

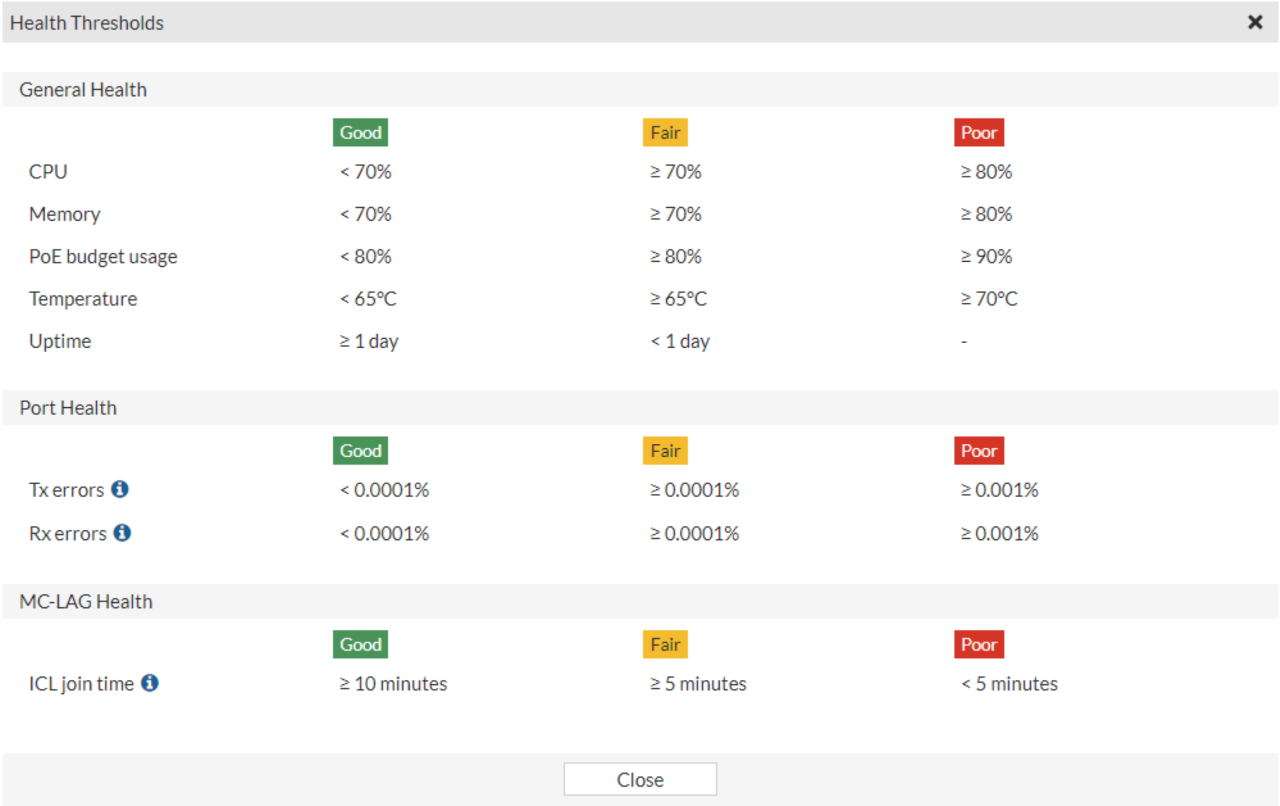
General ✓ Good

11%	CPU Usage
41%	Memory Usage
1 day(s)	Connection Uptime
47°C	Temperature
100%	PoE Power Budget Remaining
35%	Fan Status
OK	Power Supply Unit Status

Port Health ✓ Good

No results

- The new *Legend* button in the *General* pane displays the *Health Thresholds* pane, which lists the thresholds for the good, fair, and poor ratings of the general health, port health, and MC-LAG health.



Health Thresholds

General Health

	Good	Fair	Poor
CPU	< 70%	≥ 70%	≥ 80%
Memory	< 70%	≥ 70%	≥ 80%
PoE budget usage	< 80%	≥ 80%	≥ 90%
Temperature	< 65°C	≥ 65°C	≥ 70°C
Uptime	≥ 1 day	< 1 day	-

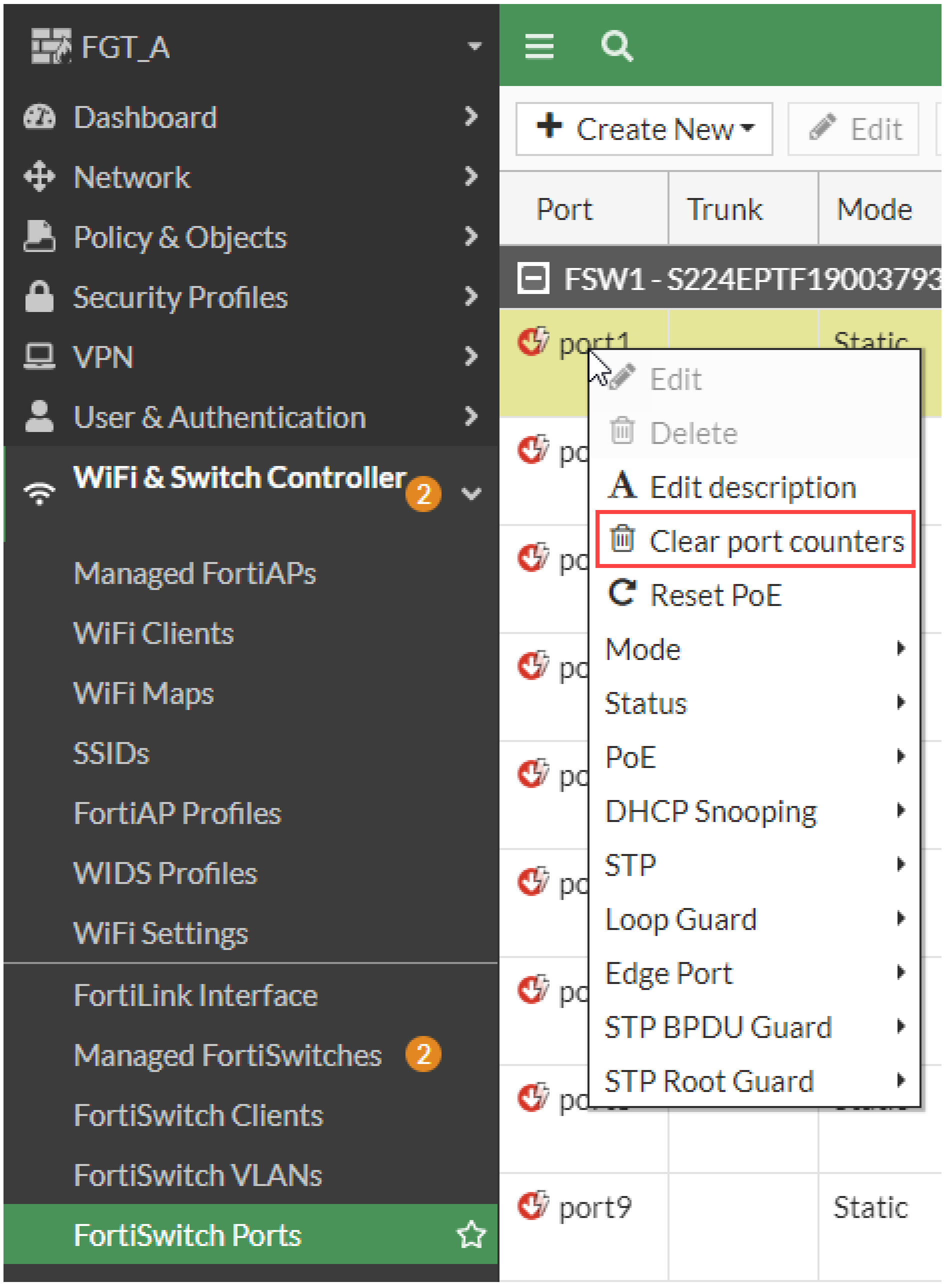
Port Health

	Good	Fair	Poor
Tx errors ℹ	< 0.0001%	≥ 0.0001%	≥ 0.001%
Rx errors ℹ	< 0.0001%	≥ 0.0001%	≥ 0.001%

MC-LAG Health

	Good	Fair	Poor
ICL join time ℹ	≥ 10 minutes	≥ 5 minutes	< 5 minutes

- You can now clear port counters by going to the *WiFi & Switch Controller > FortiSwitch Ports* page, right-clicking a port, and selecting *Clear port counters*.



Support dynamic discovery in FortiLink mode over a layer-3 network

With this enhancement, dynamic discovery in FortiLink mode over a layer-3 network detects FortiSwitch split ports and newer FortiSwitch models. Split ports on all supported FortiSwitch models can be managed and displayed correctly on a FortiGate device.

In previous releases, dynamic discovery did not support FortiSwitch split ports or newer FortiSwitch models.

Configure flap guard through the switch controller

A flapping port is a port that changes status rapidly from up to down. A flapping port can create instability in protocols such as Spanning Tree Protocol (STP). If a port is flapping, STP must continually recalculate the role for each port. Flap guard also prevents unwanted access to the physical ports.

Flap guard detects how many times a port changes status during a specified number of seconds, and the system shuts down the port if necessary. You can manually reset the port and restore it to the active state.

Flap guard is configured and enabled on each port through the switch controller. The default setting is disabled.

The flap rate counts how many times a port changes status during a specified number of seconds. The range is 1 to 30 with a default setting of 5.

The flap duration is the number of seconds during which the flap rate is counted. The range is 5 to 300 seconds with a default setting of 30 seconds.

The flap timeout is the number of minutes before the flap guard is reset. The range is 0 to 120 minutes. The default setting of 0 means that there is no timeout.

- If a triggered port times out while the switch is in a down state, the port is initially in a triggered state until the switch has fully booted up and calculated that the timeout has occurred.
- The following models do not store time across reboot; therefore, any triggered port is initially in a triggered state until the switch has fully booted up—at which point the trigger is cleared:
  - FS-1xxE
  - FS-2xxD/E
  - FS-4xxD
  - FS-4xxE

To configure flap guard on a port through the switch controller:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set flapguard {enable | disable}
            set flap-rate <1-30>
            set flap-duration <5-300 seconds>
            set flap-timeout <0-120 minutes>
         next
      end
   end
```

For example:

```
config switch-controller managed-switch
   edit S424ENTF19000007
      config ports
         edit port10
            set flapguard enable
            set flap-rate 15
            set flap-duration 100
            set flap-timeout 30
      next
    end
  end
```

Resetting a port

After flap guard detects that a port is changing status rapidly and the system shuts down the port, you can reset the port and restore it to service.

To reset a port:

```
execute switch-controller flapguard reset <FortiSwitch_serial_number> <port_name>
```

For example:

```
execute switch-controller flapguard reset S424ENTF19000007 port10
```

Viewing the flap-guard configuration

To display flap-guard information for all ports of a FortiSwitch unit:

```
diagnose switch-controller switch-info flapguard status <FortiSwitch_serial_number>
```

For example:

```
diagnose switch-controller switch-info flapguard status S424ENTF19000007
```

Allow FortiSwitch console port login to be disabled

Administrators can now use the FortiSwitch profile to control whether users can log in with the managed FortiSwitchOS console port. By default, users can log in with the managed FortiSwitchOS console port.

To change the FortiSwitch profile:

```
config switch-controller switch-profile
  edit {default | <FortiSwitch_profile_name>}
    set login {enable | disable} enabled by default
  end
```

To disable logging in to the managed FortiSwitch consort port in the default FortiSwitch profile:

```
config switch-controller switch-profile
  edit default
    set login disable
  end
```

To change which FortiSwitch profile is used by a managed switch

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    set switch-profile {default | <FortiSwitch_profile_name>}
  end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      set switch-profile new_switch_profile
   end
```

Configure multiple flow-export collectors

You can now configure multiple flow-export collectors using the `config collectors` command. For each collector, you can specify the collector IP address, the collector port number, and the collector layer-4 transport protocol for exporting packets.

Using multiple flow-export collectors requires FortiSwitchOS 7.0.0 or later. If you are using an earlier version of FortiSwitchOS, only the first flow-export collector is supported.

You can also specify how often a template packet is sent using the new `set template-export-period` command. By default, a template packet is sent every 5 minutes. The range of values is 1-60 minutes.

To configure multiple flow-export collectors on managed FortiSwitch units:

```
config switch-controller flow-tracking
   set sample-mode {local | perimeter | device-ingress}
   set sample-rate <0-99999>
   set format {netflow1 | netflow5 | netflow9 | ipfix}
   set level {vlan | ip | port | proto}
   set max-export-pkt-size <512-9216 bytes; default is 512>
   set template-export-period <1-60 minutes, default is 5>
   set timeout-general <60-604800 seconds; default is 3600>
   set timeout-icmp <60-604800 seconds; default is 300>
   set timeout-max <60-604800 seconds; default is 604800>
   set timeout-tcp <60-604800 seconds; default is 3600>
   set timeout-tcp-fin <60-604800 seconds; default is 300>
   set timeout-tcp-rst <60-604800 seconds; default is 120>
   set timeout-udp <60-604800 seconds; default is 300>
   config collectors
      edit <collector_name>
      set ip <IPv4_address>
      set port <0-65535>
      set transport {udp | tcp | sctp}
      end
   config aggregates
      edit <aggregate_ID>
         set <IPv4_address>
      end
end
```

For example:

```
config switch-controller flow-tracking
   config collectors
      edit "Analyzer_1"
         set ip 172.16.201.55
         set port 4739
         set transport sctp
```

```
        next
        edit "Collector_HQ"
           set ip 172.16.116.82
           set port 2055
        next
    end
    set template-export-period 10
end
```

Enhanced FortiSwitch Ports page and Diagnostics and Tools pane

The *WiFi & Switch Controller* > *FortiSwitch Ports* page and *Diagnostics and Tools* pane have been improved, and a new *Port Statistics* pane is available.

In *Trunk* view, the *FortiSwitch Ports* page has been improved in the following ways:

- The *LLDP Profile*, *Loop Guard* , and *Security Policy* columns were removed.
- When you right-click a port, the menu now contains a *Mode* submenu.
- The *Enabled Features* column lists LACP when it has been enabled.

In *Port* view, the *FortiSwitch Ports* page has been improved in the following ways:

- New *VLAN* and *Transceiver Power (Transmitted/Received)* columns are now available.
- When you double-click a port, a new *Port Statistics* pane is displayed, which shows the transmitted and received traffic, frame errors by type, and transmitted and received frames. You can also select a port and then click the *View Statistics* button in the upper right corner. The *Compare with* dropdown list allows you to select another port to compare with the currently selected port. The statistics are refreshed every 15 seconds.

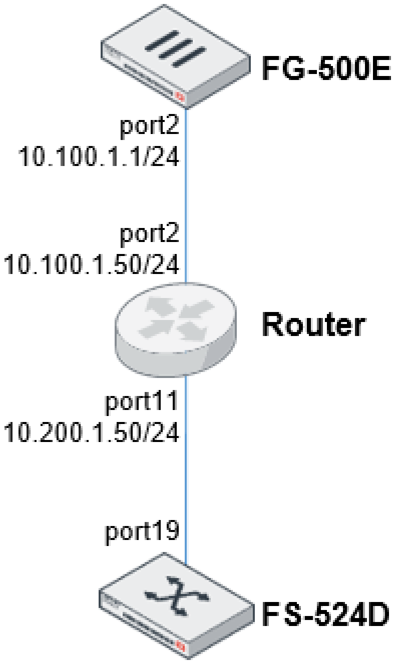
The *Diagnostics and Tools* pane (from *WiFi & Switch Controller* > *Managed FortiSwitches*) has been improved in the following ways:

- The fan status and power supply unit (PSU) status are now reported in the *General* pane.
- A new *Clients* tab lists the clients connected to each port of the selected FortiSwitch unit.

Manage FortiSwitch units on VXLAN interfaces

You can use Virtual Extensible LAN (VXLAN) interfaces to create a layer-2 overlay network when managing a FortiSwitch unit over a layer-3 network. After a VXLAN tunnel is set up between a FortiGate device and a FortiSwitch unit, the FortiGate device can use the VXLAN interface to manage the FortiSwitch unit. Only the management traffic uses the VXLAN tunnel; the FortiSwitch data traffic does not go through the VXLAN tunnel to the FortiGate device.

In the following configuration example, the FG-500E device is connected with a VXLAN tunnel to the FS-524D unit. After FortiLink is enabled on the VXLAN interface, the FortiGate device can managed the FortiSwitch unit.



To manage the FortiSwitch unit with the VXLAN interface:

1. Configure the FortiSwitch unit.
2. Configure the FortiGate device.

Configure the FortiSwitch unit

1. Configure a VLAN to use as the VXLAN interface.
```
config system interface
   edit "vlan-1000"
      set ip 10.200.1.2 255.255.255.0
      set vlanid 1000
      set interface "internal"
   next
end
```
2. Configure the VXLAN interface with the remote IP address of the FortiGate device.
```
config system vxlan
   edit "vx-4094"
      set vni 123456
      set vlanid 4094
      set interface "vlan-1000"
      set remote-ip "10.100.1.1"
   next
end
```
3. Configure a static route with the VXLAN remote IP address as the destination.
```
config router static
   edit 1
      set device "vlan-1000"
      set dst 10.100.1.1 255.255.255.255
      set gateway 10.200.1.50
   next
end
```

4. Set up the switch port that physically connects to the router and enable FortiLink mode over layer-3 network.

```
config switch interface
   edit port19
      set fortilink-l3-mode enable
   end
```

5. Configure the switch trunk to make it static and disable the automatic VLAN provisioning.

```
config switch trunk
   edit "__FoRtILnk0L3__"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port19"
   next
end
```

6. Configure the FortiLink interface to set the native VLAN to match the VLAN used for the VXLAN defined in step 1.

```
config switch interface
   edit "__FoRtILnk0L3__"
      set native-vlan 1000
      set allowed-vlans 1,1000,4088-4094
      set dhcp-snooping trusted
      ....
   next
end
```

7. Enable DHCP discovery.

```
config switch-controller global
   set ac-discovery-type dhcp
end
```

Configure the FortiGate device

1. Configure the system interface.

```
config system interface
   edit "port2"
      set vdom "root"
      set ip 10.100.1.1 255.255.255.0
      set allowaccess ping https http
      set type physical
      set snmp-index 4
   next
end
```

2. Configure the VXLAN interface.

```
config system vxlan
   edit "flk-vxlan"
      set interface "port2"
      set vni 123456
      set remote-ip "10.200.1.2"
   next
end
```

3. Configure the FortiLink interface as the VXLAN type and set the IP address.

```
config system interface
   edit "flk-vxlan"
```

```
        set vdom "root"
        set fortilink enable
        set ip 10.255.2.1 255.255.255.0
        set allowaccess ping fabric
        set type vxlan
        set lldp-reception enable
        set lldp-transmission enable
        set snmp-index 26
        set interface "port2"
    next
end
```

4. Configure a static route.

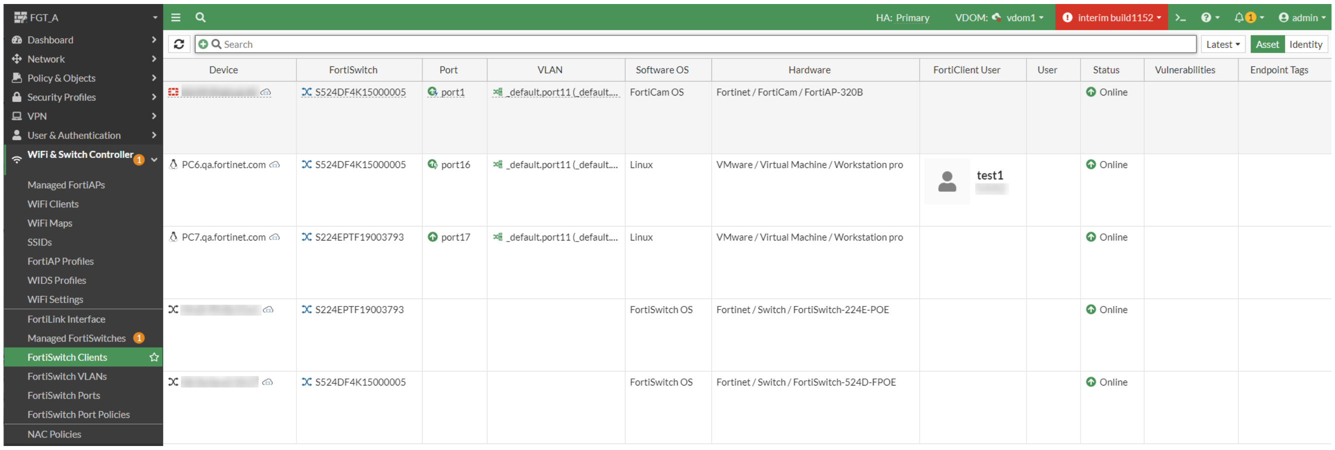
```
config router static
    edit 2
        set dst 10.200.1.0 255.255.255.0
        set gateway 10.100.1.50
        set distance 5
        set device "port2"
    next
end
```

5. Configure the DHCP server with option 138 to provide the switch-controller IP address to the FortiSwitch unit. DNS and NTP services are provided by the FortiGate device.

```
config system dhcp server
    edit 6
        set dns-service local
        set ntp-service local
        set default-gateway 10.255.2.1
        set netmask 255.255.255.0
        set interface "flk-vxlan"
        config ip-range
            edit 1
                set start-ip 10.255.2.2
                set end-ip 10.255.2.254
            next
        end
        config options
            edit 1
                set code 138
                set type ip
                set ip "10.255.2.1"
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch"
    next
end
```

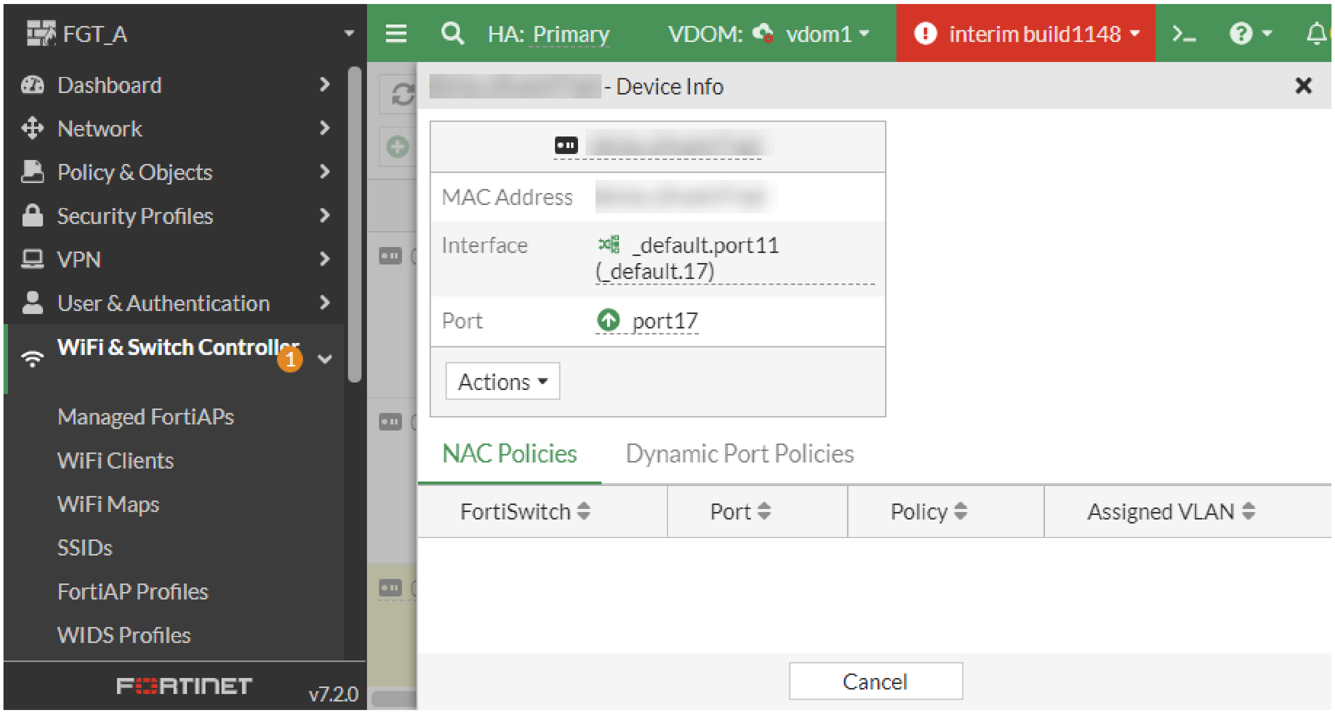
Add new FortiSwitch Clients page

The new *WiFi & Switch Controller* > *FortiSwitch Clients* page lists all devices connected to the FortiSwitch unit for a particular VDOM.



Device	FortiSwitch	Port	VLAN	Software OS	Hardware	FortiClient User	User	Status	Vulnerabilities	Endpoint Tags
[redacted]	S524DF4K15000005	port1	_default.port11 (_default....	FortiCam OS	Fortinet / FortiCam / FortiAP-320B			Online		
PC6.qa.fortinet.com	S524DF4K15000005	port16	_default.port11 (_default....	Linux	VMware / Virtual Machine / Workstation pro	test1 [redacted]		Online		
PC7.qa.fortinet.com	S224EPTF19003793	port17	_default.port11 (_default....	Linux	VMware / Virtual Machine / Workstation pro			Online		
[redacted]	S224EPTF19003793			FortiSwitch OS	Fortinet / Switch / FortiSwitch-224E-POE			Online		
[redacted]	S524DF4K15000005			FortiSwitch OS	Fortinet / Switch / FortiSwitch-524D-FPOE			Online		

Double-click a row to display the *Device Info* pane.



[redacted] - Device Info

[redacted]

MAC Address	[redacted]
Interface	_default.port11 (_default.17)
Port	port17

NAC Policies | Dynamic Port Policies

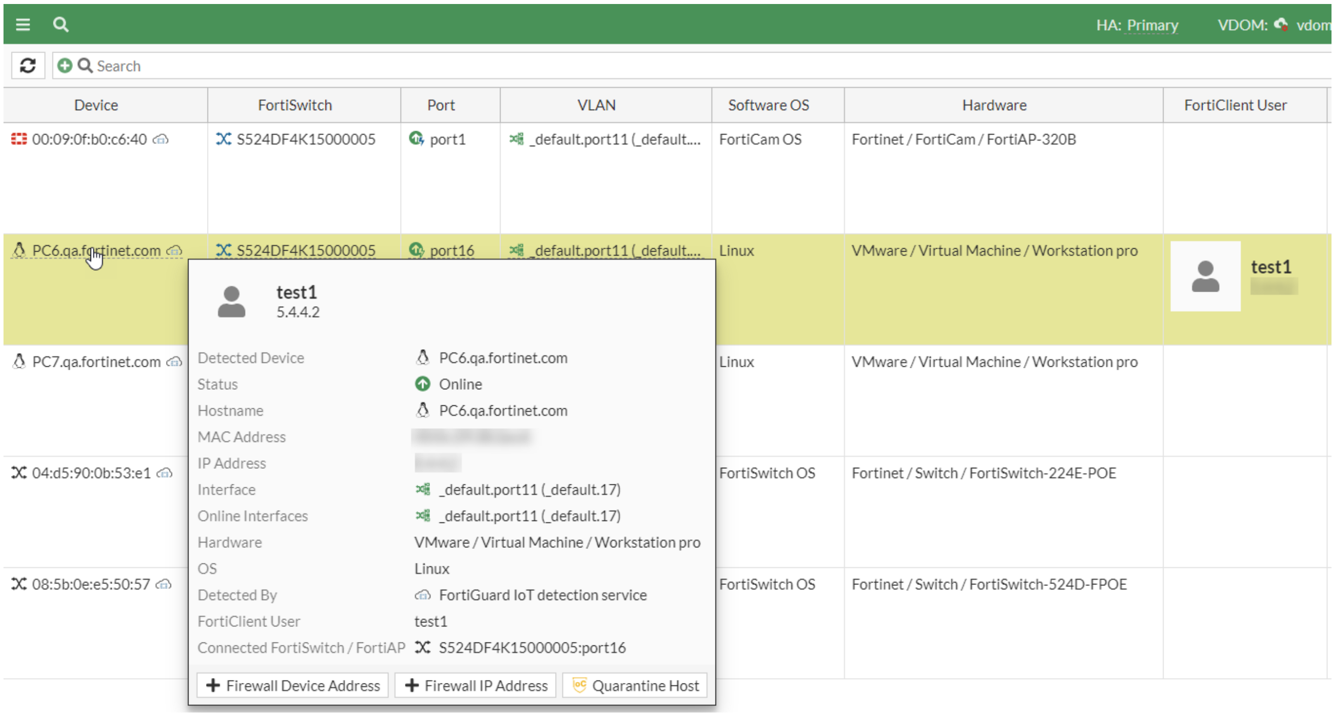
FortiSwitch	Port	Policy	Assigned VLAN

The *Device Info* pane displays the NAC policies and dynamic port policies that the device matches.

From the Actions dropdown menu, you can do the following:

- Create a firewall device address.
- Quarantine the host.

Hover over the device name in the *FortiSwitch Clients* page to get more details.



Device	FortiSwitch	Port	VLAN	Software OS	Hardware	FortiClient User
00:09:0f:b0:c6:40	S524DF4K15000005	port1	_default.port11 (_default....	FortiCam OS	Fortinet / FortiCam / FortiAP-320B	
PC6.qa.fortinet.com	S524DF4K15000005	port16	_default.port11 (_default....	Linux	VMware / Virtual Machine / Workstation pro	test1 [redacted]
PC7.qa.fortinet.com				Linux	VMware / Virtual Machine / Workstation pro	
04:d5:90:0b:53:e1				FortiSwitch OS	Fortinet / Switch / FortiSwitch-224E-POE	
08:5b:0e:e5:50:57				FortiSwitch OS	Fortinet / Switch / FortiSwitch-524D-FPOE	

test1
5.4.4.2

Detected Device	PC6.qa.fortinet.com
Status	Online
Hostname	PC6.qa.fortinet.com
MAC Address	[redacted]
IP Address	[redacted]
Interface	_default.port11 (_default.17)
Online Interfaces	_default.port11 (_default.17)
Hardware	VMware / Virtual Machine / Workstation pro
OS	Linux
Detected By	FortiGuard IoT detection service
FortiClient User	test1
Connected FortiSwitch / FortiAP	S524DF4K15000005:port16

From the detail window, you can do the following:

- Create a firewall device address.
- Create a firewall IP address.
- Quarantine the host.

To create the firewall device address:

1. Click *Firewall Device Address*.
2. In the *Name* field, enter a name for the firewall device address.
3. Click *Change* if you want a different color for the icon on the GUI.
4. If you want a different MAC address or range of MAC addresses, click + and then enter the MAC address or range of MAC addresses.
5. From the *Interface* dropdown list, select an interface.
6. In the *Comments* field, enter a description of the firewall device address.
7. Click *OK*.

To create the firewall IP address:

1. Click *Firewall IP Address*.
2. In the *Name* field, enter a name for the firewall IP address.
3. Click *Change* if you want a different color for the icon on the GUI.
4. In the *IP/Netmask* field, change the value as needed.
5. From the *Interface* dropdown list, select an interface.
6. Enable or disable *Static route configuration*.

7. In the *Comments* field, enter a description of the firewall device address.
8. Click *OK*.

To quarantine the host:

1. Click *Quarantine Host*.
2. In the *Description* field, enter the reason for quarantining the host.
3. Click *OK*.

Automatic revision backup upon FortiSwitch logout or firmware upgrade - 7.2.1

You can specify whether your managed FortiSwitch configuration is automatically backed up each time a user logs out or before a system upgrade is started. By default, both options are disabled.

To specify that the managed FortiSwitch unit creates a revision configuration file each time a user logs out:

```
config switch-controller switch-profile
   edit {default | FortiSwitch_profile_name}
      set revision-backup-on-logout enable
   next
end
```

To specify that the managed FortiSwitch unit creates a revision configuration file before a system upgrade is started:

```
config switch-controller switch-profile
   edit {default | FortiSwitch_profile_name}
      set revision-backup-on-upgrade enable
   next
end
```

Configure the frequency of IGMP queries - 7.2.1

You can now use the FortiOS CLI to specify how often the managed FortiSwitch unit will send IGMP version-2 queries when the IGMP-snooping querier is configured:

```
config switch-controller igmp-snooping
   set query-interval <10-1200 seconds>
end
```

By default, queries are sent every 125 seconds. The value for `aging-time` must be greater than the value for `query-interval`.

Add FortiView Internal Hubs monitor - 7.2.4

When you sample IP packets on managed FortiSwitch units with flow tracking, you can use the *FortiView Internal Hubs* monitor in FortiOS to report the IP addresses and the number of bytes collected from devices behind a FortiSwitch unit. If you drill down on one of the devices, you can see a chart displaying the devices and how they are connected.

To use the *FortiView Internal Hubs* monitor:

- The IP address for the flow collector (`collector-ip`) must be the same IP address as the FortiLink interface.
- The FortiGate model must have a hard drive, and you must enable historical FortiView and disk logging in the *Log & Report* > *Log Settings* page.
- FortiAnalyzer is not supported.

To enable flow tracking on a managed FortiSwitch unit:

```
config system interface
   edit <FortiLink_interface>
      set ip <IP_address_and_netmask>
      set switch-controller-netflow-collect enable
   next
end
config switch-controller flow-tracking
   set sample-mode {local | perimeter | device-ingress}
   set sample-rate <0-99999>
   set format {netflow1 | netflow5 | netflow9 | ipfix}
   set level {vlan | ip | port | proto}
   set max-export-pkt-size <512-9216 bytes; default is 512>
   set template-export-period <1-60 minutes, default is 5>
   set timeout-general <60-604800 seconds; default is 3600>
   set timeout-icmp <60-604800 seconds; default is 300>
   set timeout-max <60-604800 seconds; default is 604800>
   set timeout-tcp <60-604800 seconds; default is 3600>
   set timeout-tcp-fin <60-604800 seconds; default is 300>
   set timeout-tcp-rst <60-604800 seconds; default is 120>
   set timeout-udp <60-604800 seconds; default is 300>
   config collectors
      edit <flow_collector_name>
         set ip <flow_collector_IPv4_address>
         set port <0-65535>
         set transport {udp | tcp | sctp}
      end
   config aggregates
      edit <aggregate_ID>
         set <IPv4_address>
      end
end
```

For example, to configure port11 as the FortiLink interface, enable the collection of data in NetFlow format from the switch controller, enable flow tracking in the managed switch, and send NetFlow data to the FortiGate device:

```
config system interface
   edit "port11"
      set fortilink enable
      set ip 10.255.1.1 255.255.255.0
      set switch-controller-netflow-collect enable
   next
end
config switch-controller flow-tracking
   set sample-mode perimeter
   set sample-rate 10
   set format netflow9
   config collectors
      edit "1"
         set ip 10.255.1.1
         set port 0
         set transport udp
      next
   end
   set level ip
   set max-export-pkt-size 512
   set template-export-period 5
   set timeout-general 300
   set timeout-icmp 300
   set timeout-max 604800
   set timeout-tcp 300
   set timeout-tcp-fin 300
   set timeout-tcp-rst 120
   set timeout-udp 300
end
```

To check the status of the flow collector:

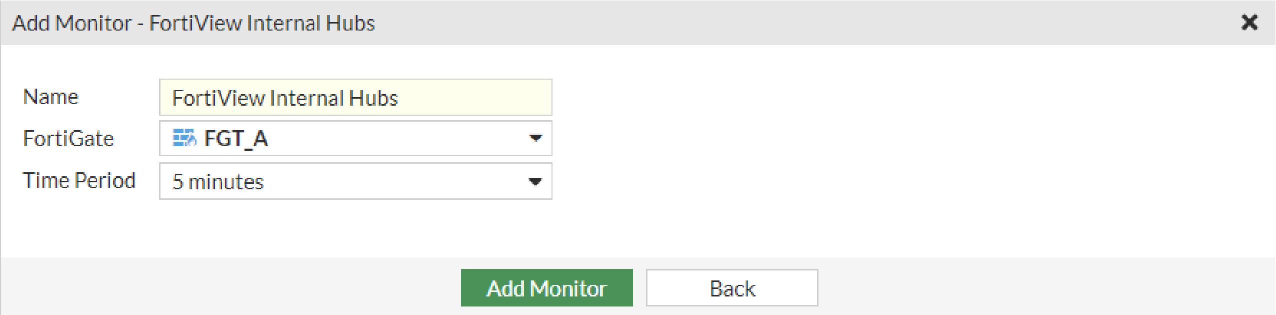
```
diagnose switch-controller flow-collector status
```

For example:

```
FGT_A (vdom1) # diagnose switch-controller flow-collector status
status : enabled
interface : port11
netflow packets : 1300
unknown packets : 0
flows : 42
flows filtered : 201
flowsets skipped : 17129
```

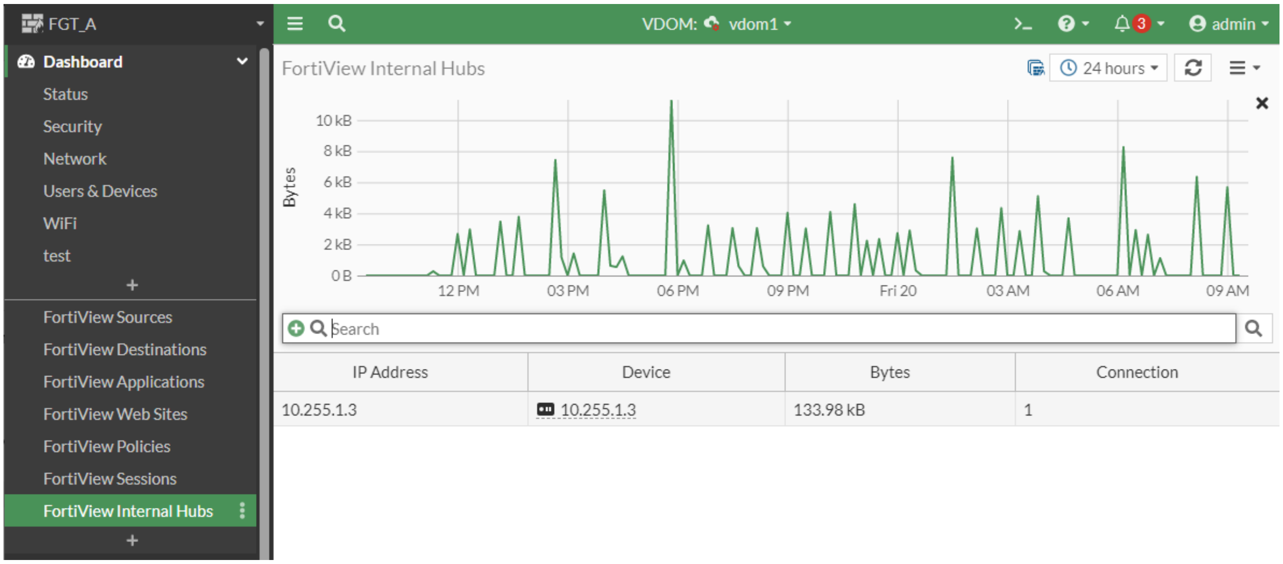
To add the *FortiView Internal Hubs* monitor:

1. Under *Dashboard* and click + to add a monitor.
2. In the *Add Monitor* pane, click the + by *FortiView Internal Hubs*.
3. From the *FortiGate* dropdown list, select which FortiGate device to monitor.
4. From the *Time Period* dropdown list, select how long to monitor (5 minutes, 1 hour, or 24 hours).



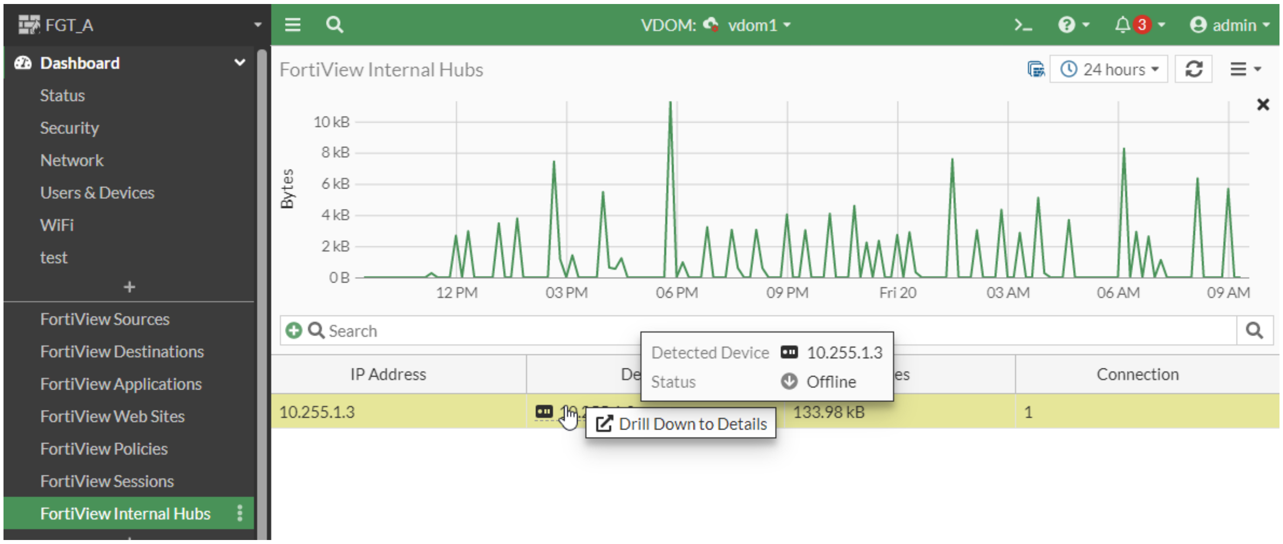
Name	FortiView Internal Hubs
FortiGate	FGT_A
Time Period	5 minutes

5. Click *Add Monitor*.
6. Under *Dashboard*, select *FortiView Internal Hubs* to display the *FortiView Internal Hubs* page.



IP Address	Device	Bytes	Connection
10.255.1.3	10.255.1.3	133.98 kB	1

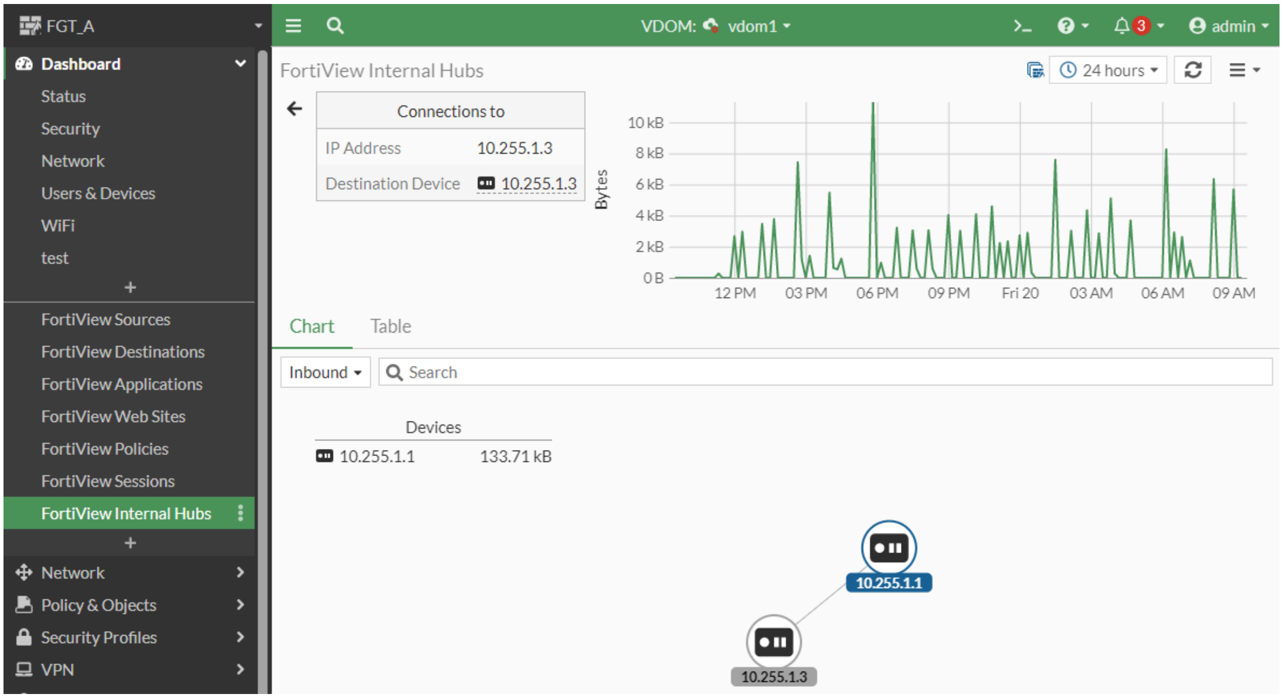
7. Right-click on one of the devices and select *Drill Down to Details*.



Detected Device	10.255.1.3
Status	Offline

IP Address	De	es	Connection
10.255.1.3	10.	133.98 kB	1

8. You can select the *Chart* or *Table* tab to change how the details are displayed.



Connections to	
IP Address	10.255.1.3
Destination Device	10.255.1.3

Devices	
10.255.1.1	133.71 kB

Configure DHCP-snooping static entries - 7.2.4

After you enable DHCP snooping for a VLAN, you can configure static entries by binding an IPv4 address with a MAC address for a specific switch interface:

- Specify a VLAN that has DHCP snooping enabled. The VLAN must be a native VLAN or allowed VLAN for the port.
- Specify a port that is not defined as trusted.
- Specify the MAC address in the form of xx:xx:xx:xx:xx:xx.
- Bind a single MAC address to a single IPv4 address. Multiple IP addresses cannot be bound to the same MAC address. The MAC address cannot be used in more than one static entry. Duplicate static entries are not supported on a VLAN.

DHCP-snooping static entries must be configured to be able to use dynamic ARP inspection (DAI) for IP/MAC entries not discovered by DHCP snooping.

Specifying the VLAN, IP address, MAC address, and interface name is required.

You can specify a maximum of 64 DHCP static entries for the entire FortiSwitch unit.

- You cannot use a DHCP trusted switch interface or an 802.1X interface for the static entry's switch interface.
- After you configure a DHCP-snooping static entry for a VLAN, you cannot remove that VLAN from the switch interface.
- After you configure a DHCP-snooping static entry for a switch interface, the switch interface cannot be included as a member of a trunk until the DHCP-snooping static entry is deleted.
- If you configure a DHCP-snooping static entry for a trunk, the trunk cannot be deleted until the DHCP-snooping static entry is deleted.

To create a static entry for DHCP snooping and DAI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config dhcp-snooping-static-client
         edit <DHCP_static_client_name>
            set vlan <VLAN_ID>
            set ip <DHCP_static_client_static_IP_address>
            set mac <DHCP_static_client_MAC_address>
            set port <interface_name>
         next
      next
   end
```

For example:

```
config switch-controller managed-switch
   edit S524DN4K16000116
      config dhcp-snooping-static-client
         edit DHCPclient
            set vlan 100
            set ip 192.168.101.1
            set mac 00:21:cc:d2:76:72
            set port port19
         next
      next
   end
```

Track device traffic statistics when NAC is enabled - 7.2.4

Starting in FortiOS 7.2.4 with FortiSwitchOS 7.2.3, you can use the FortiOS CLI to report device statistics when NAC is enabled. The device statistics report the MAC addresses of known devices, the number of packets and bytes received, the number of seconds since the last update, and the age of the MAC counter in seconds.

- Only statistics for receive counters are reported.
- If a device moves to a different FortiSwitch unit, the MAC counters are reallocated.
- If a FortiSwitch unit cannot track both bytes and packets, a zero is displayed for whichever value cannot be tracked. If a FortiSwitch unit cannot track device statistics at all, the entry will be missing from the CLI command output.
- This feature is supported on the following FortiSwitch models: FSR-124D, FSR-224F-FPOE, FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-M426E-FPOE, FS-424E-Fiber, FS-448E, FS-448E-POE, FS-448E-FPOE, FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE, FS-1024D, FS-1024E, FS-T1024E, FS-1048E, and FS-3032E.
- Accuracy is not guaranteed.

To display device statistics:

1. Enable NAC.
```
config user nac-policy
  edit <NAC_policy_name>
    set status enable
  next
end
```
2. Enable packet counting in the MAC policy. By default, packet counting is disabled.
```
config switch-controller mac-policy
  edit <MAC_policy_name>
    set count enable
  next
end
```
3. Specify how long inactive MAC addresses are kept before being removed from the client database. By default, MAC addresses are kept for 24 hours. The range of values is 0-168 hours. If you set this option to 0, the value for the `mac-aging-interval` setting is used instead.
```
config switch-controller global
  set mac-retention-period <number_of_hours>
end
```
4. Enter the following command to display the device statistics:
```
diagnose switch-controller telemetry show mac-stats
```

For example:

```
diagnose switch-controller telemetry show mac-stats

MAC                Packets        Bytes      Last Update (secs ago)  Age
------------------------------------------------------------------------------------
00:00:00:00:00:0f     234562    2356546842           41             23433
00:00:00:00:14:21      44273        456346           68              7477
00:03:7a:a8:82:e7      12346         34545           30            983452
00:04:f2:f3:2b:7f       4357        345345           30             23423
00:04:f2:f6:77:05     463453       4564564          430         362456265
00:04:f2:f6:7a:6a      34535       1312354           30             23423
00:04:f2:f6:7b:66      73821        345345           68            374546
00:05:9a:3c:7a:00         43          9144           68            456725
```

Enhance switch PoE port settings - 7.2.4

Starting in FortiOS 7.2.4 with FortiSwitchOS 7.2.3, you can configure the following PoE port settings on managed switches:

- Port mode—You can set the port mode to IEEE802.3 AF or IEEE802.3 AT.
- Port priority—You can set the port priority to critical, high, medium, or low. If there is not enough power, power is allotted first to critical-priority ports, then to high-priority ports, then to medium-priority ports, and then to low-priority ports. Medium priority is available only on the following models: FS-224D-FPOE, FS-224E-POE, FS-248E-POE, FS-248E-FPOE, FS-424E-POE, FS-424E-FPOE, FS-M426E-FPOE, FS-448E-POE, FS-448E-FPOE, FS-524D-FPOE, and FS-548D-FPOE.
- Port power—You can set the port to use normal, power, perpetual power, or perpetual-fast power. Refer to the FortiSwitchOS feature matrix to see which FortiSwitch models support this feature.

Port power setting	Description
normal	PoE power is not provided while a switch restarts.
perpetual	PoE power is provided during a soft reboot (switch is restarted while powered up).
perpetual-fast	PoE power is provided during a hard reboot (the switch's power is physically turned off and then on again).

To configure the PoE port settings:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set poe-port-mode {IEEE802_3AF | IEEE802_3AT}
            set poe-port-priority {critical-priority | high-priority | low-priority | medium-
                  priority}
            set poe-port-power {normal | perpetual | perpetual-fast}
         next
      end
   next
end
```

Increase the number of NAC devices supported - 7.2.4

NAC now supports more connected devices—up to 48 times the maximum number of managed FortiSwitch units supported on the FortiGate device. You can use the `diagnose switch-controller mac-device nac known` command to check the number of known devices. When 95 percent of the maximum number of devices is reached, a warning icon is displayed in the *Matched NAC Devices* widget in the FortiOS GUI. When the maximum number is reached, a switch-controller event is logged.

The range and default values for the `set nac-periodic-interval` command (under `config switch-controller system`) have changed. The default value is now 60, and the range of values is now 5-180.

The range and default values for the `set dynamic-periodic-interval` command (under `config switch-controller system`) have changed. The default value is now 60, and the range of values is now 5-180.

NAC

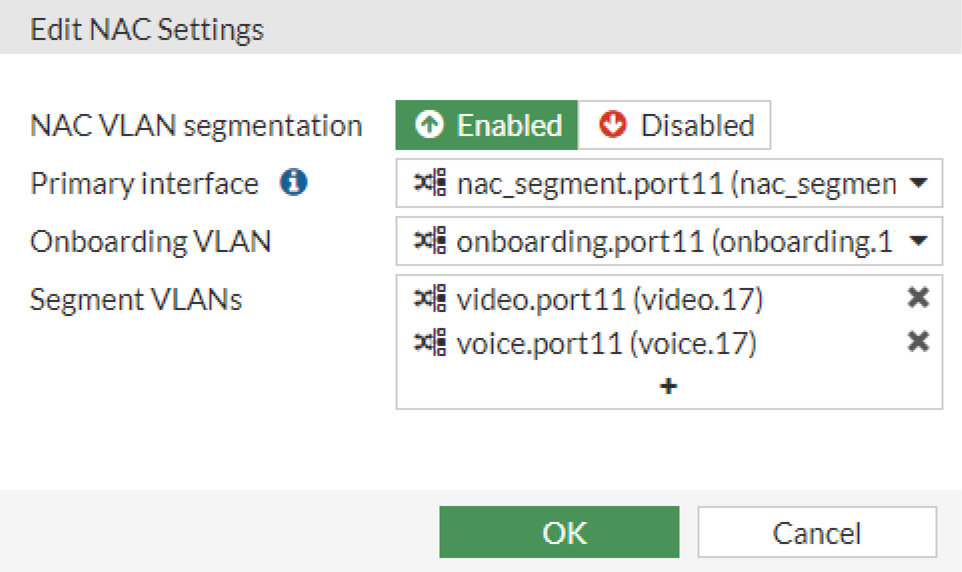
This section includes information about NAC-related new features:

- Allow the configuration of NAC LAN segments in the GUI on page 558

Allow the configuration of NAC LAN segments in the GUI

You can configure NAC LAN segments in three places in the GUI:

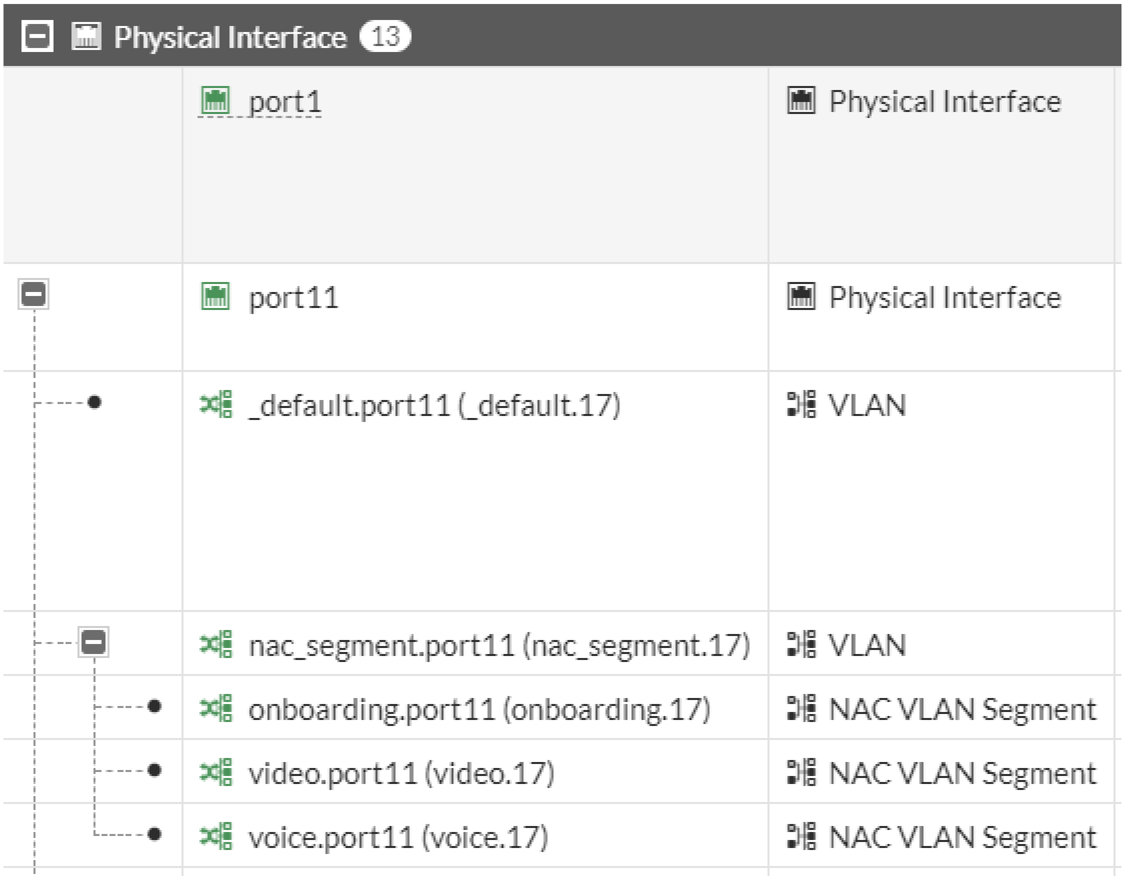
- When you select a NAC VLAN in the *WiFi & Switch Controller > NAC Policies* page and click *Edit*, the *Edit NAC Settings* page allows you to enable or disable NAC VLAN segmentation and select the primary interface, onboarding VLAN, and segment VLANs.



Edit NAC Settings

NAC VLAN segmentation	Enabled / Disabled
Primary interface	nac_segment.port11 (nac_segmen
Onboarding VLAN	onboarding.port11 (onboarding.1
Segment VLANs	video.port11 (video.17) voice.port11 (voice.17)

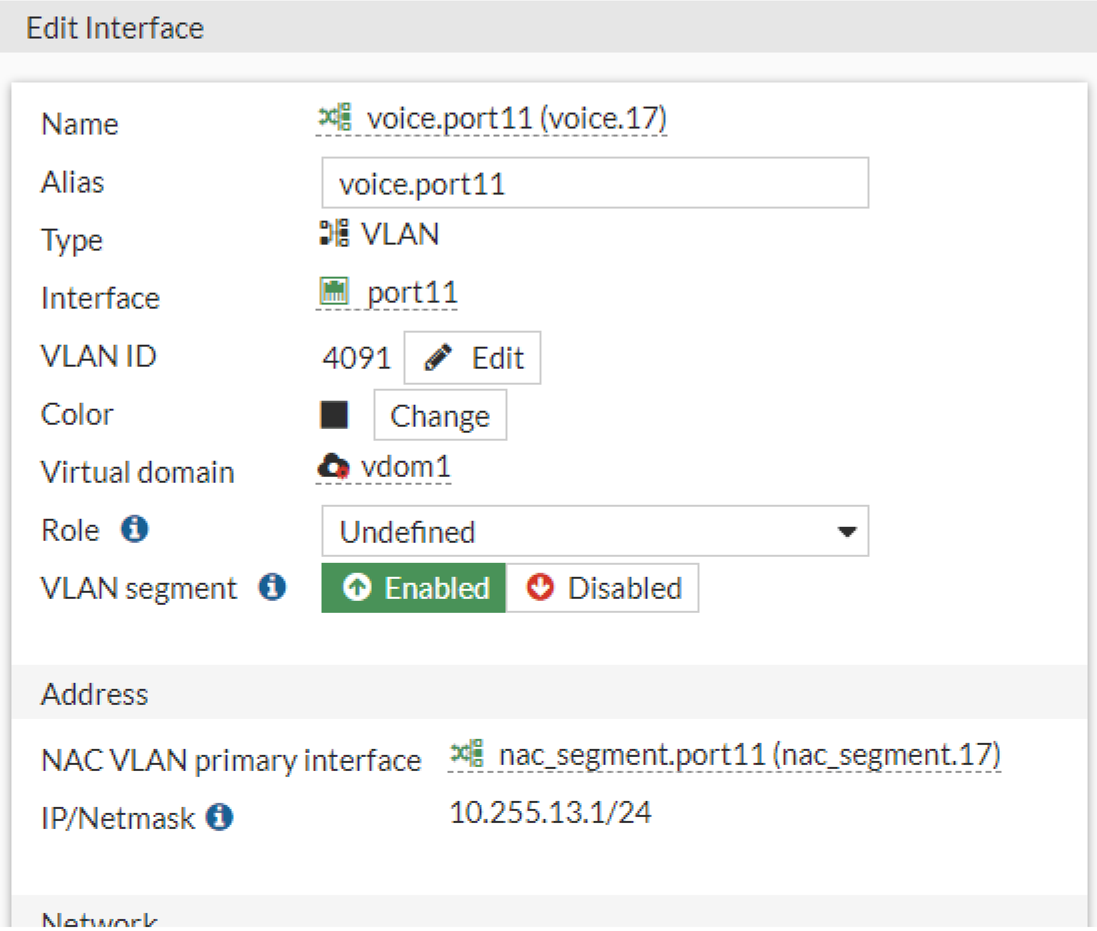
- The *Network > Interfaces* page shows each LAN segment VLAN as a child of the parent NAC segment.



Physical Interface 13

	port1	Physical Interface
⊟	port11	Physical Interface
	_default.port11 (_default.17)	VLAN
⊟	nac_segment.port11 (nac_segment.17)	VLAN
	onboarding.port11 (onboarding.17)	NAC VLAN Segment
	video.port11 (video.17)	NAC VLAN Segment
	voice.port11 (voice.17)	NAC VLAN Segment

- The *VLAN segment* buttons allow you to enable or disable VLAN segments in the *New Interface* and *Edit Interface* pages.



Edit Interface

Name: voice.port11 (voice.17)

Alias: voice.port11

Type: VLAN

Interface: port11

VLAN ID: 4091

Color: ■

Virtual domain: vdom1

Role: Undefined

VLAN segment: [✓ Enabled] Disabled

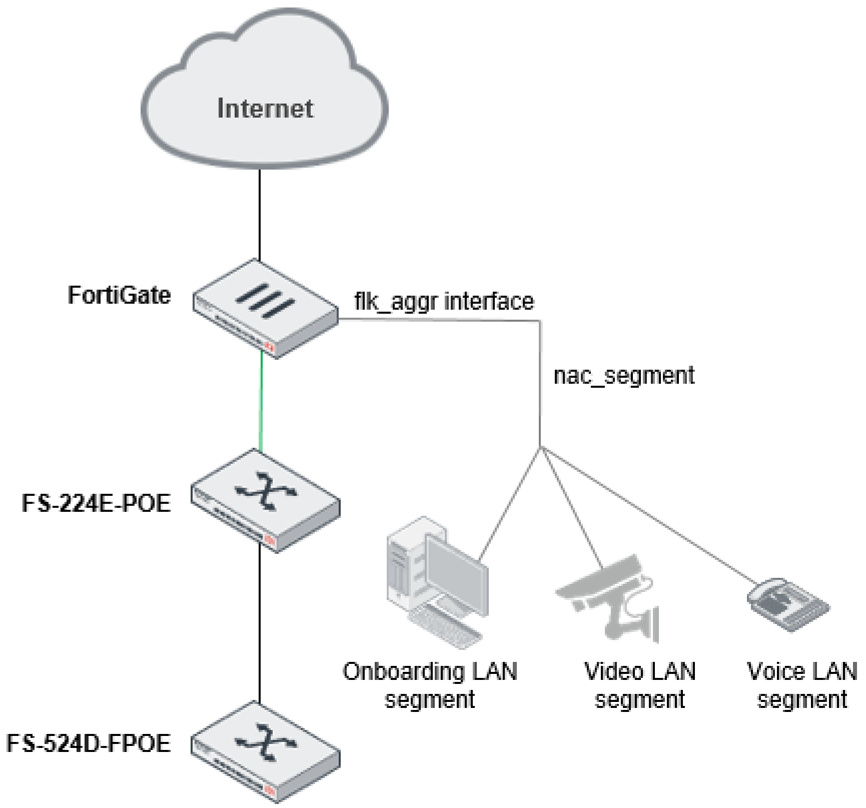
Address

NAC VLAN primary interface: nac_segment.port11 (nac_segment.17)

IP/Netmask: 10.255.13.1/24

Network

Configuration example



In the configuration example, a FortiLink aggregate interface flk_aggr is created on the FortiGate device and connected to the two downstream FortiSwitch units. A nac_segment VLAN is created on the FortiLink aggregate interface flk_aggr. The DHCP server is created on this interface to assign addresses from 10.255.13.2-10.255.13.254. Under nac_segment, there are three LAN segments, onboarding, video, and voice.

When a device connects to a FortiSwitch port that is configured with a NAC policy, the device is assigned first to the onboarding VLAN, and nac_segment issues an IP address to the device. After the NAC policy is processed and a match occurs, the device is moved to either the video or the voice VLAN.

The IP address is not changed in this process. All sessions continue to flow according to the firewall policies for that VLAN.

FortiExtender

This section includes information about FortiExtender related new features:

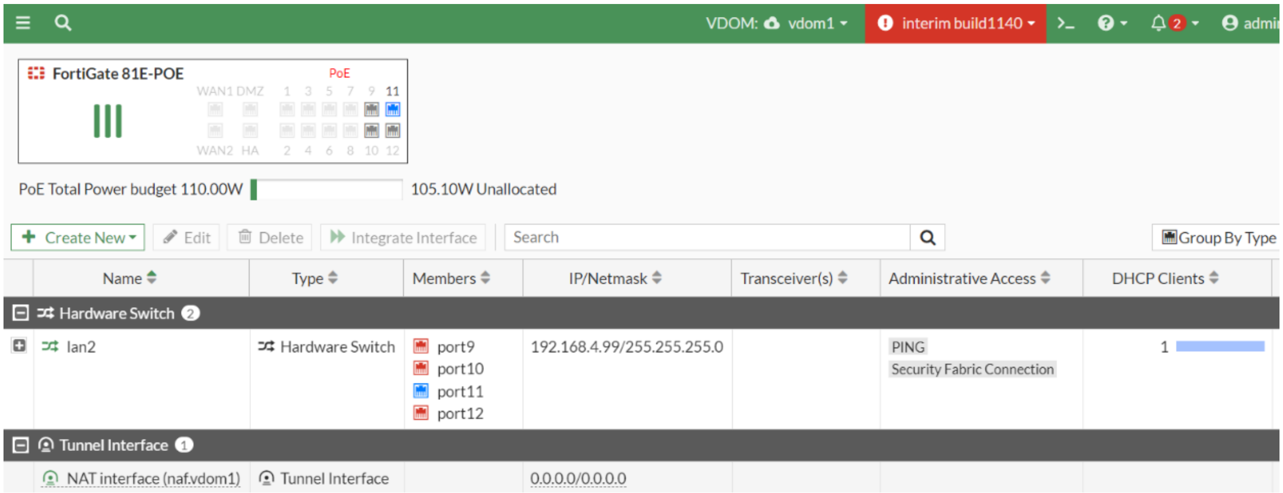
- Allow FortiExtender to be managed and used in a non-root VDOM on page 562
- FortiExtender monitoring enhancement 7.2.1 on page 566
- Provision FortiExtender firmware upon authorization 7.2.1 on page 571
- De-authorize FortiExtender devices 7.2.4 on page 572

Allow FortiExtender to be managed and used in a non-root VDOM

This feature allows FortiExtender to be managed and used in a non-root VDOM.

GUI operating procedures

1. The FortiExtender appears in the Network section in each VDOM.

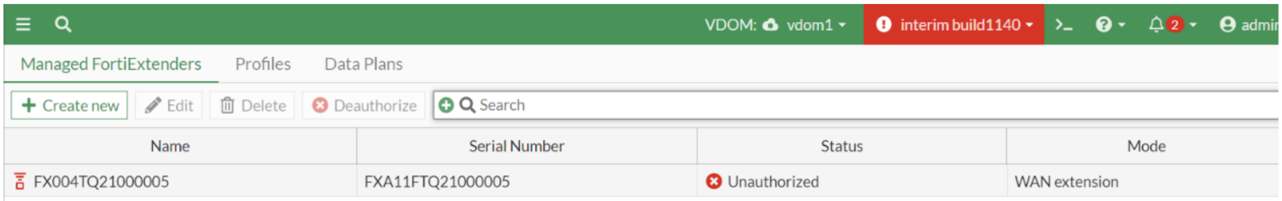


PoE Total Power budget 110.00W 105.10W Unallocated

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients
Hardware Switch 2						
lan2	Hardware Switch	port9 port10 port11 port12	192.168.4.99/255.255.255.0		PING Security Fabric Connection	1
Tunnel Interface 1						
NAT interface (naf.vdom1)	Tunnel Interface		0.0.0.0/0.0.0.0			

2. The FortiExtender can be discovered in the VDOM.

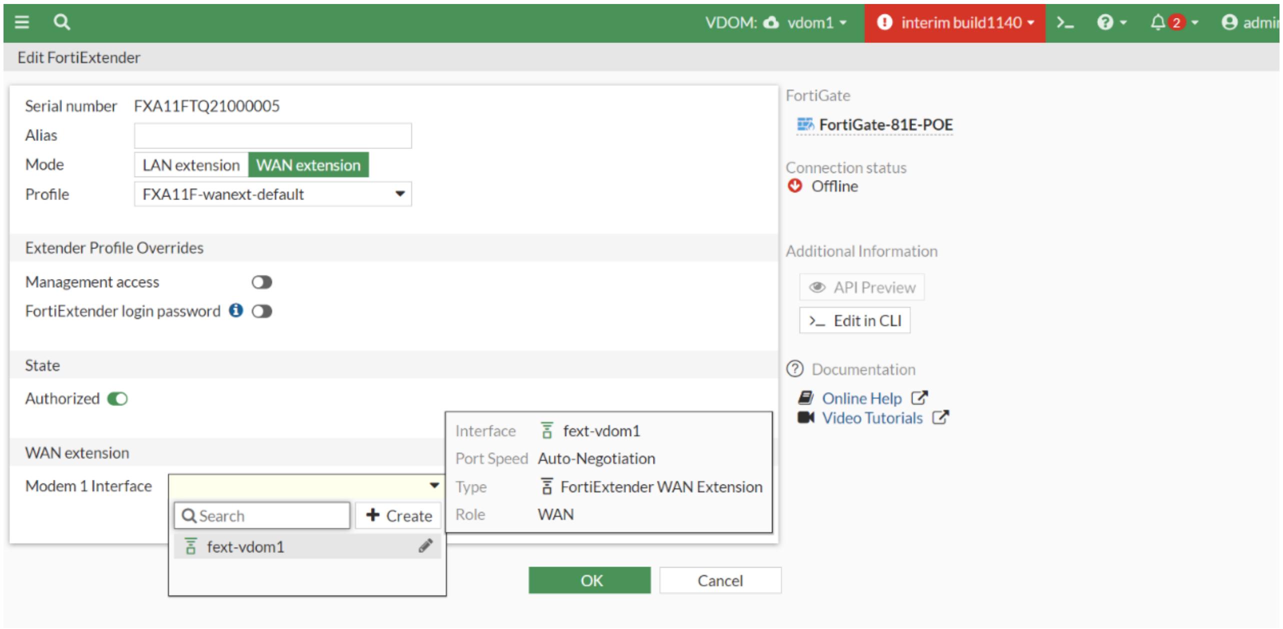
The VDOM must get an interface (lan2) with Security Fabric Connection and a DHCP server. Then the FortiExtender can be discovered when connecting to lan2 port11.



Name	Serial Number	Status	Mode
FX004TQ21000005	FXA11FTQ21000005	Unauthorized	WAN extension

3. After it is authorized, the FortiExtender can provide an interface to the VDOM.

The FortiExtender can be authorized to bond a FortiExtender type interface to the LTE modem.



Edit FortiExtender

Serial number	FXA11FTQ21000005
Alias	
Mode	LAN extension / WAN extension
Profile	FXA11F-wanext-default

Extender Profile Overrides

Management access ○

FortiExtender login password ℹ ○

State

Authorized ●

WAN extension

Modem 1 Interface

Search | + Create

fext-vdom1

Interface	fext-vdom1
Port Speed	Auto-Negotiation
Type	FortiExtender WAN Extension
Role	WAN

OK | Cancel

FortiGate

FortiGate-81E-POE

Connection status

Offline

Additional Information

API Preview

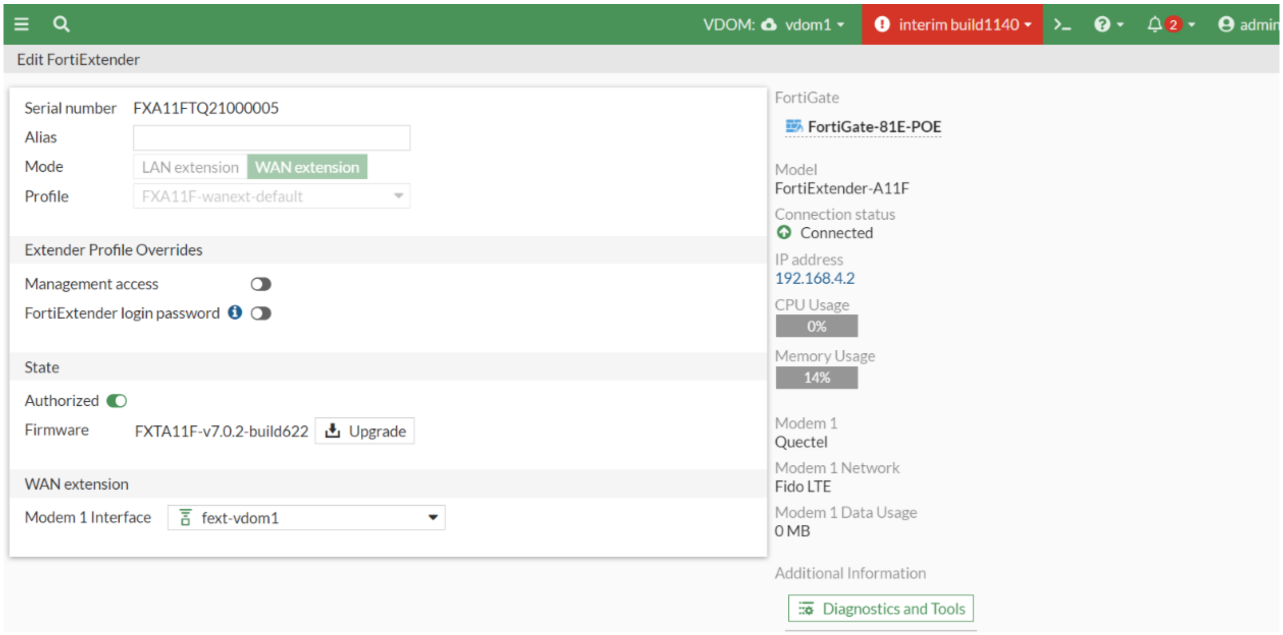
Edit in CLI

Documentation

Online Help

Video Tutorials

The FortiExtender is connected to the FortiGate after authorization.



Edit FortiExtender

Serial number	FXA11FTQ21000005
Alias	
Mode	LAN extension / WAN extension
Profile	FXA11F-wanext-default

Extender Profile Overrides

Management access ○

FortiExtender login password ℹ ○

State

Authorized ●

Firmware FXTA11F-v7.0.2-build622 Upgrade

WAN extension

Modem 1 Interface fext-vdom1

FortiGate

FortiGate-81E-POE

Model

FortiExtender-A11F

Connection status

Connected

IP address

192.168.4.2

CPU Usage

0%

Memory Usage

14%

Modem 1

Quectel

Modem 1 Network

Fido LTE

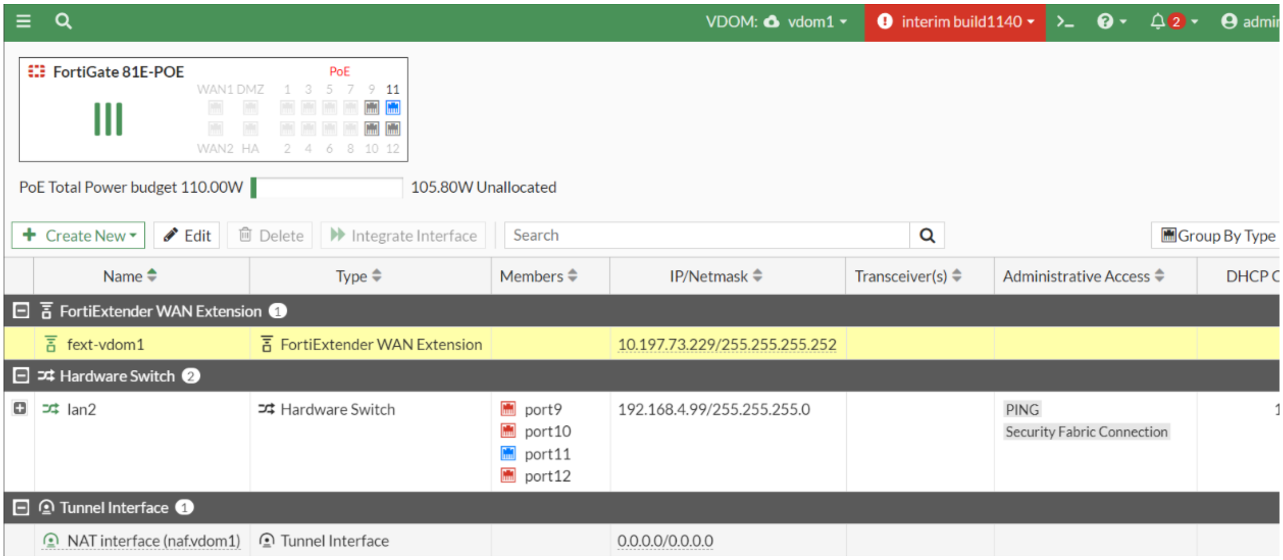
Modem 1 Data Usage

0 MB

Additional Information

Diagnostics and Tools

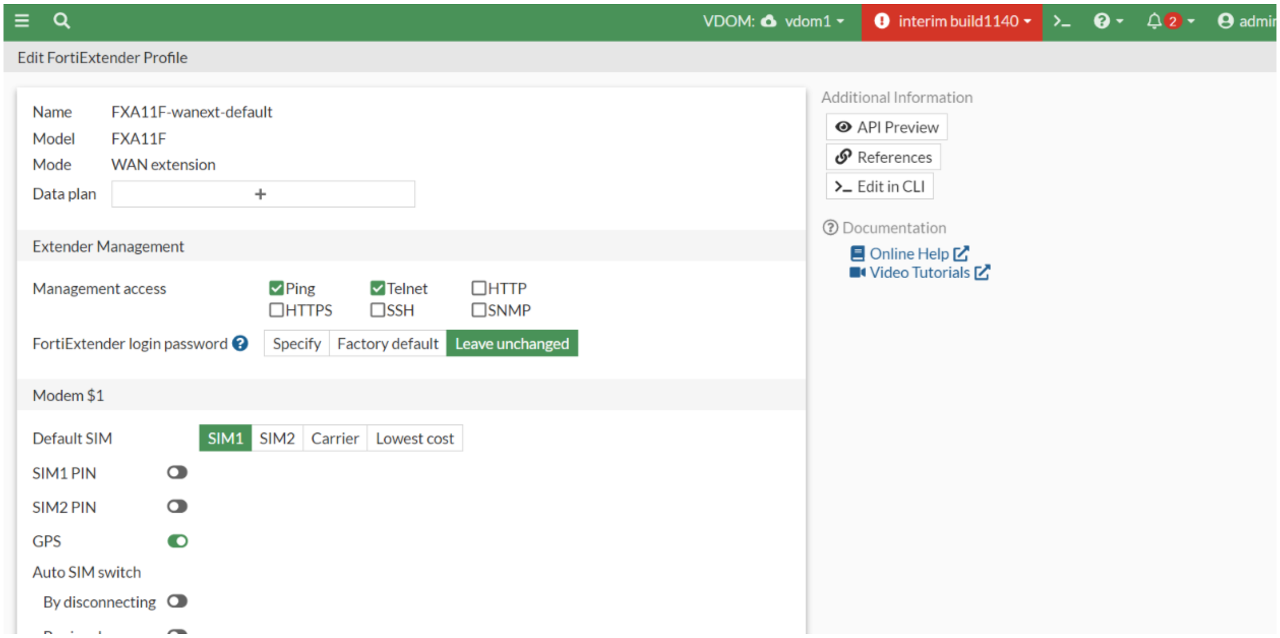
The FortiGate gets the IP and gateway for the FortiExtender type interface in the VDOM.



PoE Total Power budget 110.00W 105.80W Unallocated

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP C
FortiExtender WAN Extension 1						
fext-vdom1	FortiExtender WAN Extension		10.197.73.229/255.255.255.252			
Hardware Switch 2						
lan2	Hardware Switch	port9 port10 port11 port12	192.168.4.99/255.255.255.0		PING Security Fabric Connection	1
Tunnel Interface 1						
NAT interface (naf.vdom1)	Tunnel Interface		0.0.0.0/0.0.0.0			

4. A FortiExtender profile and data plan can be set up per VDOM.



Edit FortiExtender Profile

Name	FXA11F-wanext-default
Model	FXA11F
Mode	WAN extension
Data plan	+

Extender Management

Management access ☑ Ping ☑ Telnet ☐ HTTP ☐ HTTPS ☐ SSH ☐ SNMP

FortiExtender login password: Specify | Factory default | [✓ Leave unchanged]

Modem $1

Default SIM: [✓ SIM1] | SIM2 | Carrier | Lowest cost

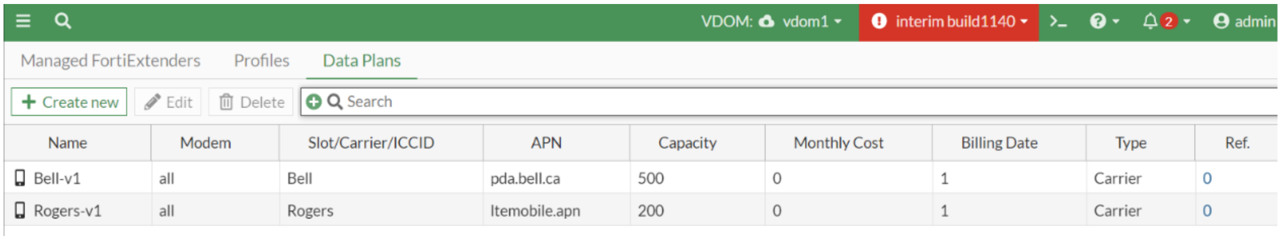
SIM1 PIN ○ (off)

SIM2 PIN ○ (off)

GPS ● (on)

Auto SIM switch

By disconnecting ○ (off)



Name	Modem	Slot/Carrier/ICCID	APN	Capacity	Monthly Cost	Billing Date	Type	Ref.
Bell-v1	all	Bell	pda.bell.ca	500	0	1	Carrier	0
Rogers-v1	all	Rogers	ltemobile.apn	200	0	1	Carrier	0

CLI operating procedures

1. Set up the interface to discover FortiExtender in the VDOM.

```
config system interface
    edit "lan2"
        set vdom "vdom1"
        set ip 192.168.4.99 255.255.255.0
        set allowaccess ping fabric
        set type hard-switch
        set snmp-index 32
    next
end
```

2. Create a FortiExtender type interface in the VDOM.

```
config system interface
    edit "fext-vdom1"
        set vdom "vdom1"
        set mode dhcp
        set type fext-wan
        set role wan
        set snmp-index 34
    next
end
```

3. Authorize the discovered FortiExtender and bond the FortiExtender type interface.

```
config extender-controller extender
    edit "FX004TQ21000005"
        set id "FXA11FTQ21000005"
        set authorized enable
        set device-id 1
        set extension-type wan-extension
        set profile "FXA11F-wanext-default"
        config wan-extension
            set modem1-extension "fext-vdom1"
        end
    next
end
```

4. Check the IP and gateway from the FortiExtender interface.

```
FortiGate-81E-POE (vdom1) # get system interface | grep fext-vdom1
== [ fext-vdom1 ]
name: fext-vdom1   mode: dhcp    ip: 10.197.73.229 255.255.255.252   status: up
 netbios-forward: disable    type: fext-wan    netflow-sampler: disable    sflow-sampler:
disable    src-check: enable    explicit-web-proxy: disable    explicit-ftp-proxy:
disable    proxy-captive-portal: disable    mtu-override: disable    drop-overlapped-
fragment: disable    drop-fragment: disable

FortiGate-81E-POE (vdom1) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
```

```
           * - candidate default

    Routing table for VRF=0
    S*      0.0.0.0/0 [5/0] via 10.197.73.230, fext-vdom1, [1/0]
    C       10.197.73.228/30 is directly connected, fext-vdom1
    C       192.168.4.0/24 is directly connected, lan2
```

5. Modify the FortiExtender profile.

```
config extender-controller extender-profile
    edit "FXA11F-wanext-default"
        set id 4
        set model FXA11F
        set allowaccess ping telnet
        config cellular
            config sms-notification
            end
            config modem1
            end
        end
    next
end
```

6. Create the FortiExtender data plan.

```
config extender-controller dataplan
    edit "Rogers-v1"
        set type carrier
        set carrier "Rogers"
        set apn "ltemobile.apn"
        set capacity 200
    next
end
```

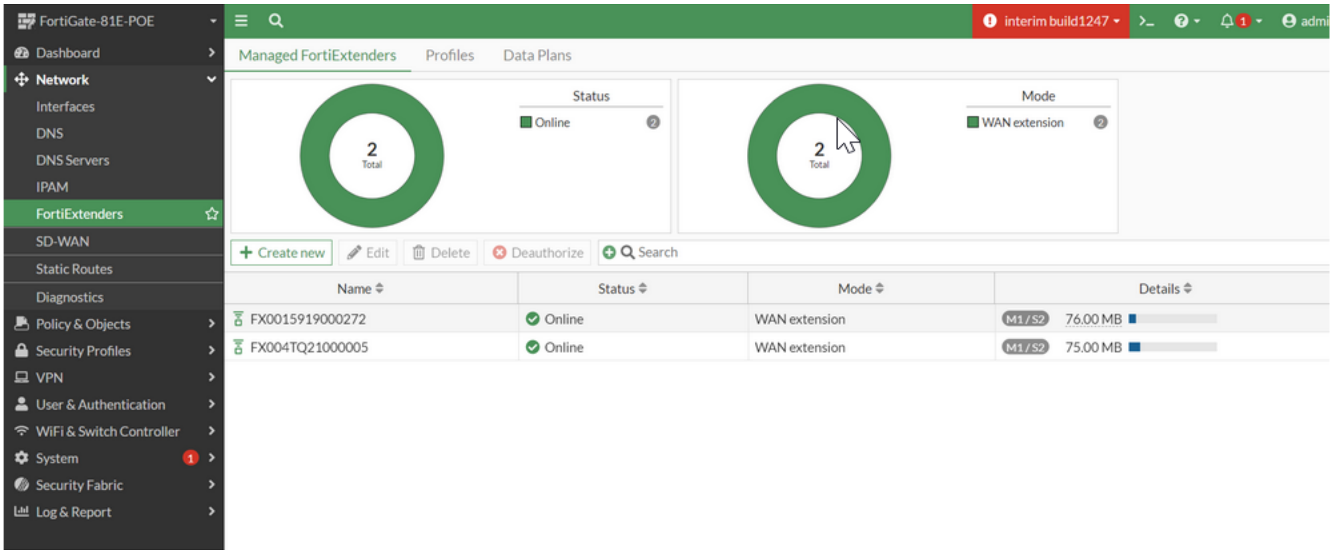
FortiExtender monitoring enhancement - 7.2.1

The Managed FortiExtenders tab on the Network > FortiExtenders page has been enhanced with the following additional monitoring features:

- Profile tab on the Network > FortiExtenders page has two new charts: Status and Mode.
- Updated Status column with Online, Offline, Waiting For Authorization states.
- A new default Details column filled with the data used by the modem/SIM card when FortiExtender is in WAN-extension mode, or filled with the connected IPsec tunnel used with the FortiGate when FortiExtender is in LAN-extension mode.
- When FortiExtender is in WAN-extension mode, you can view modem information by left-clicking or hovering the mouse over the FortiExtender name to show a tooltip, and then clicking "Diagnostics and Tools".
- The "Serial #" column which used to be a default column is now optional.

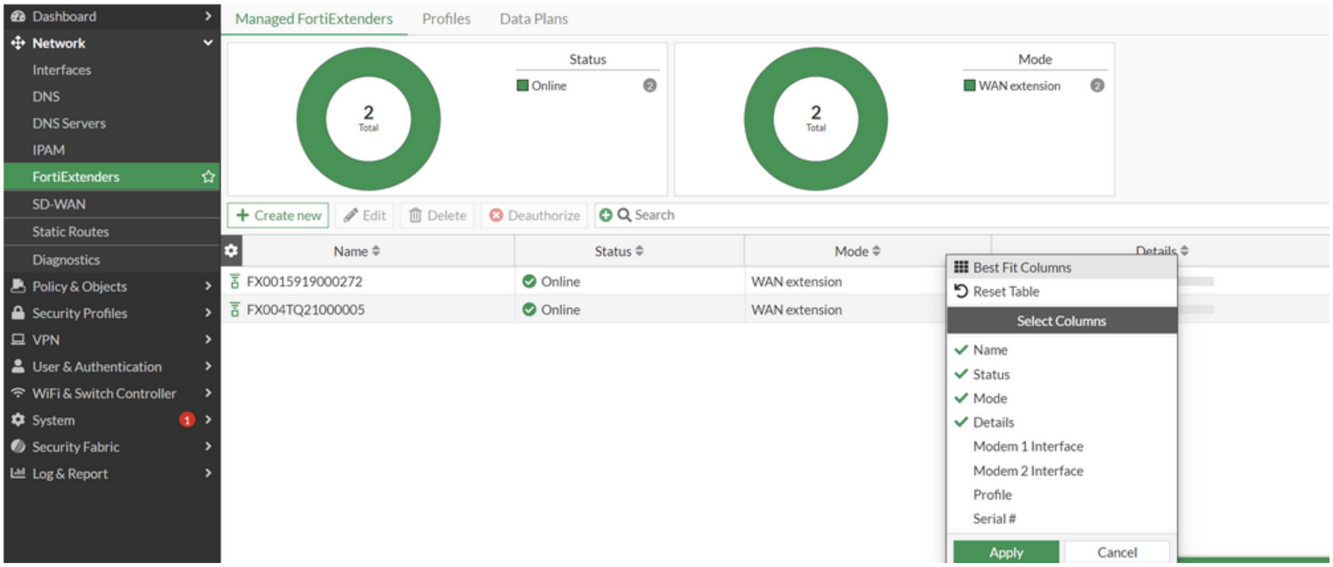
FortiExtender default page and option selection

By default, the page shows the name of each FortiExtender, but Serial number is not in default display.



Name	Status	Mode	Details
FX0015919000272	✓ Online	WAN extension	M1 / S2 76.00 MB
FX004TQ21000005	✓ Online	WAN extension	M1 / S2 75.00 MB

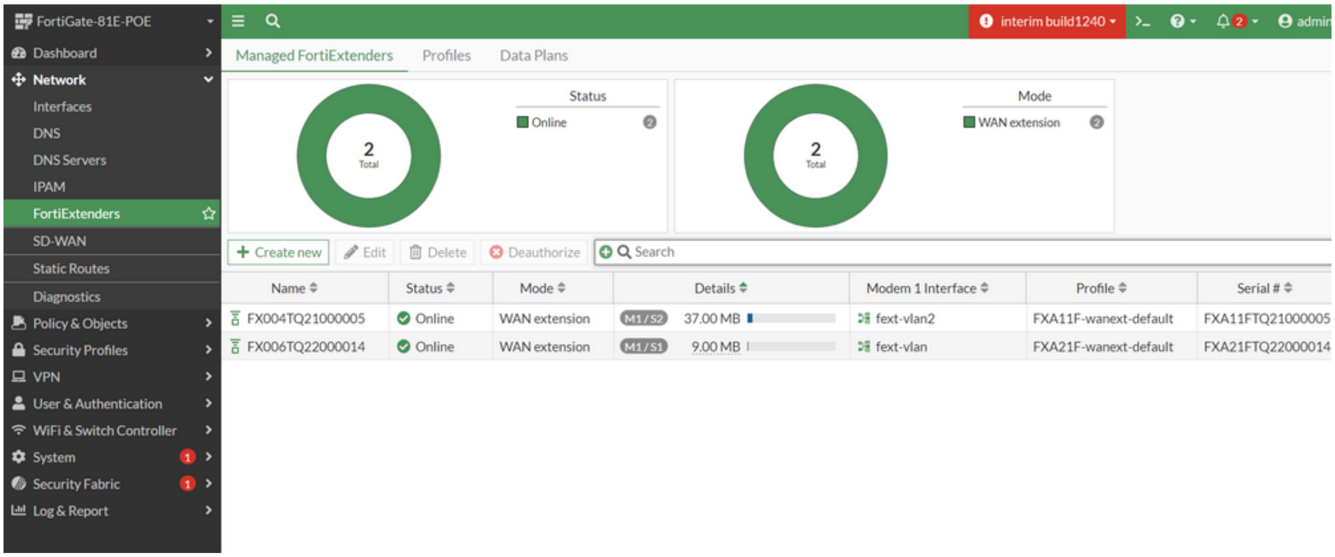
You can click in the default column to view more options and add more columns, such as "Serial #".



Name	Status	Mode	Details
FX0015919000272	✓ Online	WAN extension	
FX004TQ21000005	✓ Online	WAN extension	

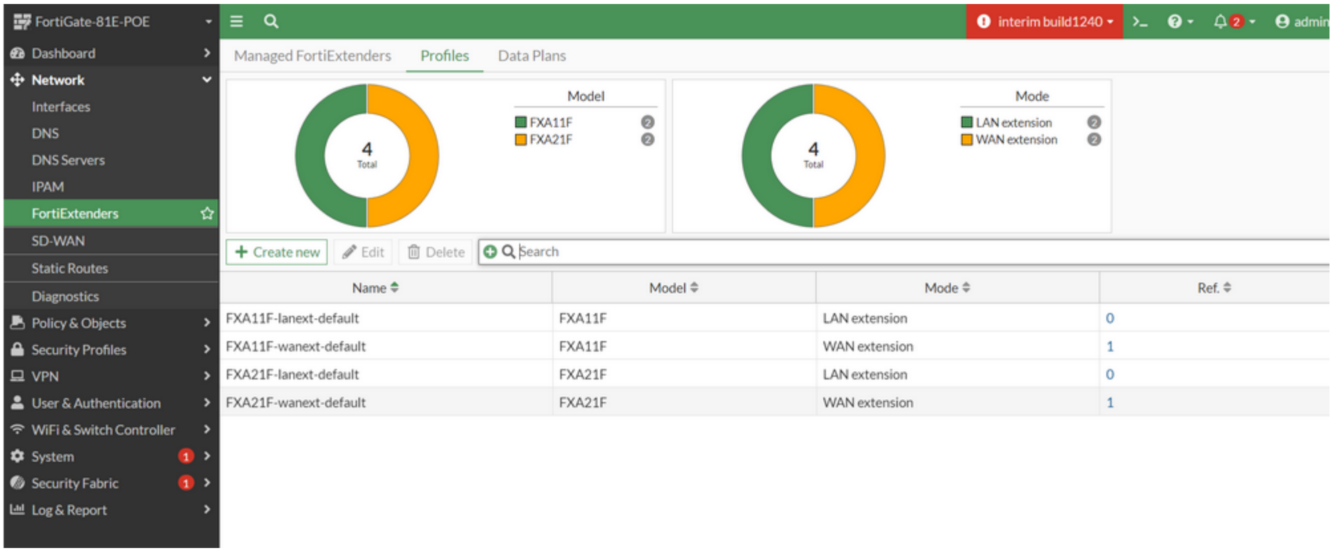
FortiGate GUI monitoring page when FortiExtender is authorized in wan-extension mode

- The "Modem 1 Interface #" column shows the FortiGate virtual interface which is built on the FortiExtender. This is the FortiGate WAN interface which extends to the FortiExtender LTE-modem.
- The "Details" column shows the data used on Modem1 / SIM1 in FXA21FTQ22000014.



Name	Status	Mode	Details	Modem 1 Interface	Profile	Serial #
FX004TQ21000005	Online	WAN extension	M1 / S2 37.00 MB	fext-vlan2	FXA11F-wanext-default	FXA11FTQ21000005
FX006TQ22000014	Online	WAN extension	M1 / S1 9.00 MB	fext-vlan	FXA21F-wanext-default	FXA21FTQ22000014

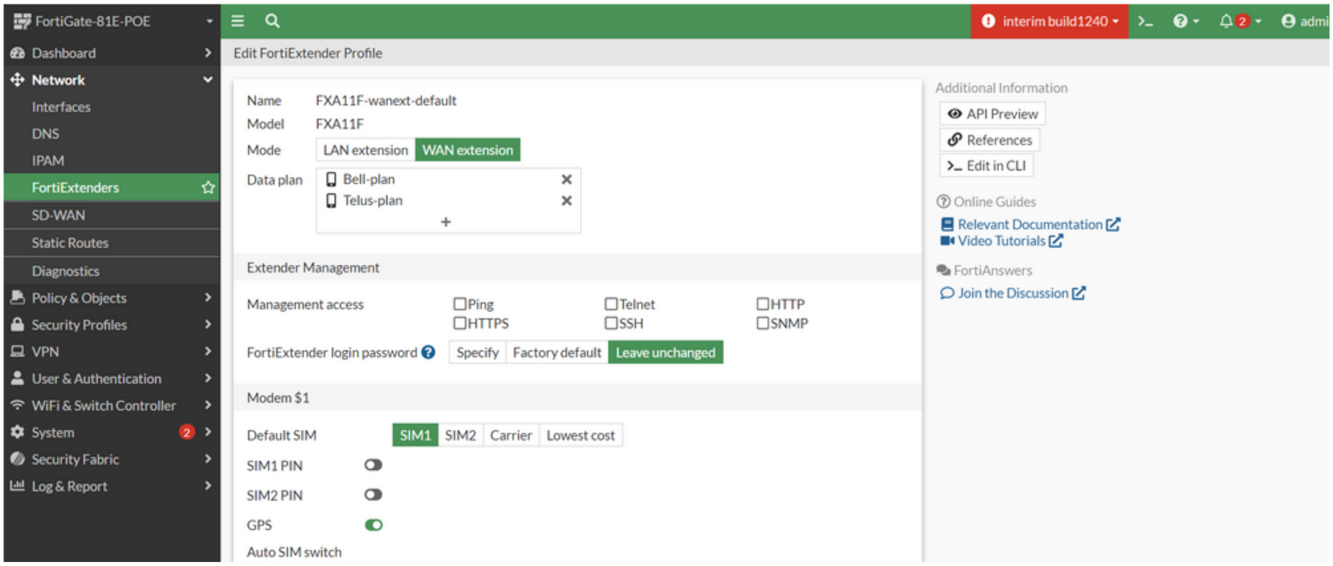
FortiGate GUI provides the profiles used for each FortiExtender



Name	Model	Mode	Ref.
FXA11F-lanext-default	FXA11F	LAN extension	0
FXA11F-wanext-default	FXA11F	WAN extension	1
FXA21F-lanext-default	FXA21F	LAN extension	0
FXA21F-wanext-default	FXA21F	WAN extension	1

FortiGate GUI provides profile settings for wan-extension

- "Default SIM" defines which SIM card starts to work first.
- SIM switch can be enabled by data plan. Assuming SIM1 uses Bell card. When its usage has reached the data limit in the plan, SIM2 (using Telus card) will be engaged to for service.



Edit FortiExtender Profile

Name FXA11F-wanext-default

Model FXA11F

Mode LAN extension [✓ WAN extension]

Data plan Bell-plan, Telus-plan

Extender Management

Management access □Ping □HTTPS □Telnet □SSH □HTTP □SNMP

FortiExtender login password Specify Factory default [✓ Leave unchanged]

Modem $1

Default SIM [✓ SIM1] SIM2 Carrier Lowest cost

SIM1 PIN ○

SIM2 PIN ○

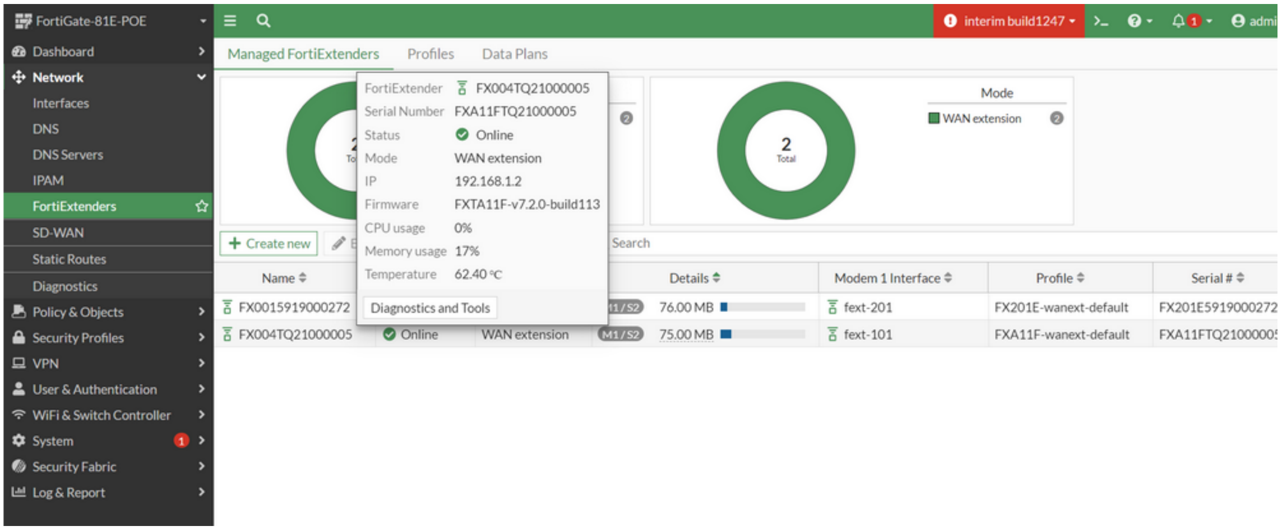
GPS ●

Auto SIM switch

FortiGate GUI provides detailed FortiExtender diagnostics pages

You can left-click the name of an FortiExtender or hover the mouse over the name to get the tooltip, as shown in the following image.

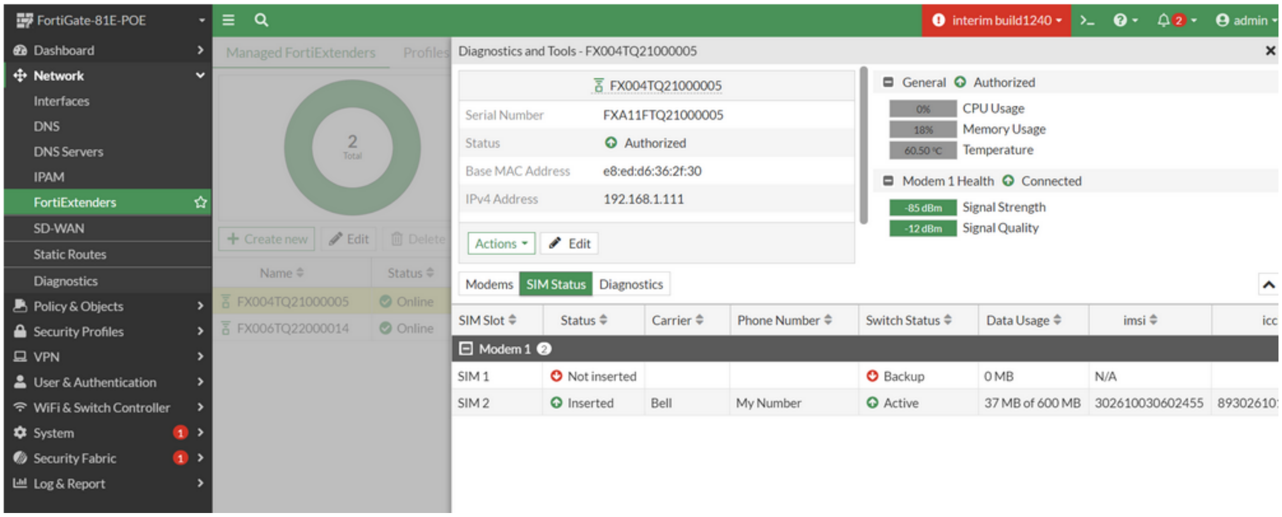
1. Click the name of an FortiExtender to get the following page.



FortiExtender	FX004TQ21000005
Serial Number	FXA11FTQ21000005
Status	Online
Mode	WAN extension
IP	192.168.1.2
Firmware	FXTA11F-v7.2.0-build113
CPU usage	0%
Memory usage	17%
Temperature	62.40 °C

Name				Details	Modem 1 Interface	Profile	Serial #
FX0015919000272			1 / S2	76.00 MB	fext-201	FX201E-wanext-default	FX201E5919000272
FX004TQ21000005	Online	WAN extension	M1 / S2	75.00 MB	fext-101	FXA11F-wanext-default	FXA11FTQ2100000

2. Click "Diagnostics and Tools" to open the Diagnostics and Tools page.



Diagnostics and Tools - FX004TQ21000005

FX004TQ21000005

Serial Number	FXA11FTQ21000005
Status	Authorized
Base MAC Address	e8:ed:d6:36:2f:30
IPv4 Address	192.168.1.111

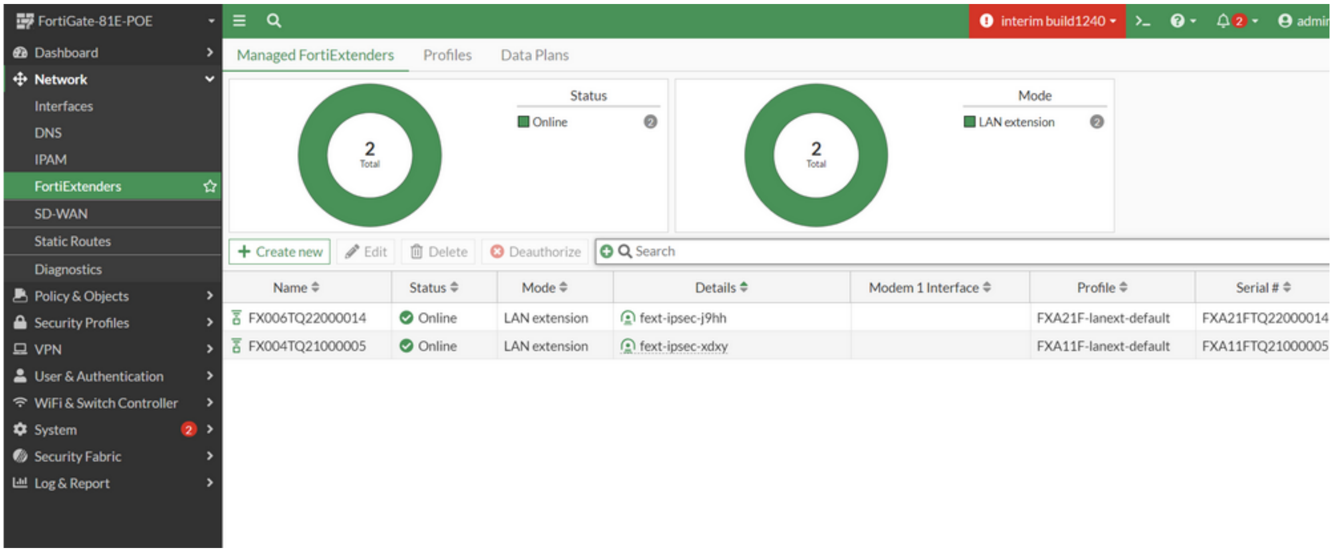
General Authorized
0% CPU Usage
18% Memory Usage
60.50 °C Temperature

Modem 1 Health Connected
-85 dBm Signal Strength
-12 dBm Signal Quality

SIM Slot	Status	Carrier	Phone Number	Switch Status	Data Usage	imsi	icc
Modem 1 2							
SIM 1	Not inserted			Backup	0 MB	N/A	
SIM 2	Inserted	Bell	My Number	Active	37 MB of 600 MB	302610030602455	89302610

FortiGate GUI monitoring page when FortiExtender is authorized in lan-extension mode

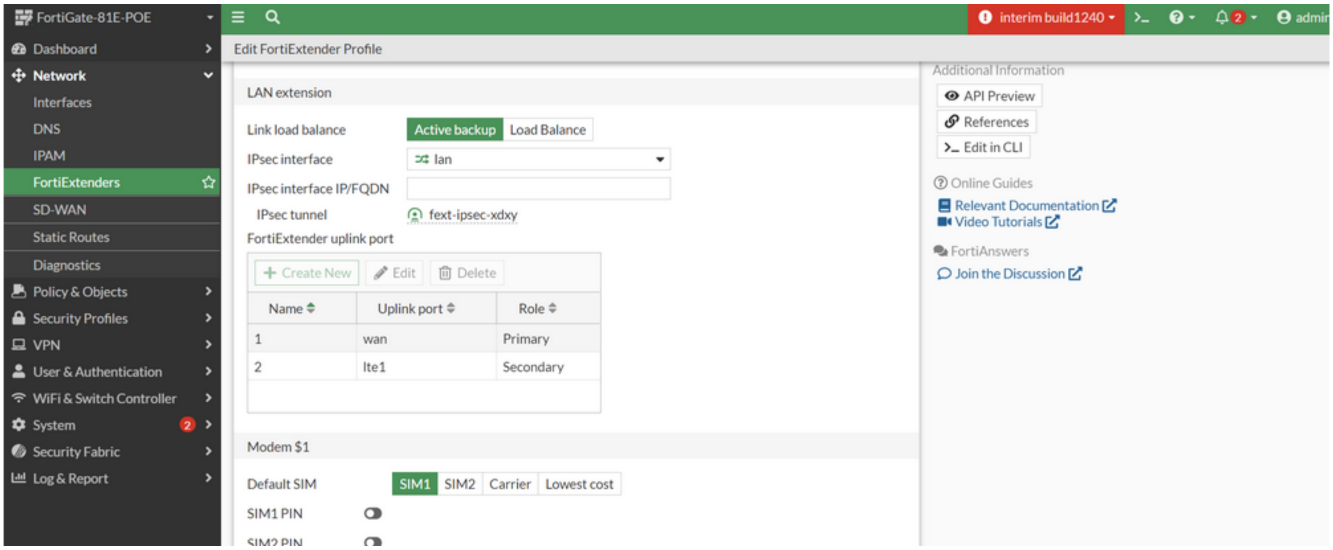
The "Details" column shows the IPSec tunnel between FortiGate and FortiExtender.



Name	Status	Mode	Details	Modem 1 Interface	Profile	Serial #
FX006TQ22000014	Online	LAN extension	fext-ipsec-j9hh		FXA21F-lanext-default	FXA21FTQ22000014
FX004TQ21000005	Online	LAN extension	fext-ipsec-xdxy		FXA11F-lanext-default	FXA11FTQ21000005

FortiGate GUI provides Profile settings for lan-extension

- You can set the IPsec tunnel connection between FortiExtender and FortiGate on this page.
- After multiple connections from FortiExtender (as uplink) are established, you can select load balance mode on this page.



Edit FortiExtender Profile

LAN extension

Link load balance: [✓ Active backup] Load Balance

IPsec interface: lan

IPsec interface IP/FQDN:

IPsec tunnel: fext-ipsec-xdxy

FortiExtender uplink port

+ Create New | Edit | Delete

Name	Uplink port	Role
1	wan	Primary
2	lte1	Secondary

Modem $1

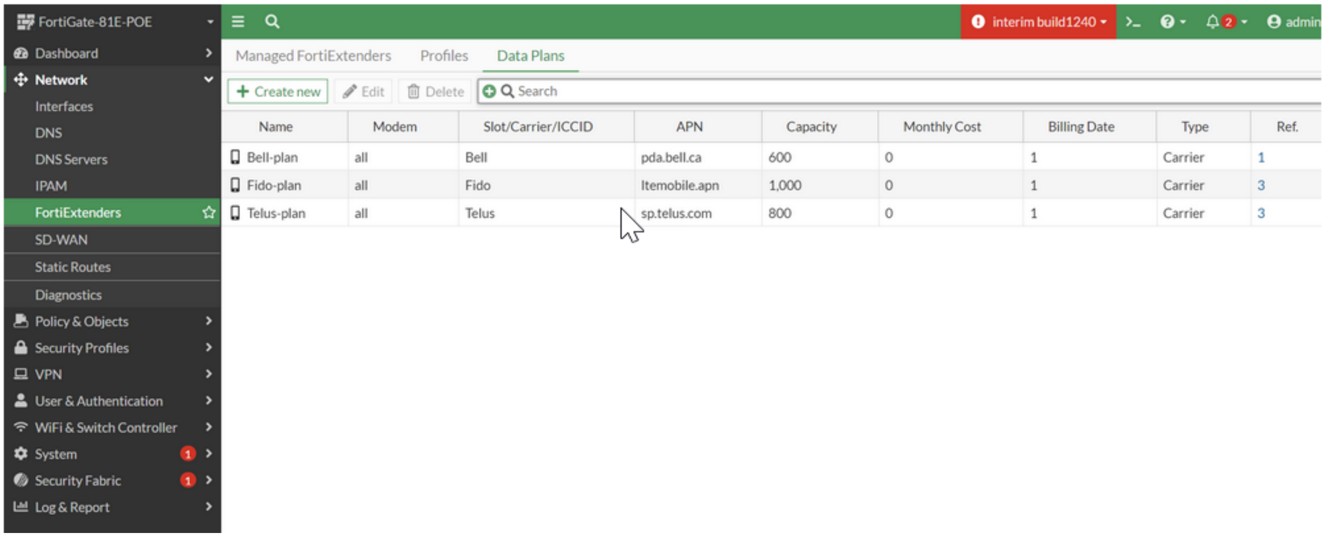
Default SIM: [✓ SIM1] SIM2 Carrier Lowest cost

SIM1 PIN ○

SIM2 PIN ○

FortiGate GUI provides the settings for data plan

- Each data plan is associated with a carrier name. After the SIM card is active, the modem will detect the carrier and use the corresponding plan.
- Each data plan has a data limit (capacity) that can be used by the SIM card. The data limit is reset after the billing date.



Name	Modem	Slot/Carrier/ICCID	APN	Capacity	Monthly Cost	Billing Date	Type	Ref.
Bell-plan	all	Bell	pda.bell.ca	600	0	1	Carrier	1
Fido-plan	all	Fido	ltemobile.apn	1,000	0	1	Carrier	3
Telus-plan	all	Telus	sp.telus.com	800	0	1	Carrier	3

Provision FortiExtender firmware upon authorization - 7.2.1

FortiExtender is now able to automatically perform firmware provisioning using CLI commands. This allows for federated upgrade of multiple FortiExtender units upon discovery and authorization by the FortiGate. Each FortiExtender device will be upgraded to the latest firmware from FortiGuard, based on the matching FortiExtender firmware version that matches each FortiOS firmware version.

1. FortiGuard has a matrix which contains the following table for each FortiExtender. The matrix code is FEXV.

   ```
   FGTVersion=7.2.1|FGTBuildNum=01247|FEXPlatform=FX201E|FEXVersion=7.2.0|FEXBuildNum=00113
   |ImageIdentifier=07002000FIMG1000102000
   ```

2. Test condition: The FortiGate has v7.2.1 b1247 and the FortiExtender has v7.0.3 b056.

   ```
   config system global
        set fortiextender-provision-on-authorization enable
   end
   ```

3. Once the FortiGate has authorized the FortiExtender, automatic update is enabled for one time.

   ```
     config extension-controller extender
        edit "FX0015919000272"
             set id "FX201E5919000272"
             set authorized enable <<-------------------- Upon user auth,
             set device-id 1
             set extension-type wan-extension
             set profile "FX201E-wanext-default"
             set override-allowaccess enable
             set allowaccess ping telnet
             set override-login-password-change enable
             config wan-extension
             set modem1-extension "fext-201"
             end
                set firmware-provision-latest once <<------- Config is automatically set to
                     "once"
        next
     end
   ```

4. Once the FortiGate starts to manage the FortiExtender and detects that the FortiExtender's build number is lower than that in the matrix (v7.2.0 b0113), the FortiGate will push the image (b0113) to the FortiExtender.

De-authorize FortiExtender devices - 7.2.4

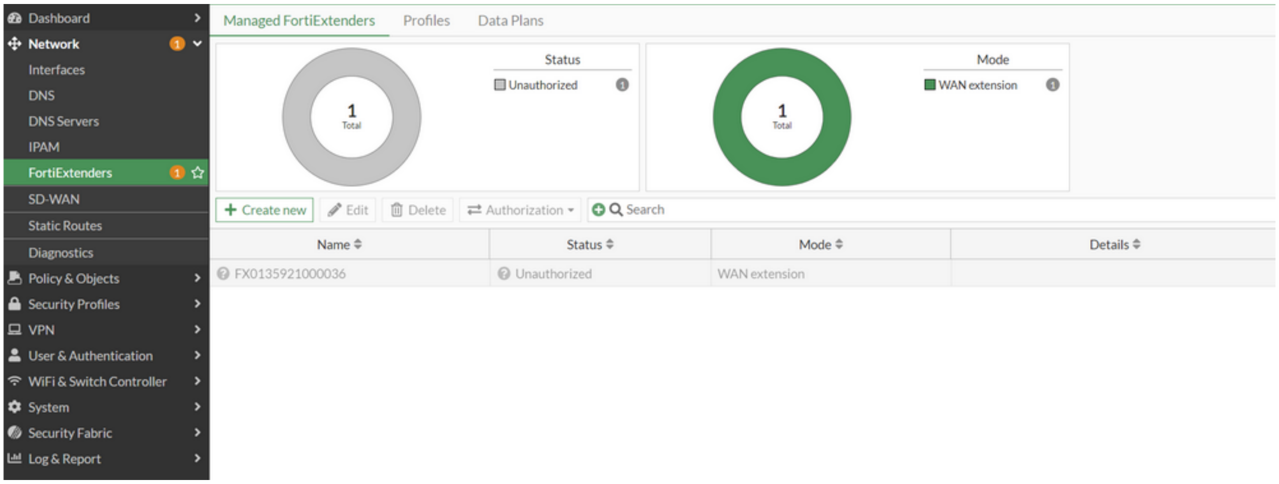
This information is also available in the FortiExtender 7.2.4 Admin Guide:

- De-authorize FortiExtender devices

FortiExtenders discovered by the FortiGate configured as a controller used to show up on the FortiGate GUI as pending authorization, causing confusion in certain situation. This enhancement enables you to disable a discovered FortiExtender device on a FortiGate configured as a FortiExtender controller from the GUI or the CLI.

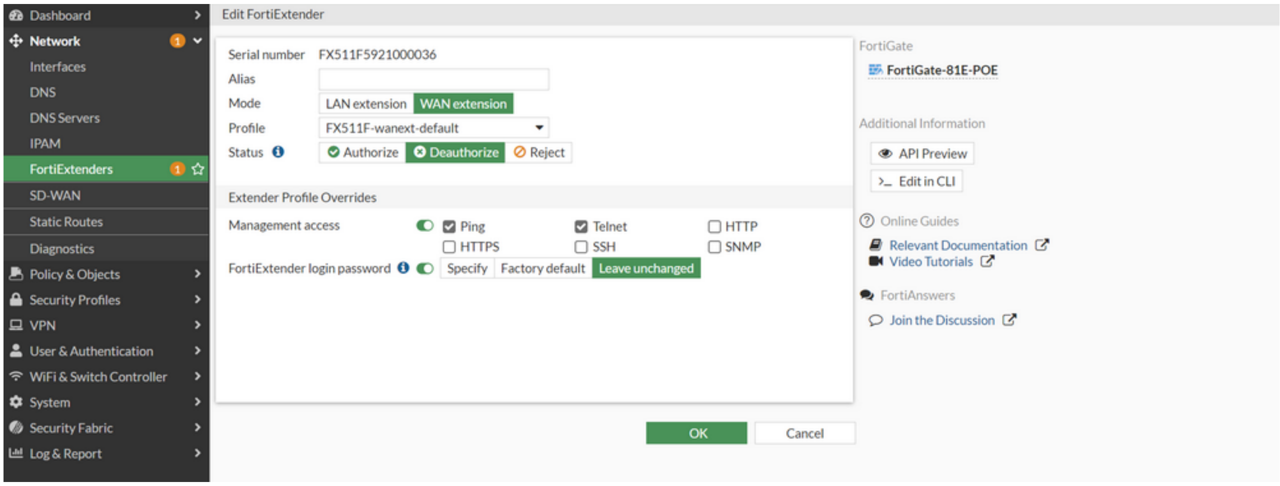
GUI

1. Locate the FortiExtender in "Unauthorized" status.



Name	Status	Mode	Details
FX0135921000036	Unauthorized	WAN extension	

2. Select the FortiExtender and click "Edit". Note: The original status is "Deauthorized"

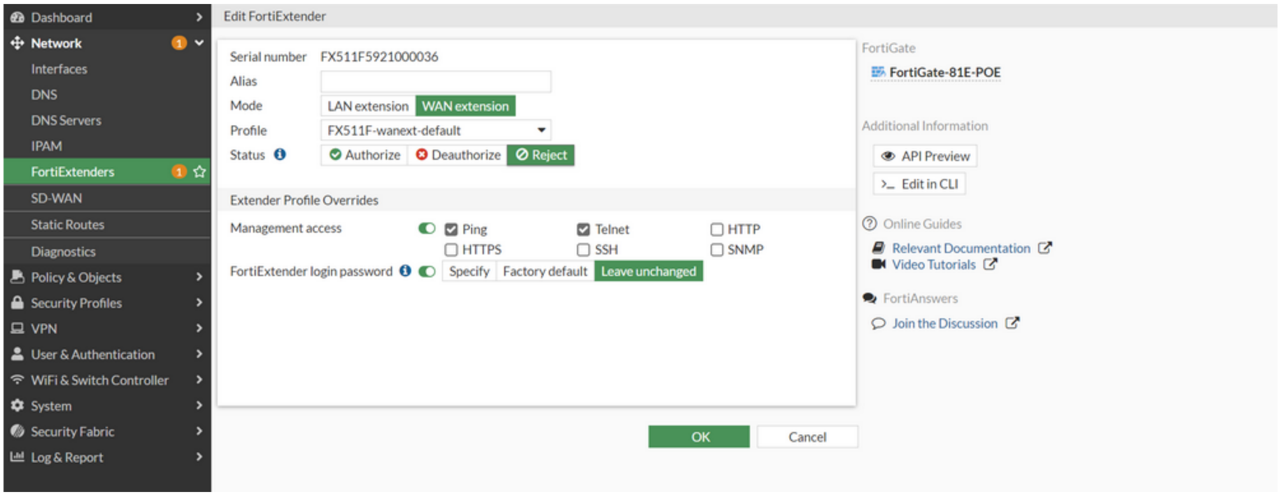


Serial number FX511F5921000036
Alias
Mode LAN extension [✓ WAN extension]
Profile FX511F-wanext-default
Status Authorize [✓ Deauthorize] Reject

Extender Profile Overrides

Management access ● ☑ Ping ☑ Telnet ☐ HTTP ☐ HTTPS ☐ SSH ☐ SNMP
FortiExtender login password ● Specify Factory default [✓ Leave unchanged]

3. Set the status to "Reject", and click OK.

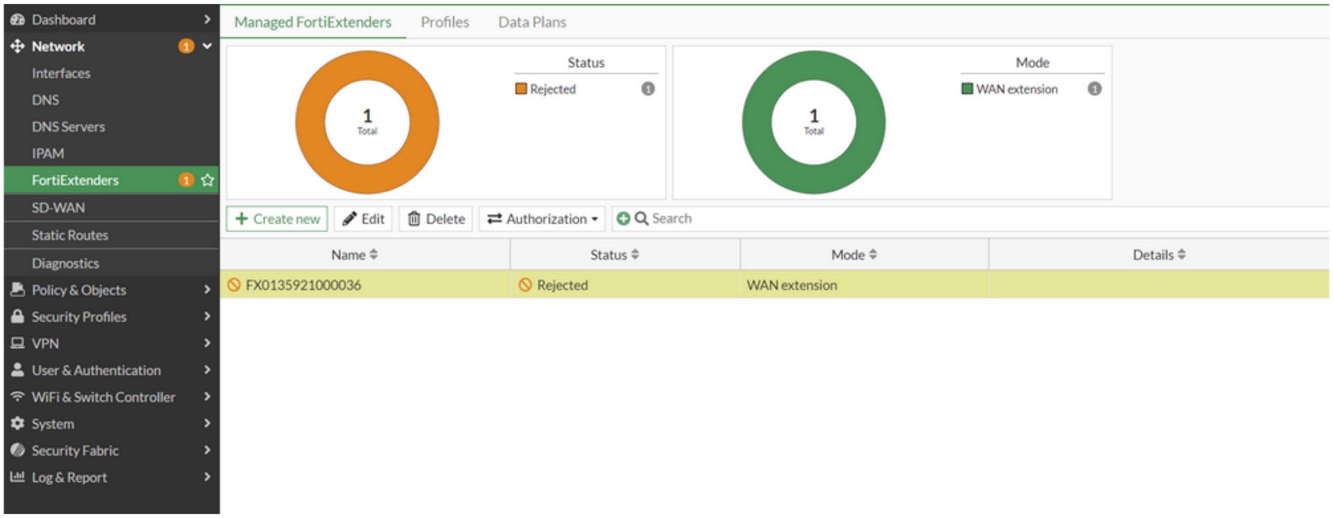


Serial number FX511F5921000036
Alias
Mode LAN extension [✓ WAN extension]
Profile FX511F-wanext-default
Status Authorize Deauthorize [✓ Reject]

Extender Profile Overrides

Management access ● ☑ Ping ☑ Telnet ☐ HTTP ☐ HTTPS ☐ SSH ☐ SNMP
FortiExtender login password ● Specify Factory default [✓ Leave unchanged]

The following image shows the status of the FortiExtender after it is being rejected.



Name	Status	Mode	Details
FX0135921000036	Rejected	WAN extension	

CLI

When the FortiExtender is in "discovered' state.

```
config extension-controller extender
    edit "FX0135921000036"
        set id "FX511F5921000036"
        set authorized discovered
```

You can change it to "disable" state. It will be shown as "Reject" in the GUI.

```
config extension-controller extender
    edit "FX0135921000036"
        set id "FX511F5921000036"
        set authorized disable
```

Log and report

This section includes information about logging and reporting related new features:

- Logging on page 575

Logging

This section includes information about logging related new features:

- Add IOC detection for local out traffic on page 575
- HTTP transaction log fields on page 577
- Updated System Events log page on page 581
- New Security Events log page on page 584
- Improve FortiAnalyzer log caching on page 587
- Add FortiAnalyzer Reports page on page 590
- Summary tabs on System Events and Security Events log pages 7.2.1 on page 592
- Add time frame selector to log viewer pages 7.2.1 on page 593
- Updating log viewer and log filters 7.2.1 on page 594
- Consolidate log reports and settings into dedicated Reports and Log Settings pages 7.2.4 on page 597
- Add Logs Sent Daily chart for remote logging sources 7.2.4 on page 599

Add IOC detection for local out traffic

Indicator of compromise (IOC) detection for local out traffic helps detect any FortiGate locally-generated traffic that is destined for a known compromised location. The FortiGate will generate an event log to warn administrators of an IOC detection. This feature currently only supports IPv4 traffic.

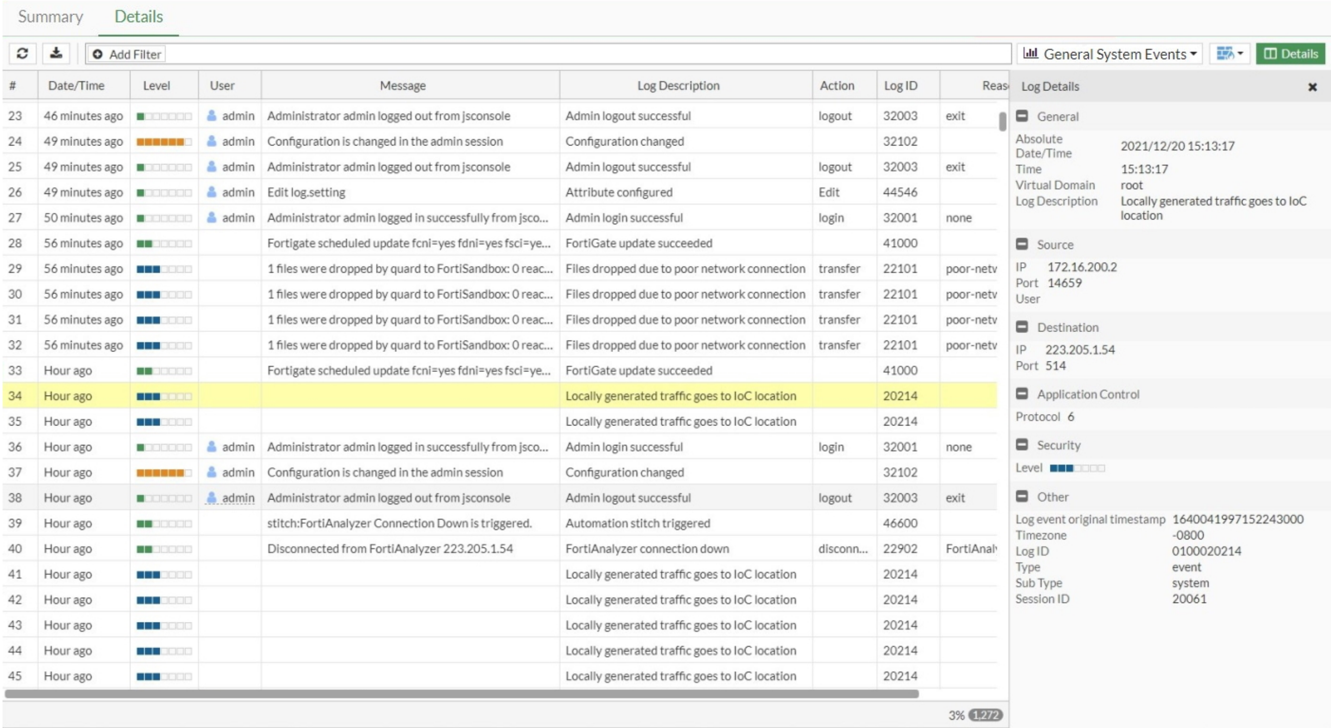
To log IOC detection in local out traffic:

```
config log setting
    set local-out {enable | disable}
    set local-out-ioc-detection {enable | disable}
end
```

These settings are both enabled by default. IOC detection is a VDOM-specific feature, so logging must be enabled on each VDOM.

Sample event log:

In the GUI, go to *Log & Report* > *System Events*, click the *General System Events* card, and click the *Details* tab.



#	Date/Time	Level	User	Message	Log Description	Action	Log ID	Reas
23	46 minutes ago	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	logout	32003	exit
24	49 minutes ago	■■■■■■□	admin	Configuration is changed in the admin session	Configuration changed		32102	
25	49 minutes ago	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	logout	32003	exit
26	49 minutes ago	■□□□□□□	admin	Edit log.setting	Attribute configured	Edit	44546	
27	50 minutes ago	■□□□□□□	admin	Administrator admin logged in successfully from jsco...	Admin login successful	login	32001	none
28	56 minutes ago	■■□□□□□		Fortigate scheduled update fcni=yes fdni=yes fsci=ye...	FortiGate update succeeded		41000	
29	56 minutes ago	■■■□□□□		1 files were dropped by quard to FortiSandbox: 0 reac...	Files dropped due to poor network connection	transfer	22101	poor-netv
30	56 minutes ago	■■■□□□□		1 files were dropped by quard to FortiSandbox: 0 reac...	Files dropped due to poor network connection	transfer	22101	poor-netv
31	56 minutes ago	■■■□□□□		1 files were dropped by quard to FortiSandbox: 0 reac...	Files dropped due to poor network connection	transfer	22101	poor-netv
32	56 minutes ago	■■■□□□□		1 files were dropped by quard to FortiSandbox: 0 reac...	Files dropped due to poor network connection	transfer	22101	poor-netv
33	Hour ago	■■□□□□□		Fortigate scheduled update fcni=yes fdni=yes fsci=ye...	FortiGate update succeeded		41000	
34	Hour ago	■■■□□□□			Locally generated traffic goes to IoC location		20214	
35	Hour ago	■■■□□□□			Locally generated traffic goes to IoC location		20214	
36	Hour ago	■□□□□□□	admin	Administrator admin logged in successfully from jsco...	Admin login successful	login	32001	none
37	Hour ago	■■■■■■□	admin	Configuration is changed in the admin session	Configuration changed		32102	
38	Hour ago	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	logout	32003	exit
39	Hour ago	■■□□□□□		stitch:FortiAnalyzer Connection Down is triggered.	Automation stitch triggered		46600	
40	Hour ago	■■□□□□□		Disconnected from FortiAnalyzer 223.205.1.54	FortiAnalyzer connection down	disconn...	22902	FortiAnal
41	Hour ago	■■■□□□□			Locally generated traffic goes to IoC location		20214	
42	Hour ago	■■■□□□□			Locally generated traffic goes to IoC location		20214	
43	Hour ago	■■■□□□□			Locally generated traffic goes to IoC location		20214	
44	Hour ago	■■■□□□□			Locally generated traffic goes to IoC location		20214	
45	Hour ago	■■■□□□□			Locally generated traffic goes to IoC location		20214	

3% 1,272

Log Details

General

Absolute Date/Time	2021/12/20 15:13:17
Time	15:13:17
Virtual Domain	root
Log Description	Locally generated traffic goes to IoC location

Source

IP	172.16.200.2
Port	14659
User	

Destination

IP	223.205.1.54
Port	514

Application Control

Protocol 6

Security

Level ■■■□□□□

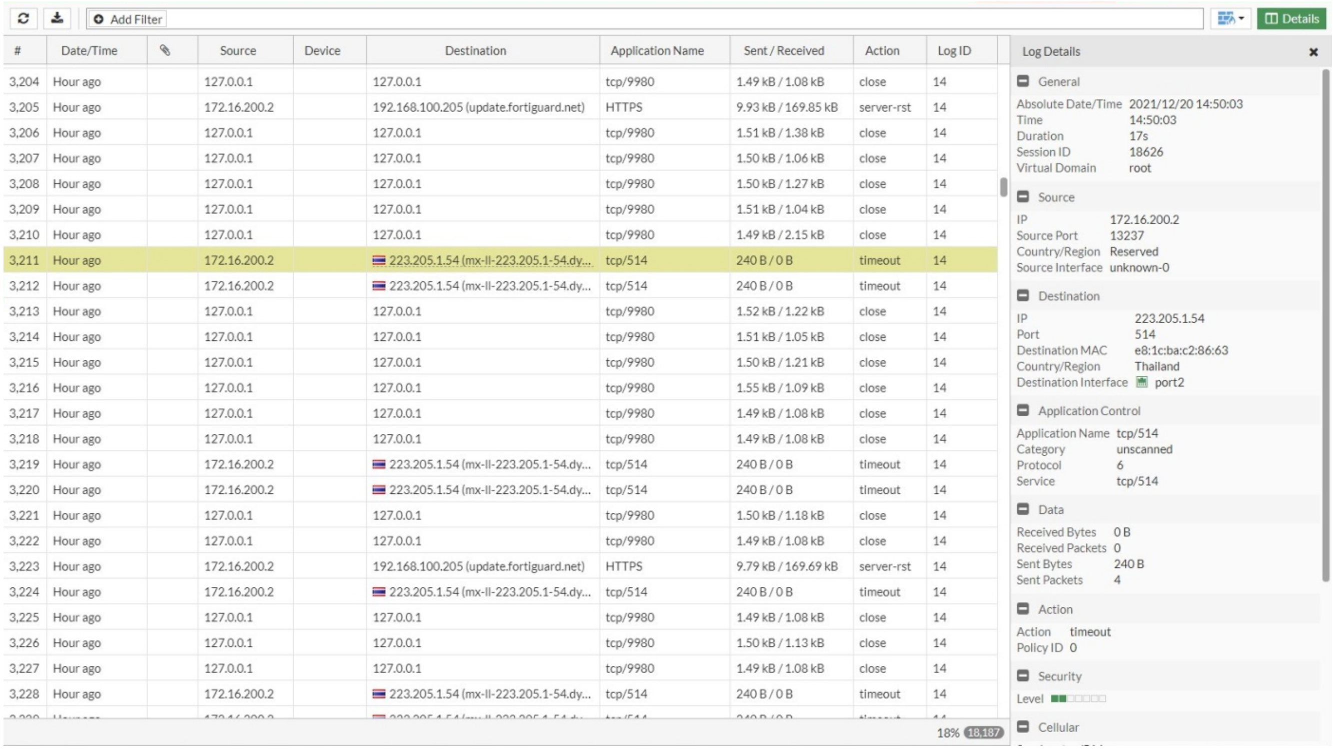
Other

Log event original timestamp	1640041997152243000
Timezone	-0800
Log ID	0100020214
Type	event
Sub Type	system
Session ID	20061

```
1: date=2021-12-20 time=16:43:54 eventtime=1640047434839814226 tz="-0800" logid="0100020214"
type="event" subtype="system" level="warning" vd="root" logdesc="Locally generated traffic
goes to IoC location" srcip=172.16.200.2 srcport=18047 dstip=223.205.1.54 dstport=514
session_id=23563 proto=6
```

Sample traffic log:

In the GUI, go to *Log & Report* > *Local Traffic*.



#	Date/Time	📎	Source	Device	Destination	Application Name	Sent / Received	Action	Log ID
3,204	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.49 kB / 1.08 kB	close	14
3,205	Hour ago		172.16.200.2		192.168.100.205 (update.fortiguard.net)	HTTPS	9.93 kB / 169.85 kB	server-rst	14
3,206	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.51 kB / 1.38 kB	close	14
3,207	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.50 kB / 1.06 kB	close	14
3,208	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.50 kB / 1.27 kB	close	14
3,209	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.51 kB / 1.04 kB	close	14
3,210	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.49 kB / 2.15 kB	close	14
3,211	Hour ago		172.16.200.2		223.205.1.54 (mx-ll-223.205.1-54.dy...	tcp/514	240 B / 0 B	timeout	14
3,212	Hour ago		172.16.200.2		223.205.1.54 (mx-ll-223.205.1-54.dy...	tcp/514	240 B / 0 B	timeout	14
3,213	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.52 kB / 1.22 kB	close	14
3,214	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.51 kB / 1.05 kB	close	14
3,215	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.50 kB / 1.21 kB	close	14
3,216	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.55 kB / 1.09 kB	close	14
3,217	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.49 kB / 1.08 kB	close	14
3,218	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.49 kB / 1.08 kB	close	14
3,219	Hour ago		172.16.200.2		223.205.1.54 (mx-ll-223.205.1-54.dy...	tcp/514	240 B / 0 B	timeout	14
3,220	Hour ago		172.16.200.2		223.205.1.54 (mx-ll-223.205.1-54.dy...	tcp/514	240 B / 0 B	timeout	14
3,221	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.50 kB / 1.18 kB	close	14
3,222	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.49 kB / 1.08 kB	close	14
3,223	Hour ago		172.16.200.2		192.168.100.205 (update.fortiguard.net)	HTTPS	9.79 kB / 169.69 kB	server-rst	14
3,224	Hour ago		172.16.200.2		223.205.1.54 (mx-ll-223.205.1-54.dy...	tcp/514	240 B / 0 B	timeout	14
3,225	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.49 kB / 1.08 kB	close	14
3,226	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.50 kB / 1.13 kB	close	14
3,227	Hour ago		127.0.0.1		127.0.0.1	tcp/9980	1.49 kB / 1.08 kB	close	14
3,228	Hour ago		172.16.200.2		223.205.1.54 (mx-ll-223.205.1-54.dy...	tcp/514	240 B / 0 B	timeout	14

Log Details

General

Absolute Date/Time	2021/12/20 14:50:03
Time	14:50:03
Duration	17s
Session ID	18626
Virtual Domain	root

Source

IP	172.16.200.2
Source Port	13237
Country/Region	Reserved
Source Interface	unknown-0

Destination

IP	223.205.1.54
Port	514
Destination MAC	e8:1c:ba:c2:86:63
Country/Region	Thailand
Destination Interface	port2

Application Control

Application Name	tcp/514
Category	unscanned
Protocol	6
Service	tcp/514

Data

Received Bytes	0 B
Received Packets	0
Sent Bytes	240 B
Sent Packets	4

Action

Action	timeout
Policy ID	0

Security

Level

Cellular

```
1: date=2021-12-20 time=16:45:18 eventtime=1640047518959313316 tz="-0800" logid="0001000014"
type="traffic" subtype="local" level="notice" vd="root" srcip=172.16.200.2 srcport=18116
srcintf="unknown-0" srcintfrole="undefined" dstip=223.205.1.54 dstport=514 dstintf="port2"
dstintfrole="undefined" srccountry="Reserved" dstcountry="Thailand" sessionid=23632 proto=6
action="timeout" policyid=0 service="tcp/514" trandisp="noop" app="tcp/514" duration=17
sentbyte=240 rcvdbyte=0 sentpkt=4 rcvdpkt=0 appcat="unscanned" dsthwvendor="Fortinet"
masterdstmac="e8:1c:ba:c2:86:63" dstmac="e8:1c:ba:c2:86:63" dstserver=0
```

HTTP transaction log fields

HTTP transaction related logs are updated to improve log analysis coverage.

- An `httpmethod` field is added.
- The URL rating method field is renamed from `method` to `ratemethod`.
- The `agent` field includes the entire User-Agent header.
- The `referer` field is removed from the `rawdata` field and added to the `referralurl` field.

Log samples

Proxy web filter logs

```
1: date=2022-02-09 time=16:39:40 eventtime=1644453580728994264 tz="-0800" logid="0317013312"
type="utm" subtype="webfilter" eventtype="ftgd_allow" level="notice" vd="vdom1" policyid=1
poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" sessionid=803
srcip=10.1.100.110 srcport=61913 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" dstip=45.33.7.16
dstport=443 dstcountry="United States" dstintf="port1" dstintfrole="undefined"
```

```
dstuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" proto=6 httpmethod="GET" service="HTTPS"
hostname="www.httpvshttps.com" agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36"
profile="webfilter" action="passthrough" reqtype="referral"
url="https://www.httpvshttps.com/" referralurl="http://www.httpvshttps.com/" sentbyte=1433
rcvdbyte=5143 direction="outgoing" msg="URL belongs to an allowed category in policy"
ratemethod="domain" cat=52 catdesc="Information Technology"
```

With rawdata field:

```
1: date=2022-02-09 time=16:56:13 eventtime=1644454573193935755 tz="-0800" logid="0317013312"
type="utm" subtype="webfilter" eventtype="ftgd_allow" level="notice" vd="vdom1" policyid=1
poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" sessionid=309
srcip=10.1.100.18 srcport=54884 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" dstip=52.21.106.99
dstport=443 dstcountry="United States" dstintf="port1" dstintfrole="undefined"
dstuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" proto=6 httpmethod="GET" service="HTTPS"
hostname="www.postman-echo.com" forwardedfor="192.168.0.99" agent="curl/7.56.0"
profile="webfilter" action="passthrough" reqtype="referral" url="https://www.postman-
echo.com/" referralurl="https://example.com/referer.html" sentbyte=886 rcvdbyte=5531
direction="outgoing" msg="URL belongs to an allowed category in policy" ratemethod="domain"
cat=52 catdesc="Information Technology" rawdata="x-forwarded-for=192.168.0.99|Request-
Content-Type=application/json"
```

Proxy antivirus log

```
1: date=2022-02-03 time=17:37:51 eventtime=1643938671287113448 tz="-0800" logid="0211008192"
type="utm" subtype="virus" eventtype="infected" level="warning" vd="vdom1" policyid=1
poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" msg="File is infected."
action="blocked" service="HTTPS" sessionid=156474 srcip=10.1.100.18 dstip=89.238.73.97
srcport=36154 dstport=443 srccountry="Reserved" dstcountry="Germany" srcintf="port2"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" srcuuid="a27c19fc-8499-51ec-
b63d-7ff51b02a295" dstuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" proto=6
direction="incoming" filename="eicar.com" quarskip="Quarantine-disabled" virus="EICAR_TEST_
FILE" viruscat="Virus" dtype="av-engine" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE"
virusid=2172 url="https://secure.eicar.org/eicar.com" forwardedfor="192.168.0.99"
profile="proxy-av" agent="curl/7.56.0" httpmethod="GET"
referralurl="https://example.com/referer.html"
analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical" rawdata="X-Forwarded-
For=192.168.0.99|Response-Content-Type=application/x-msdownload"
```

Proxy DLP log

```
1: date=2022-02-03 time=17:36:12 eventtime=1643938572487964255 tz="-0800" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" filteridx=1
dlpextra="pdf" filtertype="file-type" filtercat="file" severity="critical" policyid=1
poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" sessionid=156237
epoch=300501327 eventid=0 srcip=10.1.100.18 srcport=33392 srccountry="Reserved"
srcintf="port2" srcintfrole="undefined" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295"
dstip=172.16.200.88 dstport=443 dstcountry="Reserved" dstintf="port1"
dstintfrole="undefined" dstuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" proto=6
service="HTTPS" filetype="pdf" direction="incoming" action="block" hostname="172.16.200.88"
url="https://172.16.200.88/dlp/files/fortiauto.pdf" forwardedfor="192.168.0.99"
agent="curl/7.56.0" httpmethod="GET" referralurl="https://example.com/referer.html"
```

```
filename="fortiauto.pdf" filesize=285442 profile="proxy-dlp" rawdata="x-forwarded-
for=192.168.0.99|Response-Content-Type=application/pdf"
```

Proxy file filter log

```
1: date=2022-02-03 time=17:31:57 eventtime=1643938317607666534 tz="-0800" logid="1900064000"
type="utm" subtype="file-filter" eventtype="file-filter" level="warning" vd="vdom1"
policyid=1 poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy"
sessionid=155704 srcip=10.1.100.18 srcport=33388 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" dstip=172.16.200.88
dstport=443 dstcountry="Reserved" dstintf="port1" dstintfrole="undefined" dstuuid="a27c19fc-
8499-51ec-b63d-7ff51b02a295" proto=6 service="HTTPS" profile="proxy-ff" direction="incoming"
action="blocked" url="https://172.16.200.88/dlp/files/fortiauto.pdf"
hostname="172.16.200.88" agent="curl/7.56.0" httpmethod="GET"
referralurl="https://example.com/referer.html" forwardedfor="192.168.0.99" filtername="pdf"
filename="fortiauto.pdf" filesize=285442 filetype="pdf" msg="File was blocked by file
filter."
```

Proxy video filter log

```
1: date=2022-02-10 time=14:25:20 eventtime=1644531920649244437 tz="-0800" logid="0348013682"
type="utm" subtype="webfilter" eventtype="videofilter-channel" level="notice" vd="vdom1"
msg="Video channel is allowed." policyid=10 sessionid=1535 srcip=10.1.100.11
dstip=142.251.33.78 srcport=47348 dstport=443 srcintf="port2" srcintfrole="undefined"
dstintf="port1" dstintfrole="undefined" proto=6 httpmethod="GET" service="HTTPS"
action="passthrough" videoinfosource="Cache" profile="channel_filter" videoid="BAayV5xQ1TE"
videochannelid="UCjzrDTsJKtMQI33Vii_jEeA" hostname="www.youtube.com" agent="('Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193
Safari/537.36',)" url="https://www.youtube.com/watch?v=BAayV5xQ1TE"
```

WAF log

```
1: date=2022-02-03 time=17:44:29 eventtime=1643939069074906029 tz="-0800" logid="1203030257"
type="utm" subtype="waf" eventtype="waf-http-constraint" level="warning" vd="vdom1"
policyid=1 policytype="policy" sessionid=157514 profile="waf-profile" srcip=10.1.100.18
srcport=36206 srccountry="Reserved" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295"
dstip=89.238.73.97 dstport=443 dstcountry="Germany" dstuuid="a27c19fc-8499-51ec-b63d-
7ff51b02a295" srcintf="port2" srcintfrole="undefined" dstintf="port1"
dstintfrole="undefined" proto=6 httpmethod="GET" service="HTTPS"
url="https://secure.eicar.org/eicar.com" direction="https://example.com/referer.html"
severity="medium" action="blocked" direction="request" agent="curl/7.56.0"
constraint="header-number"
```

Flow web filter log

```
1: date=2022-02-04 time=10:48:10 eventtime=1644000490629159450 tz="-0800" logid="0317013312"
type="utm" subtype="webfilter" eventtype="ftgd_allow" level="notice" vd="vdom1" policyid=1
poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" sessionid=3198
srcip=10.1.100.18 srcport=38206 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" dstip=34.233.143.14
dstport=443 dstcountry="United States" dstintf="port1" dstintfrole="undefined"
dstuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" proto=6 httpmethod="GET" service="HTTPS"
hostname="www.postman-echo.com" forwardedfor="192.168.0.99" agent="curl/7.56.0"
profile="webfilter_flowbase" action="passthrough" reqtype="referral"
url="https://www.postman-echo.com/" referralurl="https://example.com/referer.html"
```

```
sentbyte=165 rcvdbyte=40 direction="outgoing" msg="URL belongs to an allowed category in
policy" ratemethod="domain" cat=52 catdesc="Information Technology" rawdata="Request-
Content-Type=application/json|X-Forwarded-For=192.168.0.99"
```

Flow antivirus log

```
1: date=2022-02-03 time=17:01:06 eventtime=1643936466815721219 tz="-0800" logid="0211008192"
type="utm" subtype="virus" eventtype="infected" level="warning" vd="vdom1" policyid=1
poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" msg="File is infected."
action="blocked" service="HTTPS" sessionid=151261 srcip=10.1.100.18 dstip=89.238.73.97
srcport=35976 dstport=443 srccountry="Reserved" dstcountry="Germany" srcintf="port2"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" srcuuid="a27c19fc-8499-51ec-
b63d-7ff51b02a295" dstuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" proto=6
direction="incoming" filename="eicar.com" quarskip="Quarantine-disabled" virus="EICAR_TEST_
FILE" viruscat="Virus" dtype="av-engine" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE"
virusid=2172 url="https://secure.eicar.org/eicar.com" forwardedfor="192.168.0.99"
profile="flow-av" agent="curl/7.56.0" httpmethod="GET"
referralurl="https://example.com/referer.html"
analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical" rawdata="X-Forwarded-
For=192.168.0.99"
```

Flow DLP log

```
1: date=2022-02-03 time=17:04:04 eventtime=1643936644326594838 tz="-0800" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" filteridx=3
filtertype="file-type" filtercat="file" severity="critical" policyid=1 poluuid="917edc76-
84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" sessionid=151657 epoch=0 eventid=0
srcip=10.1.100.18 srcport=33236 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" dstip=172.16.200.88
dstport=443 dstcountry="Reserved" dstintf="port1" dstintfrole="undefined" dstuuid="a27c19fc-
8499-51ec-b63d-7ff51b02a295" proto=6 service="HTTPS" filetype="unknown" direction="incoming"
action="block" hostname="172.16.200.88" url="https://172.16.200.88/dlp/files/fortiauto.pdf"
forwardedfor="192.168.0.99" agent="curl/7.56.0" httpmethod="GET"
referralurl="https://example.com/referer.html" filename="fortiauto.pdf" profile="dlp-flow"
rawdata="X-Forwarded-For=192.168.0.99"
```

Flow file filter log

```
1: date=2022-02-03 time=17:11:49 eventtime=1643937109408719896 tz="-0800" logid="1900064000"
type="utm" subtype="file-filter" eventtype="file-filter" level="warning" vd="vdom1"
policyid=1 poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy"
sessionid=152777 srcip=10.1.100.18 srcport=33320 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="a27c19fc-8499-51ec-b63d-7ff51b02a295" dstip=172.16.200.88
dstport=443 dstcountry="Reserved" dstintf="port1" dstintfrole="undefined" dstuuid="a27c19fc-
8499-51ec-b63d-7ff51b02a295" proto=6 service="HTTPS" profile="flow-ff" direction="incoming"
action="blocked" url="https://172.16.200.88/dlp/files/fortiauto.pdf"
hostname="172.16.200.88" agent="curl/7.56.0" httpmethod="GET"
referralurl="https://example.com/referer.html" forwardedfor="192.168.0.99" filtername="pdf"
filename="fortiauto.pdf" filesize=285442 filetype="pdf" msg="File was blocked by file
filter."
```

IPS log

```
1: date=2022-02-03 time=23:02:37 eventtime=1643958157685566389 tz="-0800" logid="0419016384"
type="utm" subtype="ips" eventtype="signature" level="alert" vd="vdom1" severity="info"
srcip=10.1.100.18 srccountry="Reserved" dstip=89.238.73.97 dstcountry="Germany"
srcintf="port2" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined"
sessionid=201497 action="dropped" proto=6 service="HTTPS" policyid=1 poluuid="917edc76-84b1-
51ec-bdb5-b8cb1b308a99" policytype="policy" attack="Eicar.Virus.Test.File" srcport=37042
dstport=443 hostname="secure.eicar.org" url="/eicar.com" agent="curl/7.56.0"
httpmethod="GET" referralurl="https://example.com/referer.html" direction="incoming"
attackid=29844 profile="eicar-test" ref="http://www.fortinet.com/ids/VID29844"
incidentserialno=70256054 msg="file_transfer: Eicar.Virus.Test.File" rawdataid="1/1"
forwardedfor="192.168.0.99" rawdata="Response-Content-Type=application/x-msdownload|X-
Forwarded-For=192.168.0.99"
```

Application control log

```
1: date=2022-02-03 time=22:33:09 eventtime=1643956389997354519 tz="-0800" logid="1059028704"
type="utm" subtype="app-ctrl" eventtype="signature" level="information" vd="vdom1"
appid=15893 srcip=10.1.100.18 srccountry="Reserved" dstip=3.209.99.235 dstcountry="United
States" srcport=59896 dstport=80 srcintf="port2" srcintfrole="undefined" dstintf="port1"
dstintfrole="undefined" proto=6 service="HTTP" direction="outgoing" policyid=1
poluuid="917edc76-84b1-51ec-bdb5-b8cb1b308a99" policytype="policy" sessionid=197164
applist="app-ctrl" action="pass" appcat="Web.Client" app="HTTP.BROWSER"
hostname="www.httpbin.org" incidentserialno=70256051 url="/post" agent="curl/7.56.0"
httpmethod="POST" referralurl="http://example.com" msg="Web.Client: HTTP.BROWSER"
apprisk="medium" forwardedfor="192.168.0.99" rawdataid="1/1" rawdata="Request-Content-
Type=application/x-www-form-urlencoded|X-Forwarded-For=192.168.0.99"
```

Updated System Events log page

The *Log & Report* > *Events* page is now renamed *System Events*. The *System Events* page includes:

- A *Summary* tab that displays the top five most frequent events in each type of event log and a line chart to show aggregated events by each severity level. Clicking on a peak in the line chart will display the specific event count for the selected severity level.
- A *Details* tab that displays individual, detailed log views for event type.

Clicking on an event in the *Summary* tab will automatically bring users to the *Details* tab with the appropriate filters applied.

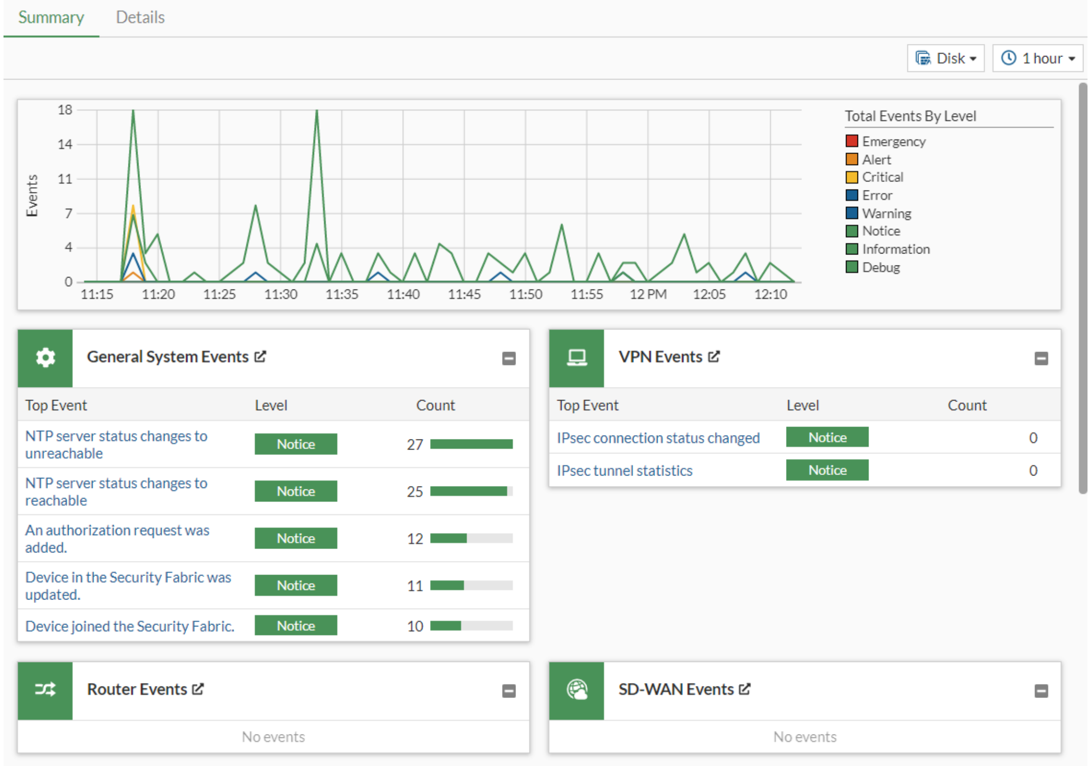
Disk logging and historical FortiView must be enabled for the *Summary* tab to display valid data.

To review system events in the GUI:

1. Go to *Log & Report* > *System Events*. The *Summary* tab opens.
2. On the right-side of the screen, select the time range from the dropdown list.

   The line chart will display all of the system events, and the non-empty event cards will list up to five *Top Event* entries within the time range set.

Data is retrieved from FortiView with the *5 minutes* range updated first. When selecting either the *1 hour* or *24 hours* time range, there may be a delay to update *Top Event* entries.



General System Events

Top Event	Level	Count
NTP server status changes to unreachable	Notice	27
NTP server status changes to reachable	Notice	25
An authorization request was added.	Notice	12
Device in the Security Fabric was updated.	Notice	11
Device joined the Security Fabric.	Notice	10

VPN Events

Top Event	Level	Count
IPsec connection status changed	Notice	0
IPsec tunnel statistics	Notice	0

Router Events

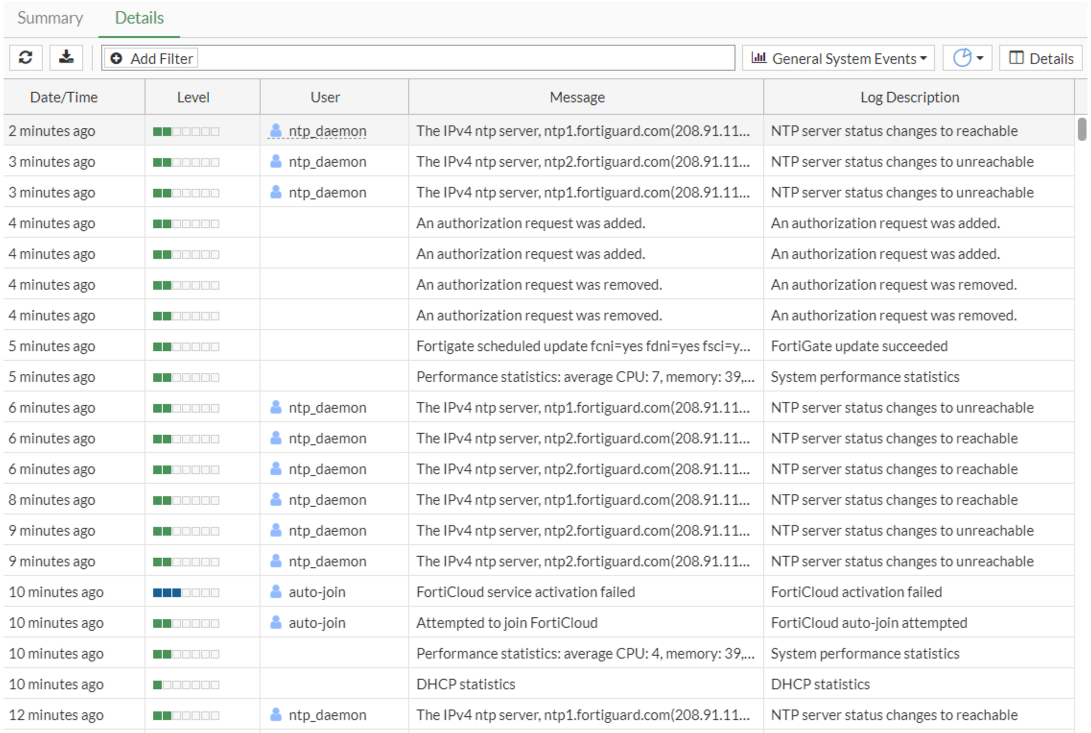
No events

SD-WAN Events

No events

3. Review the details of system events:
   - Click the event card name.

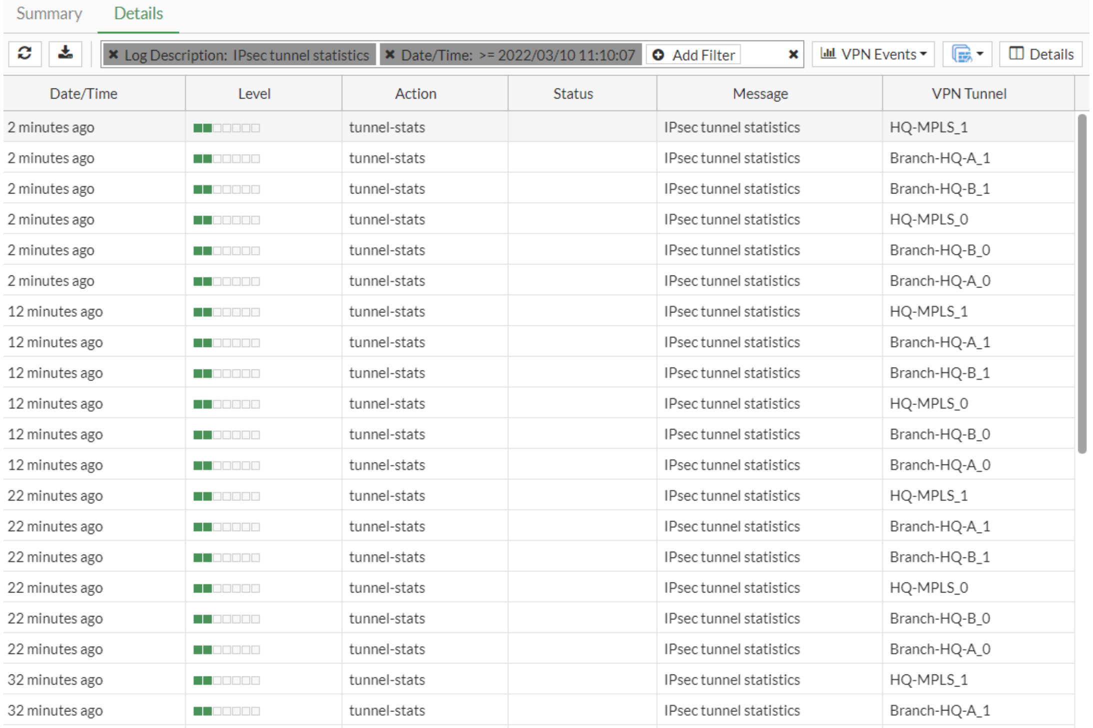
     The *Details* tab displays all event entries for the selected type of event log. The type of event log can be changed in the top-right, dropdown list.



Date/Time	Level	User	Message	Log Description
2 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(208.91.11...	NTP server status changes to reachable
3 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(208.91.11...	NTP server status changes to unreachable
3 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(208.91.11...	NTP server status changes to unreachable
4 minutes ago	■■□□□□		An authorization request was added.	An authorization request was added.
4 minutes ago	■■□□□□		An authorization request was added.	An authorization request was added.
4 minutes ago	■■□□□□		An authorization request was removed.	An authorization request was removed.
4 minutes ago	■■□□□□		An authorization request was removed.	An authorization request was removed.
5 minutes ago	■■□□□□		Fortigate scheduled update fcni=yes fdni=yes fsci=y...	FortiGate update succeeded
5 minutes ago	■■□□□□		Performance statistics: average CPU: 7, memory: 39,...	System performance statistics
6 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(208.91.11...	NTP server status changes to unreachable
6 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(208.91.11...	NTP server status changes to reachable
6 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(208.91.11...	NTP server status changes to reachable
8 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(208.91.11...	NTP server status changes to reachable
9 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(208.91.11...	NTP server status changes to unreachable
9 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(208.91.11...	NTP server status changes to unreachable
10 minutes ago	■■■□□□	auto-join	FortiCloud service activation failed	FortiCloud activation failed
10 minutes ago	■■□□□□	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted
10 minutes ago	■■□□□□		Performance statistics: average CPU: 4, memory: 39,...	System performance statistics
10 minutes ago	■□□□□□		DHCP statistics	DHCP statistics
12 minutes ago	■■□□□□	ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(208.91.11...	NTP server status changes to reachable

- Click a *Top Event* entry in an event card.

  The *Details* tab displays system events with filters for the selected event entry and time range. The type of event log can be changed in the top-right, dropdown list.



Log Description: IPsec tunnel statistics
Date/Time: >= 2022/03/10 11:10:07

Date/Time	Level	Action	Status	Message	VPN Tunnel
2 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	HQ-MPLS_1
2 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-A_1
2 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-B_1
2 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	HQ-MPLS_0
2 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-B_0
2 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-A_0
12 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	HQ-MPLS_1
12 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-A_1
12 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-B_1
12 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	HQ-MPLS_0
12 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-B_0
12 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-A_0
22 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	HQ-MPLS_1
22 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-A_1
22 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-B_1
22 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	HQ-MPLS_0
22 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-B_0
22 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-A_0
32 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	HQ-MPLS_1
32 minutes ago	■■□□□□	tunnel-stats		IPsec tunnel statistics	Branch-HQ-A_1

Up to 100 *Top Event* entries can be listed in the CLI using the `diagnose fortiview result event-log` command.

To list system events in the CLI:

```
# diagnose fortiview result event-log

    data(1646760000-1646846401):
    0). subtype-ha | eventname-HA device interface failed | level-warning | count-1 |
    1). subtype-system | eventname-DHCP statistics | level-information | count-40 |
    2). subtype-system | eventname-Super admin left VDOM | level-information | count-13 |
    3). subtype-system | eventname-Admin performed an action from GUI | level-warning |
count-5 |
    4). subtype-system | eventname-Super admin entered VDOM | level-information | count-4 |
    5). subtype-system | eventname-Global setting changed | level-notice | count-3 |
    6). subtype-system | eventname-Attribute configured | level-information | count-2 |
    7). subtype-system | eventname-Clear active sessions | level-warning | count-2 |
    8). subtype-system | eventname-Disk log rolled | level-notice | count-2 |
    9). subtype-system | eventname-Log rotation requested by FortiCron | level-notice |
count-1 |
    10). subtype-system | eventname-Report generated successfully | level-notice | count-1 |
    11). subtype-system | eventname-Test | level-warning | count-1 |
    12). subtype-system | eventname-VDOM added | level-notice | count-1 |
    13). subtype-user | eventname-Authentication failed | level-notice | count-1 |
    14). subtype-user | eventname-Authentication lockout | level-warning | count-1 |
    15). subtype-user | eventname-FortiGuard override failed | level-warning | count-1 |
```

The data is collected from FortiView for the last 24 hours by default. To specify a specific time range, customize the time filter using the `diagnose fortiview time` command.

To filter the time range of system events in the CLI:

```
# diagnose fortiview time <arg1> <arg2>
```

Where `<arg1>` is the start time in YYYY-MM-DD HH:MM:SS and `<arg2>` is the end time in YYYY-MM-DD HH:MM:SS.

New Security Events log page

The *Log & Report* UTM log subtypes have been combined into the *Security Events* log page. The *Security Events* log page includes:

- A *Summary* tab that displays the five most frequent events for all of the enabled UTM security events.
- A *Details* tab that displays individual, detailed logs for each UTM type.

Clicking on an event in the *Summary* tab will bring users to the *Details* tab with the appropriate filters automatically applied.

Disk logging and historical FortiView must be enabled for the *Summary* tab to display valid data.

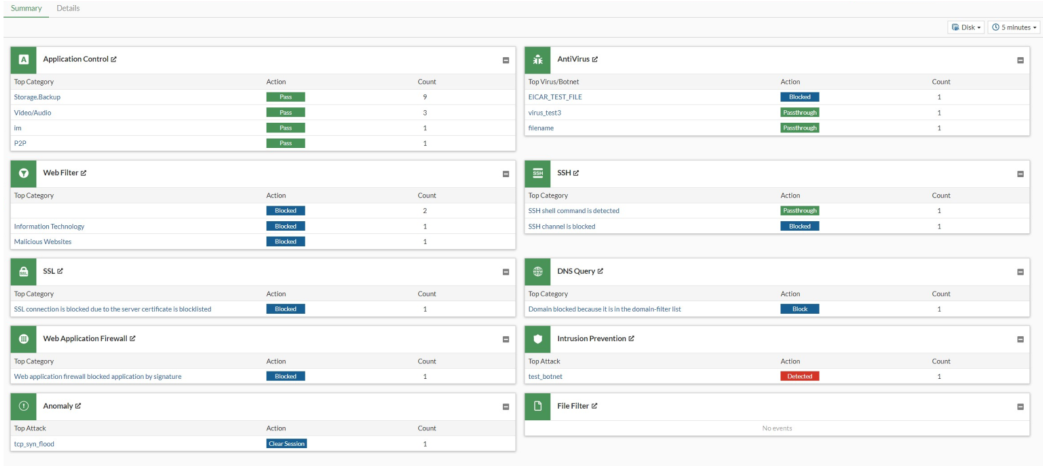
To review security events in the GUI:

1. Go to *Log & Report* > *Security Events*.
   The *Summary* tab displays up to five top events for each enabled, non-empty security event cards.

2. On the right-side of the screen, select the time range from the dropdown list.

   The non-empty security event cards will list up to five top entries within the time range set.

> Data is retrieved from FortiView with the *5 minutes* range updated first. When selecting either the *1 hour* or *24 hours* time range, there may be a delay to update top security event entries.



Application Control

Top Category	Action	Count
Storage.Backup	Pass	9
Video/Audio	Pass	3
im	Pass	1
P2P	Pass	1

AntiVirus

Top Virus/Botnet	Action	Count
EICAR_TEST_FILE	Blocked	1
virus_test3	Passthrough	1
filename	Passthrough	1

Web Filter

Top Category	Action	Count
	Blocked	2
Information Technology	Blocked	1
Malicious Websites	Blocked	1

SSH

Top Category	Action	Count
SSH shell command is detected	Passthrough	1
SSH channel is blocked	Blocked	1

SSL

Top Category	Action	Count
SSL connection is blocked due to the server certificate is blocklisted	Blocked	1

DNS Query

Top Category	Action	Count
Domain blocked because it is in the domain-filter list	Block	1

Web Application Firewall

Top Category	Action	Count
Web application firewall blocked application by signature	Blocked	1

Intrusion Prevention

Top Attack	Action	Count
test_botnet	Detected	1

Anomaly

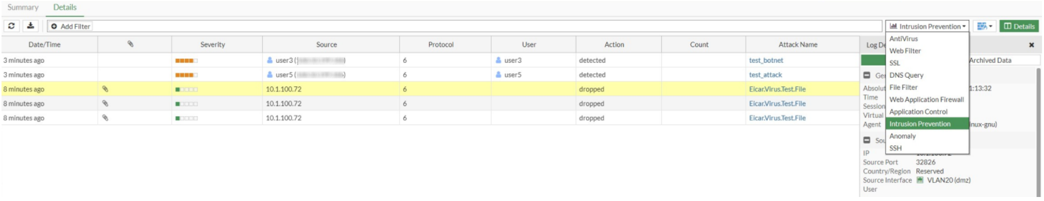
Top Attack	Action	Count
tcp_syn_flood	Clear Session	1

File Filter

No events

3. Review the details of security events:
   - Click the security event card name.

     The *Details* tab displays all event entries for the selected type of security event. The security event type can be changed in the top-right dropdown list.

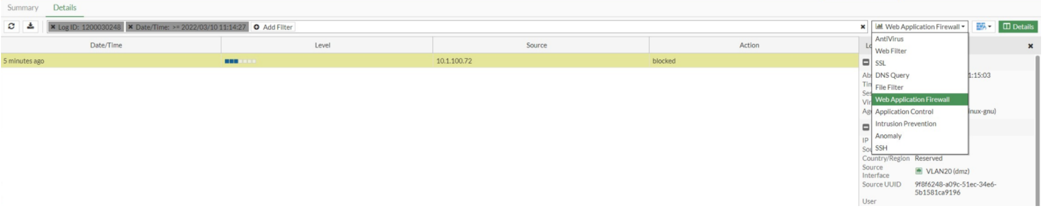


Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
3 minutes ago		■■■■□	user3 ([redacted])	6	user3	detected		test_botnet
3 minutes ago		■■■■□	user5 ([redacted])	6	user5	detected		test_attack
8 minutes ago	📎	■□□□□	10.1.100.72	6		dropped		Eicar.Virus.Test.File
8 minutes ago	📎	■□□□□	10.1.100.72	6		dropped		Eicar.Virus.Test.File
8 minutes ago	📎	■□□□□	10.1.100.72	6		dropped		Eicar.Virus.Test.File

Source Port 32826
Country/Region Reserved
Source Interface VLAN20 (dmz)
User

   - Click a top event entry in a security event card.

     The *Details* tab displays security events with filters for the selected event entry and time filter. The security event type can be changed in the top-right dropdown list.



Log ID: 1200030248
Date/Time: >= 2022/03/10 11:14:27

Date/Time	Level	Source	Action
5 minutes ago	■■■□□□□	10.1.100.72	blocked

Country/Region Reserved
Source Interface VLAN20 (dmz)
Source UUID 9f8f6248-a09c-51ec-34e6-5b1581ca9196
User

Up to 100 top security event entries can be listed in the CLI using the `diagnose fortiview result security-log` command.

To list security events in the CLI:

```
# diagnose fortiview result security-log [<filters>]
```

To list security events in the CLI with no filters applied:

```
# diagnose fortiview result security-log

    data(1646862300-1646948701):
    0). logcat-2 | logcatname-virus | logid-0211008192 | eventname-EICAR_TEST_FILE |
eventname_field-virus | action-blocked | count-1 |
    1). logcat-2 | logcatname-virus | logid-0211008192 | eventname-virus_test3 | eventname_
field-virus | action-passthrough | count-1 |
    2). logcat-2 | logcatname-virus | logid-0212008448 | eventname-filename | eventname_
field-virus | action-passthrough | count-1 |
    3). logcat-3 | logcatname-webfilter | logid-0318012800 | eventname- | eventname_field-
catdesc | action-blocked | count-2 |
    4). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Information
Technology | eventname_field-catdesc | action-blocked | count-1 |
    5). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Malicious Websites |
eventname_field-catdesc | action-blocked | count-1 |
    6). logcat-4 | logcatname-ips | logid-0419016384 | eventname-Eicar.Virus.Test.File |
eventname_field-attack | action-dropped | count-3 |
    7). logcat-4 | logcatname-ips | logid-0422016400 | eventname-test_botnet | eventname_
field-attack | action-detected | count-1 |
    8). logcat-7 | logcatname-anomaly | logid-0720018432 | eventname-tcp_syn_flood |
eventname_field-attack | action-clear_session | count-1 |
    9). logcat-10 | logcatname-app-ctrl | logid-1059028704 | eventname-Storage.Backup |
eventname_field-appcat | action-pass | count-9 |
    10). logcat-10 | logcatname-app-ctrl | logid-1059028704 | eventname-Video/Audio |
eventname_field-appcat | action-pass | count-3 |
    11). logcat-10 | logcatname-app-ctrl | logid-1059028672 | eventname-im | eventname_
field-appcat | action-pass | count-1 |
    12). logcat-10 | logcatname-app-ctrl | logid-1059028704 | eventname-P2P | eventname_
field-appcat | action-pass | count-1 |
    13). logcat-15 | logcatname-dns | logid-1501054400 | eventname-Domain blocked because it
is in the domain-filter list | eventname_field-logid | action-block | count-1 |
    14). logcat-17 | logcatname-ssl | logid-1700062300 | eventname-SSL connection is blocked
due to the server certificate is blocklisted | eventname_field-logid | action-blocked |
count-1 |
    15). logcat-16 | logcatname-ssh | logid-1600061002 | eventname-SSH shell command is
detected | eventname_field-logid | action-passthrough | count-1 |
    16). logcat-16 | logcatname-ssh | logid-1601061010 | eventname-SSH channel is blocked |
eventname_field-logid | action-blocked | count-1 |
    17). logcat-12 | logcatname-waf | logid-1200030248 | eventname-Web application firewall
blocked application by signature | eventname_field-logid | action-blocked | count-1 |
    18). logcat-8 | logcatname-voip | logid-0814044032 | eventname-Logid_44032 | eventname_
field-logid | action-permit | count-1 |
    19). logcat-5 | logcatname-emailfilter | logid-0513020480 | eventname-SPAM notification
| eventname_field-logid | action-blocked | count-1 |
```

To list blocked security events in the CLI:

```
# diagnose fortiview result security-log action=blocked

    data(1646862600-1646949001):
    0). logcat-2 | logcatname-virus | logid-0211008192 | eventname-EICAR_TEST_FILE |
eventname_field-virus | action-blocked | count-1 |
    1). logcat-3 | logcatname-webfilter | logid-0318012800 | eventname- | eventname_field-
catdesc | action-blocked | count-2 |
    2). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Information
Technology | eventname_field-catdesc | action-blocked | count-1 |
    3). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Malicious Websites |
eventname_field-catdesc | action-blocked | count-1 |
    4). logcat-17 | logcatname-ssl | logid-1700062300 | eventname-SSL connection is blocked
due to the server certificate is blocklisted | eventname_field-logid | action-blocked |
count-1 |
    5). logcat-16 | logcatname-ssh | logid-1601061010 | eventname-SSH channel is blocked |
eventname_field-logid | action-blocked | count-1 |
    6). logcat-12 | logcatname-waf | logid-1200030248 | eventname-Web application firewall
blocked application by signature | eventname_field-logid | action-blocked | count-1 |
    7). logcat-5 | logcatname-emailfilter | logid-0513020480 | eventname-SPAM notification |
eventname_field-logid | action-blocked | count-1 |
```

Improve FortiAnalyzer log caching

Reliable logging to FortiAnalyzer is improved to prevent lost logs when the connection between FortiOS and FortiAnalyzer is disrupted. When reliable mode is enabled:

1. Logs are cached in a FortiOS memory queue.
2. FortiOS sends logs to FortiAnalyzer, and FortiAnalyzer uses `seq_no` to track received logs.
3. After FortiOS sends logs to FortiAnalyzer, logs are moved to a confirm queue in FortiOS.
4. FortiOS periodically queries FortiAnalyzer for the latest `seq_no` of the last log received, and clears logs from the confirm queue up to the `seq_no`.
5. If the connection between FortiOS and FortiAnalyzer is disrupted, FortiOS resends the logs in the confirm queue to FortiAnalyzer when the connection is reestablished.

FortiAnalyzer 7.2.0 and later is required.

To enable reliable mode:

```
config log fortianalyzer setting
    set reliable enable
end
```

To view the memory and confirm queues:

1. Verify that log synchronization is enabled for FortiAnalyzer:

```
# diagnose test application fgtlogd 1
vdom-admin=0
mgmt=root

fortilog:
faz: global , enabled
    server=172.16.200.251, realtime=1, ssl=1, state=connected
    server_log_status=Log is allowed.,
    src=, mgmt_name=FGh_Log_root_172.16.200.251, reliable=1, sni_prefix_type=none,
    required_entitlement=none, region=ca-west-1,,
    logsync_enabled:1, logsync_conn_id:65535, seq_no:790
...
```

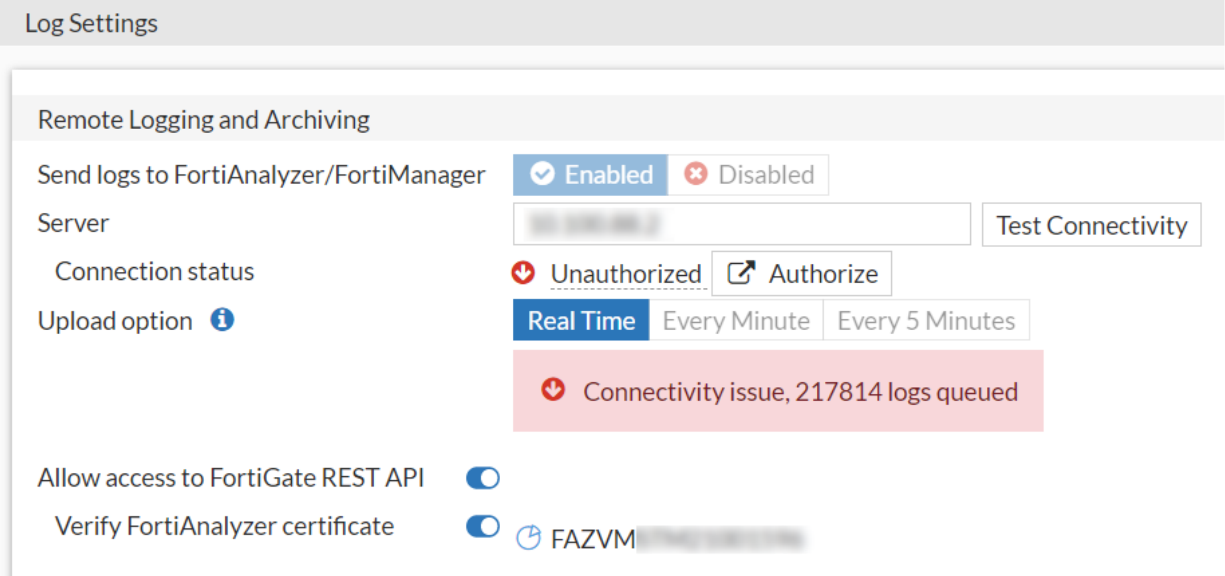
2. When a network disruption disconnects FortiOS from FortiAnalyzer and FortiOS continues to generate logs, the logs are cached in the memory queue.
   - View the number of logs in the cache and queue:

```
# diagnose test application fgtlogd 41

cache maximum: 189516595(180MB) objects: 40 used: 27051(0MB) allocated: 29568(0MB)

VDOM:root
Memory queue for: global-faz
    queue:
        num:9 size:6976(0MB) total size:26068(0MB) max:189516595(180MB) logs:28
Confirm queue for: global-faz
    queue:
        num:29 size:19092(0MB) total size:27051(0MB) max:189516595(180MB) logs:7
```

```
# diagnose test application fgtlogd 30
VDOM:root
Memory queue for: global-faz
        queue:
                num:9 size:6976(0MB) total size:26068(0MB) max:189516595(180MB)
                        type:3, cat=1, log_count=1, seq_no=0, data len=359 size:435
                        type:3, cat=1, log_count=1, seq_no=0, data len=307 size:383
                        ......
                        type:3, cat=0, log_count=4, seq_no=0, data len=1347 size:1423
                        type:3, cat=4, log_count=1, seq_no=0, data len=653 size:729
                'total log count':28,  'total data len':6292

Confirm queue for: global-faz
        queue:
                num:29 size:19092(0MB) total size:26068(0MB) max:189516595(180MB)
                        type:3, cat=1, log_count=1, seq_no=1, data len=290 size:366
                        type:3, cat=1, log_count=1, seq_no=2, data len=233 size:309
                        ......
                        type:3, cat=0, log_count=1, seq_no=28, data len=524 size:600
                        type:3, cat=1, log_count=1, seq_no=29, data len=307 size:383
                'total log count':76,  'total data len':16888
```

   There are nine OFTP items cached to the memory queue, and 29 OFTP items to send from FortiOS to FortiAnalyzer that are waiting for confirmation from FortiAnalyzer.

- Go to *Log & Report* > *Log Settings* to view the queue in the GUI:



Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager: Enabled | Disabled

Server: [redacted] Test Connectivity

Connection status: Unauthorized | Authorize

Upload option: Real Time | Every Minute | Every 5 Minutes

Connectivity issue, 217814 logs queued

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate: FAZVM[redacted]

3. Re-establish the connection between FortiOS and FortiAnalyzer and confirm that the queue has cleared by checking the `seq_no`, which indicates the latest confirmation log from FortiAnalyzer:

```
# diagnose test application fgtlogd 30
VDOM:root
Memory queue for: global-faz
    queue:
        num:0 size:0(0MB) total size:0(0MB) max:189516595(180MB)
        'total log count':0,  'total data len':0

Confirm queue for: global-faz
    queue:
        num:0 size:0(0MB) total size:0(0MB) max:189516595(180MB)
        'total log count':0,  'total data len':0
```

The queue has been cleared, meaning that FortiOS received confirmation from FortiAnalyzer and cleared the confirm queue.

```
# diagnose test application fgtlogd 1
vdom-admin=0
mgmt=root

fortilog:
faz: global , enabled
        server=172.16.200.251, realtime=1, ssl=1, state=connected
        server_log_status=Log is allowed.,
        src=, mgmt_name=FGh_Log_root_172.16.200.251, reliable=1, sni_prefix_type=none,
        required_entitlement=none, region=ca-west-1,
        logsync_enabled:1, logsync_conn_id:65535, seq_no:67
            status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
            SNs: last sn update:38 seconds ago.
                Sn list:
               (FAZ-VMTM21000000,age=38s)
            queue: qlen=0.
```

OFTP items with a `seq_no` lower than 67 have been sent to FortiAnalyzer and were confirmed.

Add FortiAnalyzer Reports page

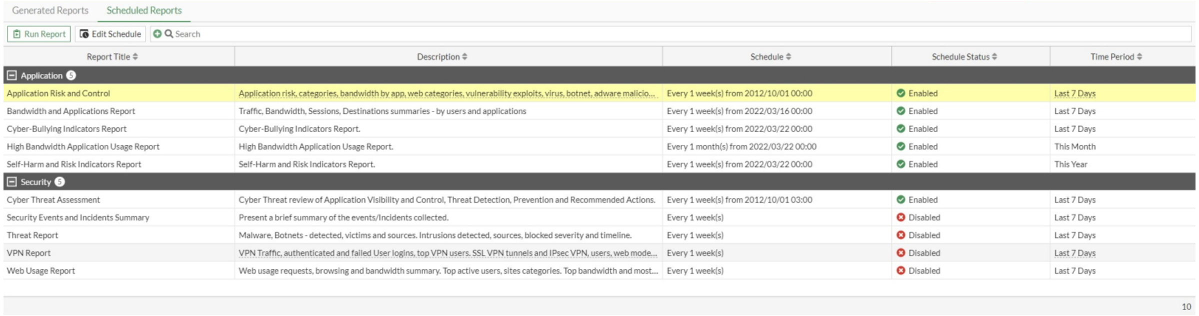
FortiAnalyzer reports can be viewed in the GUI on the *Log & Report > FortiAnalyzer Reports* page. Administrators can generate, delete, and edit report schedules, and view and download generated reports.

FortiAnalyzer must be configured in FortiOS. If the FortiGate is unauthorized on FortiAnalyzer, or the connection to FortiAnalyzer is down, the *FortiAnalyzer Reports* page loads with *No results*.

When the Security Fabric is enabled, only the root FortiGate can run, edit, and delete FortiAnalyzer reports. Downstream FortiGates can only view the generated reports.

To edit a report schedule:

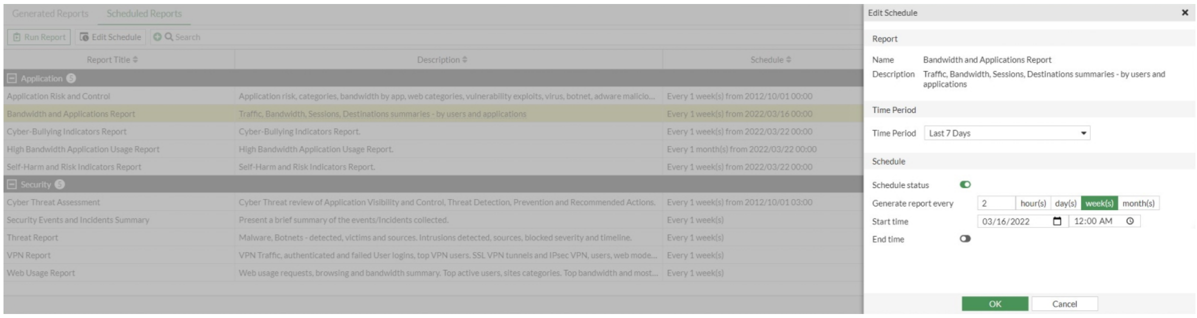
1. Go to *Log & Report > FortiAnalyzer Reports* and select the *Scheduled Reports* tab.



Report Title	Description	Schedule	Schedule Status	Time Period
Application 5				
Application Risk and Control	Application risk, categories, bandwidth by app, web categories, vulnerability exploits, virus, botnet, adware malicio...	Every 1 week(s) from 2012/10/01 00:00	✓ Enabled	Last 7 Days
Bandwidth and Applications Report	Traffic, Bandwidth, Sessions, Destinations summaries - by users and applications	Every 1 week(s) from 2022/03/16 00:00	✓ Enabled	Last 7 Days
Cyber-Bullying Indicators Report	Cyber-Bullying Indicators Report.	Every 1 week(s) from 2022/03/22 00:00	✓ Enabled	Last 7 Days
High Bandwidth Application Usage Report	High Bandwidth Application Usage Report.	Every 1 month(s) from 2022/03/22 00:00	✓ Enabled	This Month
Self-Harm and Risk Indicators Report	Self-Harm and Risk Indicators Report.	Every 1 week(s) from 2022/03/22 00:00	✓ Enabled	This Year
Security 5				
Cyber Threat Assessment	Cyber Threat review of Application Visibility and Control, Threat Detection, Prevention and Recommended Actions.	Every 1 week(s) from 2012/10/01 03:00	✓ Enabled	Last 7 Days
Security Events and Incidents Summary	Present a brief summary of the events/Incidents collected.	Every 1 week(s)	☒ Disabled	Last 7 Days
Threat Report	Malware, Botnets - detected, victims and sources. Intrusions detected, sources, blocked severity and timeline.	Every 1 week(s)	☒ Disabled	Last 7 Days
VPN Report	VPN Traffic, authenticated and failed User logins, top VPN users. SSL VPN tunnels and IPsec VPN, users, web mode...	Every 1 week(s)	☒ Disabled	Last 7 Days
Web Usage Report	Web usage requests, browsing and bandwidth summary. Top active users, sites categories. Top bandwidth and most...	Every 1 week(s)	☒ Disabled	Last 7 Days

10

2. Select a report and click *Edit Schedule*. The *Edit Schedule* pane opens. In this example, the schedule for the Bandwidth and Applications report is changed to run from every week to every two weeks.
3. In the *Schedule* section, set the values for *Generate report every* to *2 week(s)*.



Report

Name: Bandwidth and Applications Report
Description: Traffic, Bandwidth, Sessions, Destinations summaries - by users and applications

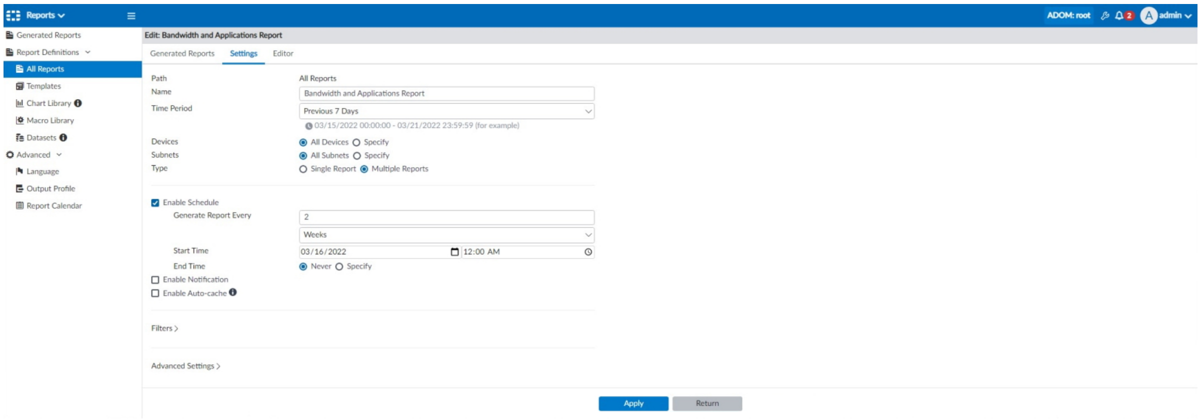
Time Period

Time Period: Last 7 Days

Schedule

Schedule status: ●
Generate report every: 2 week(s)
Start time: 03/16/2022 12:00 AM
End time: ○

4. Click *OK*.
   The schedule is also updated automatically in FortiAnalyzer for the same report (go to *Reports > Report Definitions > All Reports* and edit the report to view the settings).



Edit: Bandwidth and Applications Report

Path: All Reports
Name: Bandwidth and Applications Report
Time Period: Previous 7 Days
03/15/2022 00:00:00 - 03/21/2022 23:59:59 (for example)
Devices: ● All Devices ○ Specify
Subnets: ● All Subnets ○ Specify
Type: ○ Single Report ● Multiple Reports

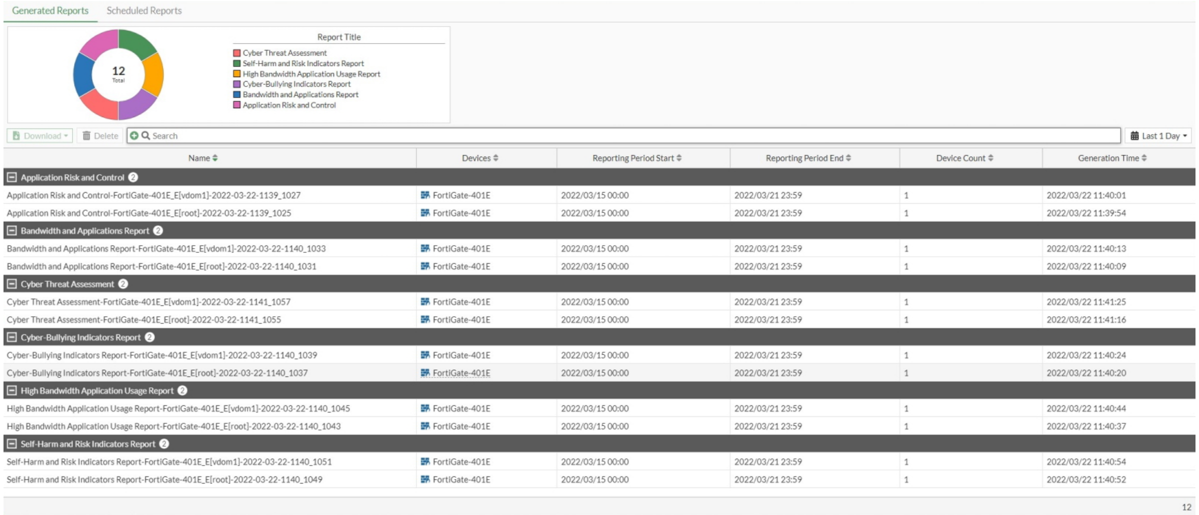
☑ Enable Schedule
Generate Report Every: 2
Weeks
Start Time: 03/16/2022 12:00 AM
End Time: ● Never ○ Specify
☐ Enable Notification
☐ Enable Auto-cache

Filters >

Advanced Settings >

To view and download reports:

1. Go to *Log & Report* > *FortiAnalyzer Reports* and select the *Generated Reports* tab.
   A pie chart displays the total count of FortiAnalyzer reports, categorized by report title. Generated reports are listed below and arranged by title, which includes reports from all VDOMs.



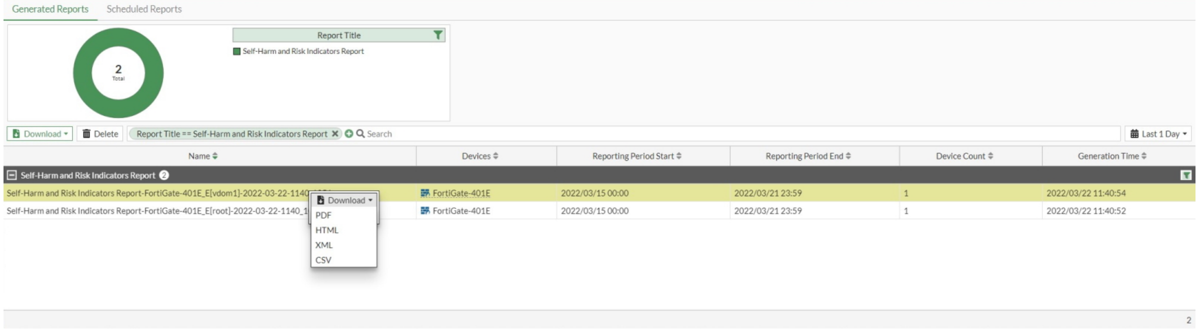
Report Title
- 🟥 Cyber Threat Assessment
- 🟩 Self-Harm and Risk Indicators Report
- 🟧 High Bandwidth Application Usage Report
- 🟪 Cyber-Bullying Indicators Report
- 🟦 Bandwidth and Applications Report
- 🟪 Application Risk and Control

Name	Devices	Reporting Period Start	Reporting Period End	Device Count	Generation Time
Application Risk and Control 2					
Application Risk and Control-FortiGate-401E_E[vdom1]-2022-03-22-1139_1027	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:01
Application Risk and Control-FortiGate-401E_E[root]-2022-03-22-1139_1025	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:39:54
Bandwidth and Applications Report 2					
Bandwidth and Applications Report-FortiGate-401E_E[vdom1]-2022-03-22-1140_1033	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:13
Bandwidth and Applications Report-FortiGate-401E_E[root]-2022-03-22-1140_1031	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:09
Cyber Threat Assessment 2					
Cyber Threat Assessment-FortiGate-401E_E[vdom1]-2022-03-22-1141_1057	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:41:25
Cyber Threat Assessment-FortiGate-401E_E[root]-2022-03-22-1141_1055	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:41:16
Cyber-Bullying Indicators Report 2					
Cyber-Bullying Indicators Report-FortiGate-401E_E[vdom1]-2022-03-22-1140_1039	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:24
Cyber-Bullying Indicators Report-FortiGate-401E_E[root]-2022-03-22-1140_1037	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:20
High Bandwidth Application Usage Report 2					
High Bandwidth Application Usage Report-FortiGate-401E_E[vdom1]-2022-03-22-1140_1045	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:44
High Bandwidth Application Usage Report-FortiGate-401E_E[root]-2022-03-22-1140_1043	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:37
Self-Harm and Risk Indicators Report 2					
Self-Harm and Risk Indicators Report-FortiGate-401E_E[vdom1]-2022-03-22-1140_1051	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:54
Self-Harm and Risk Indicators Report-FortiGate-401E_E[root]-2022-03-22-1140_1049	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:52

12

   In this example, the Self-Harm and Risk Indicators reports are filtered, and the report for vdom1 is downloaded.

2. In the pie chart, click the green segment to filter the Self-Harm and Risk Indicators reports.
3. In the filtered results, select the report for vdom1. Right-click and select *Download*.



Report Title
- 🟩 Self-Harm and Risk Indicators Report

Report Title == Self-Harm and Risk Indicators Report

Name	Devices	Reporting Period Start	Reporting Period End	Device Count	Generation Time
Self-Harm and Risk Indicators Report 2					
Self-Harm and Risk Indicators Report-FortiGate-401E_E[vdom1]-2022-03-22-1140	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:54
Self-Harm and Risk Indicators Report-FortiGate-401E_E[root]-2022-03-22-1140_1	FortiGate-401E	2022/03/15 00:00	2022/03/21 23:59	1	2022/03/22 11:40:52

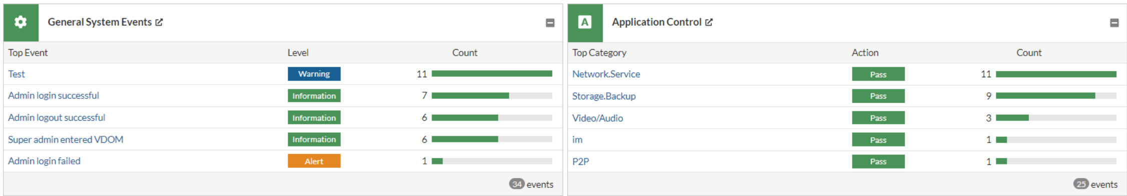
2

4. Select a file format. The report is saved to the default download location.

Summary tabs on System Events and Security Events log pages - 7.2.1

The *Summary* tabs on the *Log & Report* > *System Events* and *Log & Report* > *Security Events* pages are enabled on devices that support disk logging and have historical FortiView enabled. They include the following enhancements:

- Event list footers show a count of the events that relate to the type.



General System Events

Top Event	Level	Count
Test	Warning	11
Admin login successful	Information	7
Admin logout successful	Information	6
Super admin entered VDOM	Information	6
Admin login failed	Alert	1

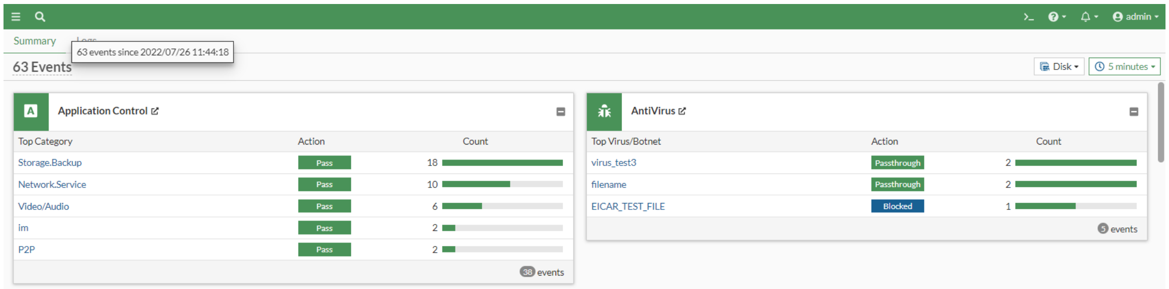
34 events

Application Control

Top Category	Action	Count
Network.Service	Pass	11
Storage.Backup	Pass	9
Video/Audio	Pass	3
im	Pass	1
P2P	Pass	1

25 events

- A count of the total events is shown at the top of the *Summary*. Hovering over the count shows the number of events with a time stamp.



63 events since 2022/07/26 11:44:18

63 Events

Application Control

Top Category	Action	Count
Storage.Backup	Pass	18
Network.Service	Pass	10
Video/Audio	Pass	6
im	Pass	2
P2P	Pass	2

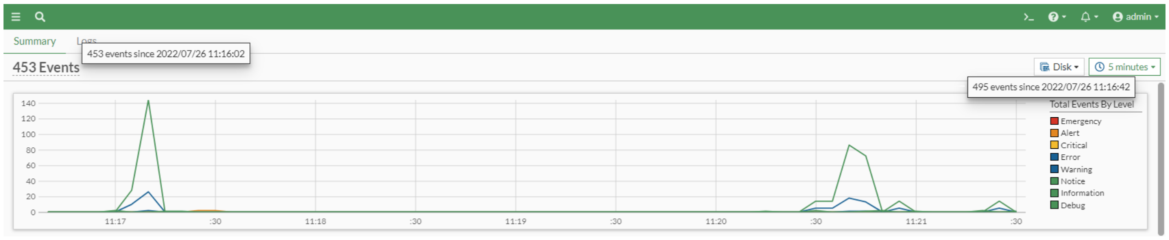
38 events

AntiVirus

Top Virus/Botnet	Action	Count
virus_test3	Passthrough	2
filename	Passthrough	2
EICAR_TEST_FILE	Blocked	1

5 events

- On *System Events* > *Summary*, hovering over the *Total Events By Level* shows the shows the number of events with a time stamp.

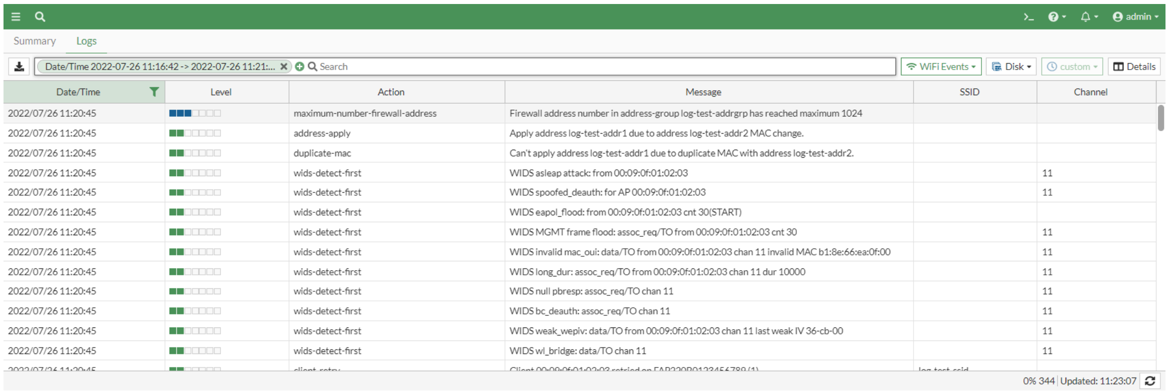


453 events since 2022/07/26 11:16:02

453 Events

495 events since 2022/07/26 11:16:42

- Clicking on any event type title opens the *Logs* page for that event type filtered by the selected time span. For example, on the *System Events* > *Summary* page, clicking *WiFi Events* opens the following page:



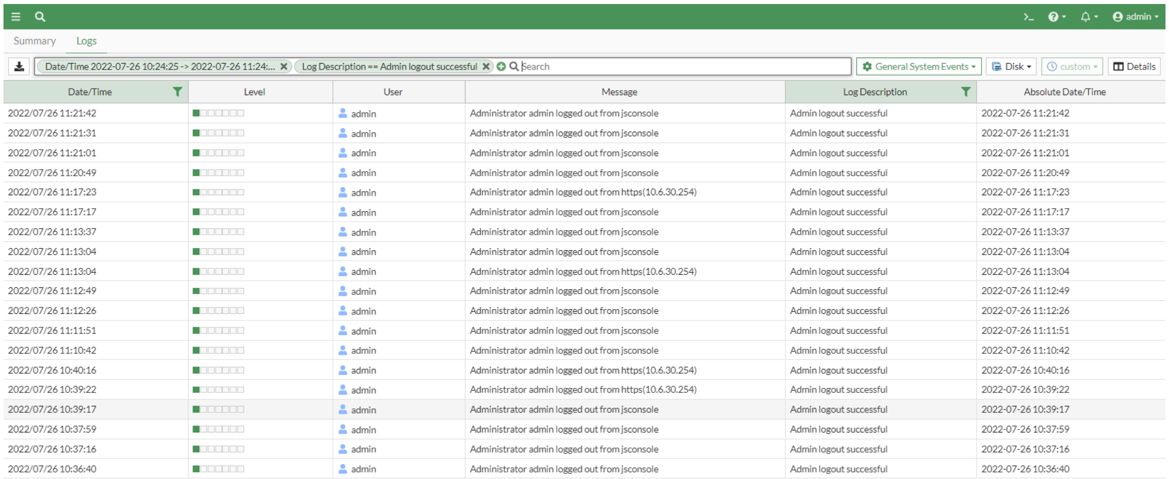
Date/Time 2022-07-26 11:16:42 -> 2022-07-26 11:21:...

Date/Time	Level	Action	Message	SSID	Channel
2022/07/26 11:20:45	■■■□□□□	maximum-number-firewall-address	Firewall address number in address-group log-test-addrgrp has reached maximum 1024		
2022/07/26 11:20:45	■■□□□□□	address-apply	Apply address log-test-addr1 due to address log-test-addr2 MAC change.		
2022/07/26 11:20:45	■■□□□□□	duplicate-mac	Can't apply address log-test-addr1 due to duplicate MAC with address log-test-addr2.		
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS asleap attack: from 00:09:0f:01:02:03		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS spoofed_deauth: for AP 00:09:0f:01:02:03		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS eapol_flood: from 00:09:0f:01:02:03 cnt 30(START)		
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS MGMT frame flood: assoc_req/TO from 00:09:0f:01:02:03 cnt 30		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS invalid mac_oui: data/TO from 00:09:0f:01:02:03 chan 11 invalid MAC b1:8e:66:ea:0f:00		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS long_dur: assoc_req/TO from 00:09:0f:01:02:03 chan 11 dur 10000		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS null pbresp: assoc_req/TO chan 11		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS bc_deauth: assoc_req/TO chan 11		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS weak_wepiv: data/TO from 00:09:0f:01:02:03 chan 11 last weak IV 36-cb-00		11
2022/07/26 11:20:45	■■□□□□□	wids-detect-first	WIDS wl_bridge: data/TO chan 11		11
2022/07/26 11:20:45	■■□□□□□	client-retry	Client 00:09:0f:01:02:03 retried on FAP220B0123456789 (1)	log-test-ssid	

0% 344 Updated: 11:23:07

- Clicking on any event entry opens the Logs page for that event type filtered by the selected time span and log description.

For example, on the *System Events* > *Summary* page in the *General System Events* box, clicking *Admin logout successful* opens the following page:



Date/Time 2022-07-26 10:24:25 -> 2022-07-26 11:24:... ✕ Log Description == Admin logout successful ✕ Search

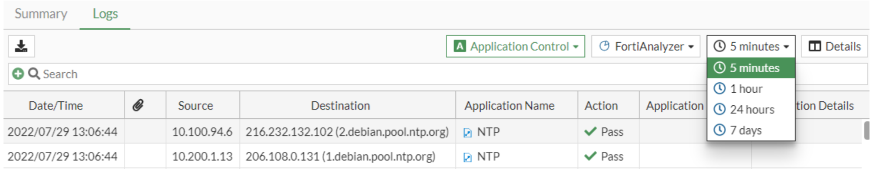
Date/Time	Level	User	Message	Log Description	Absolute Date/Time
2022/07/26 11:21:42	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:21:42
2022/07/26 11:21:31	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:21:31
2022/07/26 11:21:01	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:21:01
2022/07/26 11:20:49	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:20:49
2022/07/26 11:17:23	■□□□□□□	admin	Administrator admin logged out from https(10.6.30.254)	Admin logout successful	2022-07-26 11:17:23
2022/07/26 11:17:17	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:17:17
2022/07/26 11:13:37	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:13:37
2022/07/26 11:13:04	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:13:04
2022/07/26 11:13:04	■□□□□□□	admin	Administrator admin logged out from https(10.6.30.254)	Admin logout successful	2022-07-26 11:13:04
2022/07/26 11:12:49	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:12:49
2022/07/26 11:12:26	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:12:26
2022/07/26 11:11:51	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:11:51
2022/07/26 11:10:42	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 11:10:42
2022/07/26 10:40:16	■□□□□□□	admin	Administrator admin logged out from https(10.6.30.254)	Admin logout successful	2022-07-26 10:40:16
2022/07/26 10:39:22	■□□□□□□	admin	Administrator admin logged out from https(10.6.30.254)	Admin logout successful	2022-07-26 10:39:22
2022/07/26 10:39:17	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 10:39:17
2022/07/26 10:37:59	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 10:37:59
2022/07/26 10:37:16	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 10:37:16
2022/07/26 10:36:40	■□□□□□□	admin	Administrator admin logged out from jsconsole	Admin logout successful	2022-07-26 10:36:40

Add time frame selector to log viewer pages - 7.2.1

Logs can be filtered by date and time in the *Log & Report* > *System Events* and *Security Events* pages. The log viewer can be filtered with a custom range or with specific time frames.

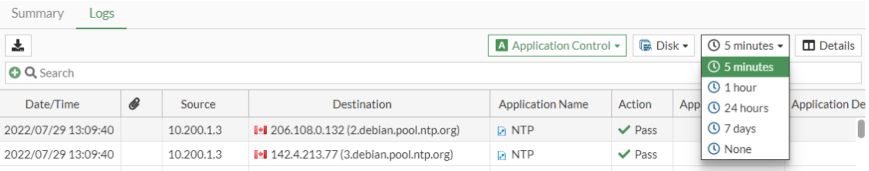
The time frame available is dependent on the source:

- Logs sourced from FortiAnalyzer, FortiGate Cloud, and FortiAnalyzer Cloud have the same time frame options as FortiView (*5 minutes*, *1 hour*, *24 hours*, or *7 days*).



Date/Time	📎	Source	Destination	Application Name	Action	Application	tion Details
2022/07/29 13:06:44		10.100.94.6	216.232.132.102 (2.debian.pool.ntp.org)	NTP	✓ Pass		
2022/07/29 13:06:44		10.200.1.13	206.108.0.131 (1.debian.pool.ntp.org)	NTP	✓ Pass		

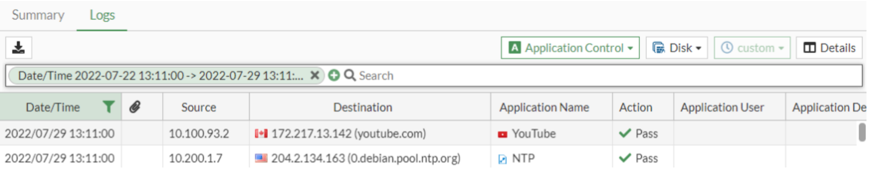
- Logs sourced from the Disk have the time frame options of *5 minutes*, *1 hour*, *24 hours*, *7 days*, or *None*.



Date/Time	📎	Source	Destination	Application Name	Action	App	Application De
2022/07/29 13:09:40		10.200.1.3	206.108.0.132 (2.debian.pool.ntp.org)	NTP	✓ Pass		
2022/07/29 13:09:40		10.200.1.3	142.4.213.77 (3.debian.pool.ntp.org)	NTP	✓ Pass		

- Logs source from Memory do not have time frame filters.

A custom time frame can be applied using the *Date/Time* filter. If the *Date/Time* filter is applied, the time frame will be disabled and set to *custom*.

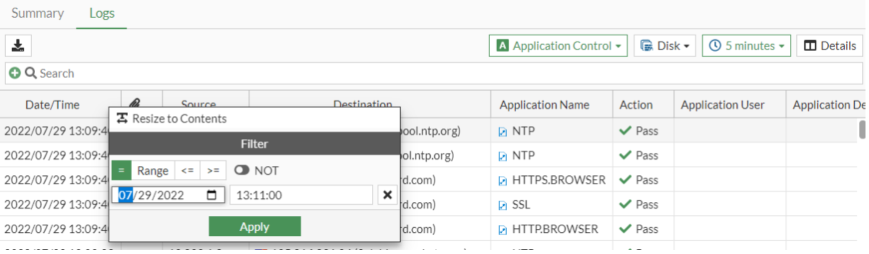


Date/Time 2022-07-22 13:11:00 -> 2022-07-29 13:11:... ✕ Search

Date/Time	📎	Source	Destination	Application Name	Action	Application User	Application De
2022/07/29 13:11:00		10.100.93.2	172.217.13.142 (youtube.com)	YouTube	✓ Pass		
2022/07/29 13:11:00		10.200.1.7	204.2.134.163 (0.debian.pool.ntp.org)	NTP	✓ Pass		

To set a custom time frame range:

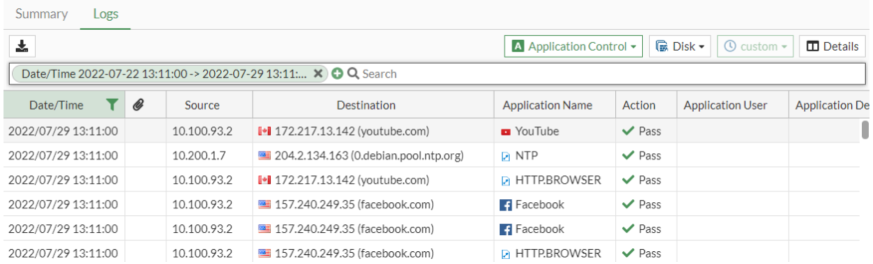
1. Go to *Log & Report > Security Events*.
2. Select the *Logs* tab.
3. Select the *Date/Time* filter. The *Filter* dialog is displayed.



07/29/2022 13:11:00

Date/Time		Source	Destination	Application Name	Action	Application User	Application De
2022/07/29 13:09:4			pool.ntp.org)	NTP	✓ Pass		
2022/07/29 13:09:4			ol.ntp.org)	NTP	✓ Pass		
2022/07/29 13:09:4			d.com)	HTTPS.BROWSER	✓ Pass		
2022/07/29 13:09:4			d.com)	SSL	✓ Pass		
2022/07/29 13:09:4			d.com)	HTTP.BROWSER	✓ Pass		

4. Select *Range*.
5. Click the *From* calendar icon and select a date.
6. Enter a time in the *From* field using the form `HH:MM:SS`.
7. Click the *To* calendar icon and select a date.
8. Enter a time in the *To* time using the form `HH:MM:SS`.
9. Click *Apply*. The logs that match the set time frame are displayed and the time frame is set to *custom*.



Date/Time 2022-07-22 13:11:00 -> 2022-07-29 13:11:...

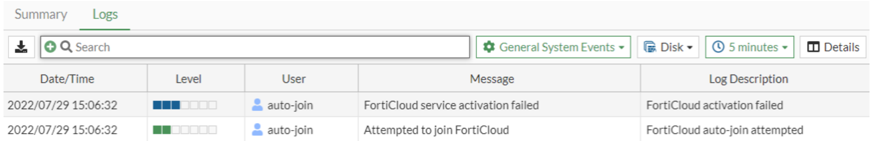
Date/Time		Source	Destination	Application Name	Action	Application User	Application De
2022/07/29 13:11:00		10.100.93.2	172.217.13.142 (youtube.com)	YouTube	✓ Pass		
2022/07/29 13:11:00		10.200.1.7	204.2.134.163 (0.debian.pool.ntp.org)	NTP	✓ Pass		
2022/07/29 13:11:00		10.100.93.2	172.217.13.142 (youtube.com)	HTTP.BROWSER	✓ Pass		
2022/07/29 13:11:00		10.100.93.2	157.240.249.35 (facebook.com)	Facebook	✓ Pass		
2022/07/29 13:11:00		10.100.93.2	157.240.249.35 (facebook.com)	Facebook	✓ Pass		
2022/07/29 13:11:00		10.100.93.2	157.240.249.35 (facebook.com)	HTTP.BROWSER	✓ Pass		

If a custom time frame filter is set, a new time frame cannot be selected until the first filter is removed. Click the `X` in the search bar or select *Remove* in the *Filter* dialog to remove the filter.

Updating log viewer and log filters - 7.2.1

The *Log & Report > System Events* and *Security Events* pages have been updated:

- The *Details* tab has been renamed the *Logs* tab.

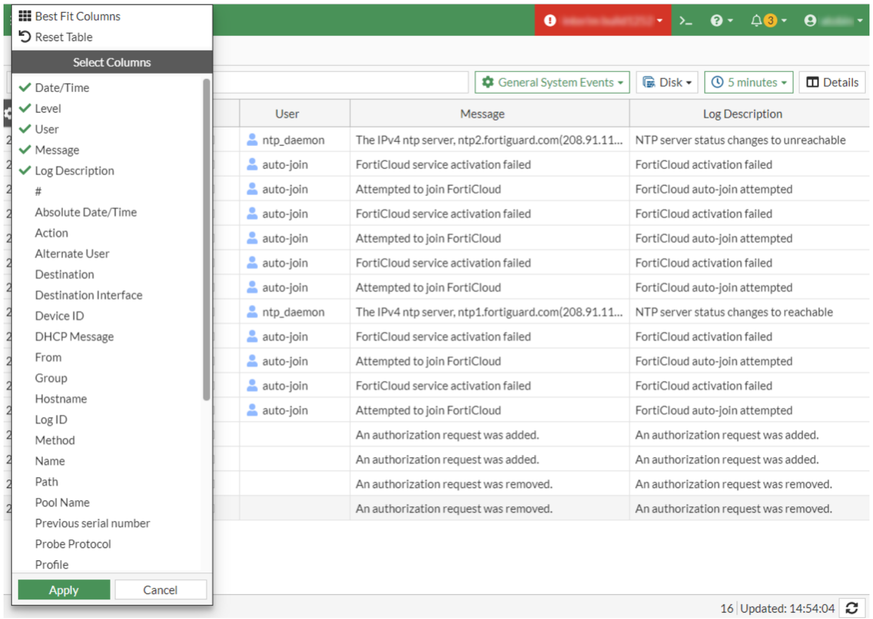


Date/Time	Level	User	Message	Log Description
2022/07/29 15:06:32	■■■□□□□	auto-join	FortiCloud service activation failed	FortiCloud activation failed
2022/07/29 15:06:32	■■□□□□□	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted

- Filters used in the log viewer have been updated to adjust the log filters and the *Log Details* pane.
- Time frame settings for each *Log & Report* pages are independent of each other.

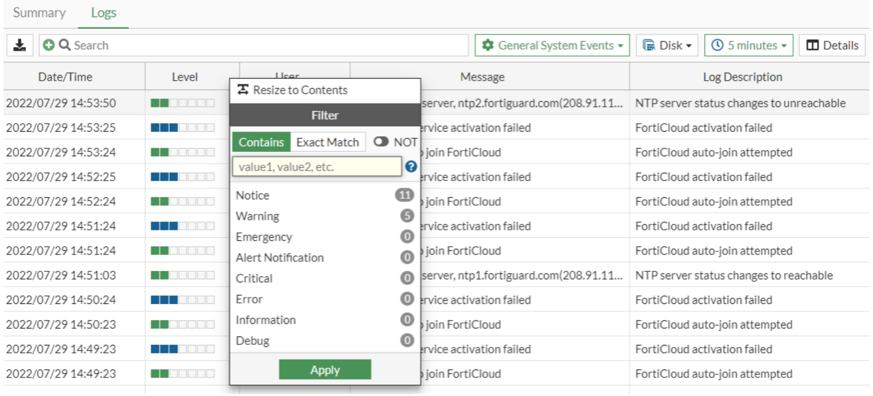
To view filtered log information:

1. Go to *Log & Report* > *System Events*.
2. Select the *Logs* tab.
3. Hover over the leftmost column and click the gear icon. A list of column you can filter is displayed.



User	Message	Log Description
ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(208.91.11...	NTP server status changes to unreachable
auto-join	FortiCloud service activation failed	FortiCloud activation failed
auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted
auto-join	FortiCloud service activation failed	FortiCloud activation failed
auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted
auto-join	FortiCloud service activation failed	FortiCloud activation failed
auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted
ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(208.91.11...	NTP server status changes to reachable
auto-join	FortiCloud service activation failed	FortiCloud activation failed
auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted
auto-join	FortiCloud service activation failed	FortiCloud activation failed
auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted
	An authorization request was added.	An authorization request was added.
	An authorization request was added.	An authorization request was added.
	An authorization request was removed.	An authorization request was removed.
	An authorization request was removed.	An authorization request was removed.

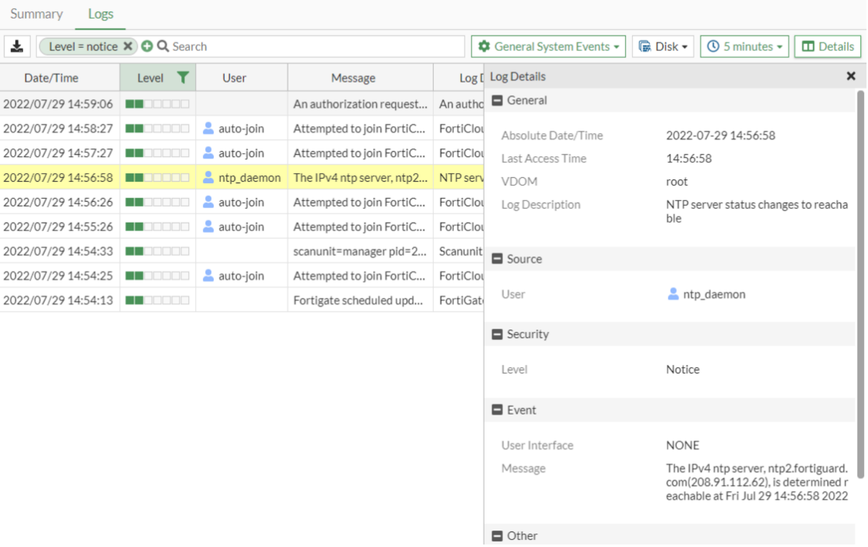
4. Select the columns you want displayed.
5. Click *Apply*. The selected columns are displayed.
6. Click the filter icon for the column you want to filter. The filter dialog is displayed and the number of logs for each filter type is listed.



Date/Time	Level	User	Message	Log Description
2022/07/29 14:53:50			server, ntp2.fortiguard.com(208.91.11...	NTP server status changes to unreachable
2022/07/29 14:53:25			rvice activation failed	FortiCloud activation failed
2022/07/29 14:53:24			join FortiCloud	FortiCloud auto-join attempted
2022/07/29 14:52:25			rvice activation failed	FortiCloud activation failed
2022/07/29 14:52:24			join FortiCloud	FortiCloud auto-join attempted
2022/07/29 14:51:24			rvice activation failed	FortiCloud activation failed
2022/07/29 14:51:24			join FortiCloud	FortiCloud auto-join attempted
2022/07/29 14:51:03			server, ntp1.fortiguard.com(208.91.11...	NTP server status changes to reachable
2022/07/29 14:50:24			rvice activation failed	FortiCloud activation failed
2022/07/29 14:50:23			join FortiCloud	FortiCloud auto-join attempted
2022/07/29 14:49:23			rvice activation failed	FortiCloud activation failed
2022/07/29 14:49:23			join FortiCloud	FortiCloud auto-join attempted

7. Select the filters you want and click *Apply*. The logs that match the set filters are displayed and the filter is listed in the search bar.
8. Select the log you want to see more information on.

9. Click *Details*. The *Log Details* pane is displayed.



Date/Time	Level	User	Message	Log [
2022/07/29 14:59:06	■■□□□□□		An authorization request...	An autho
2022/07/29 14:58:27	■■□□□□□	auto-join	Attempted to join FortiC...	FortiClou
2022/07/29 14:57:27	■■□□□□□	auto-join	Attempted to join FortiC...	FortiClou
2022/07/29 14:56:58	■■□□□□□	ntp_daemon	The IPv4 ntp server, ntp2...	NTP serv
2022/07/29 14:56:26	■■□□□□□	auto-join	Attempted to join FortiC...	FortiClou
2022/07/29 14:55:26	■■□□□□□	auto-join	Attempted to join FortiC...	FortiClou
2022/07/29 14:54:33	■■□□□□□		scanunit=manager pid=2...	Scanunit
2022/07/29 14:54:25	■■□□□□□	auto-join	Attempted to join FortiC...	FortiClou
2022/07/29 14:54:13	■■□□□□□		Fortigate scheduled upd...	FortiGat

Log Details

General

Absolute Date/Time	2022-07-29 14:56:58
Last Access Time	14:56:58
VDOM	root
Log Description	NTP server status changes to reachable

Source

User	ntp_daemon

Security

Level	Notice

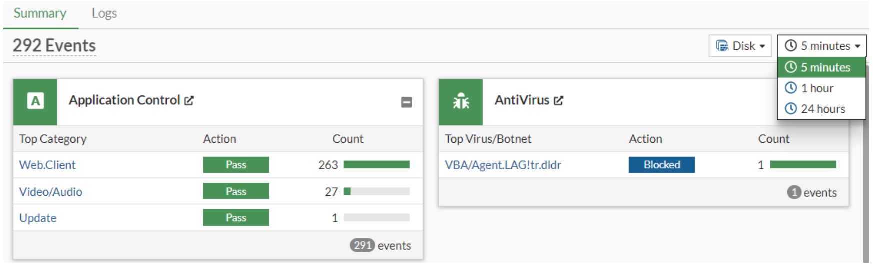
Event

User Interface	NONE
Message	The IPv4 ntp server, ntp2.fortiguard.com(208.91.112.62), is determined reachable at Fri Jul 29 14:56:58 2022

Other

To compare time frames on the Summary tab:

1. Go to *Log & Report > Security Events*.
2. Click the time frame in the top right. The available time frames are listed.



292 Events

Application Control

Top Category	Action	Count
Web.Client	Pass	263
Video/Audio	Pass	27
Update	Pass	1

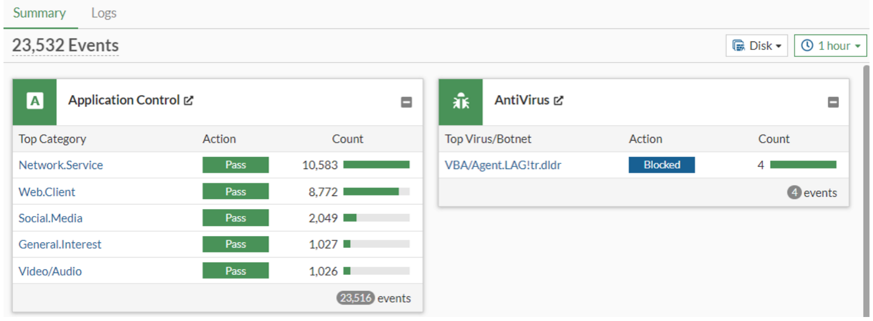
291 events

AntiVirus

Top Virus/Botnet	Action	Count
VBA/Agent.LAG!tr.dldr	Blocked	1

1 events

3. Select a new time frame. The *Top Events* will adjust for the new time frame.



23,532 Events

Application Control

Top Category	Action	Count
Network.Service	Pass	10,583
Web.Client	Pass	8,772
Social.Media	Pass	2,049
General.Interest	Pass	1,027
Video/Audio	Pass	1,026

23,516 events

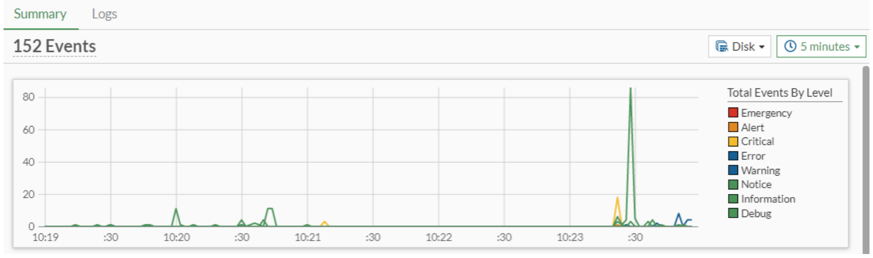
AntiVirus

Top Virus/Botnet	Action	Count
VBA/Agent.LAG!tr.dldr	Blocked	4

4 events

4. Go to *Log & Report > System Events*. The system events will display the time frame set for the *System Events* page

in the top right.



The time frame will be different than that of the *Security Events* page unless it is changed in the *System Events* page to match.

Consolidate log reports and settings into dedicated Reports and Log Settings pages - 7.2.4

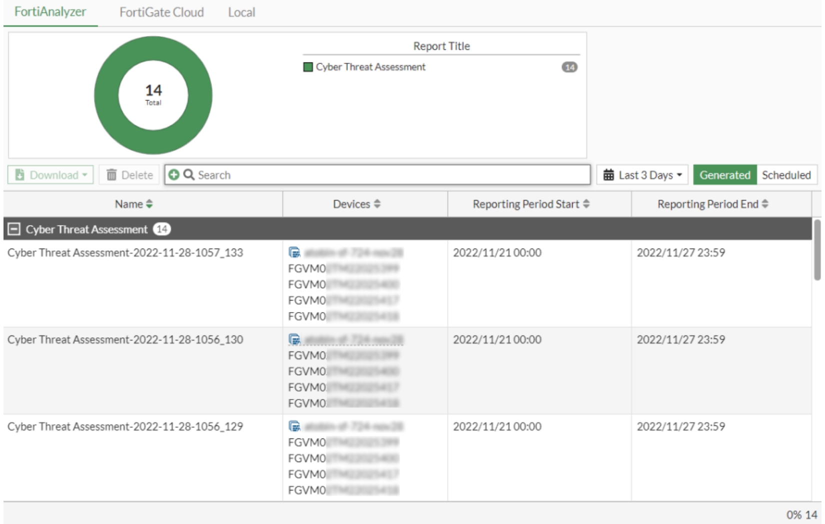
This information is also available in the FortiOS 7.2 Administration Guide:

- Reports page
- Log settings and targets

Log & Report reports and settings pages have been consolidated into two dedicated pages:

- The FortiAnalyzer, FortiGate Cloud, and local report pages have been consolidated into the *Log & Report* > *Reports* page.
- Global, local, and threat weight settings have been consolidated into the *Log & Report* > *Log Settings* page.

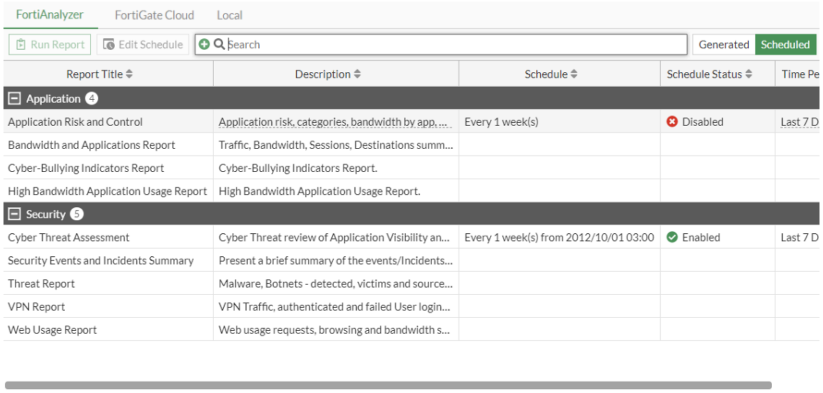
The *Log & Report* > *Reports* page includes tabs dedicated to *FortiAnalyzer*, *FortiGate Cloud*, and *Local* reports.



Name	Devices	Reporting Period Start	Reporting Period End
Cyber Threat Assessment 14			
Cyber Threat Assessment-2022-11-28-1057_133	[redacted] FGVM0[redacted] FGVM0[redacted] FGVM0[redacted] FGVM0[redacted]	2022/11/21 00:00	2022/11/27 23:59
Cyber Threat Assessment-2022-11-28-1056_130	[redacted] FGVM0[redacted] FGVM0[redacted] FGVM0[redacted] FGVM0[redacted]	2022/11/21 00:00	2022/11/27 23:59
Cyber Threat Assessment-2022-11-28-1056_129	[redacted] FGVM0[redacted] FGVM0[redacted] FGVM0[redacted] FGVM0[redacted]	2022/11/21 00:00	2022/11/27 23:59

0% 14

The *FortiAnalyzer Reports* > *Generated Reports* and *Scheduled Reports* tabs have been merged into the *FortiAnalyzer* tab of *Log & Report* > *Reports*. The *Generated* report data is displayed by default. You can review scheduled report data by selecting *Scheduled*.

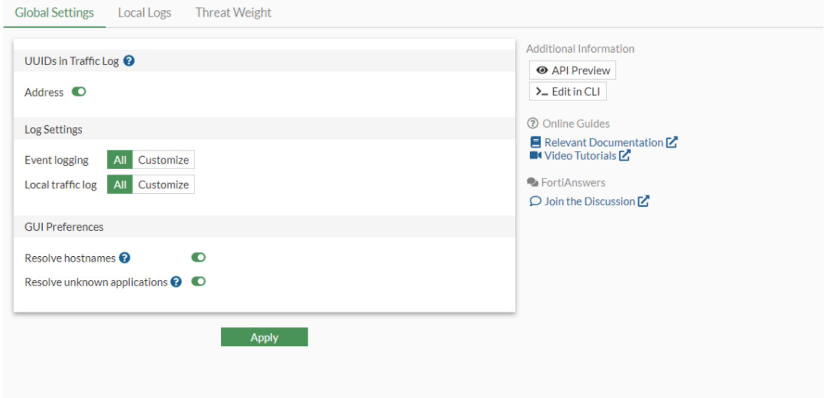


FortiAnalyzer | FortiGate Cloud | Local

Run Report | Edit Schedule | Search | Generated | Scheduled

Report Title	Description	Schedule	Schedule Status	Time Pe
Application 4				
Application Risk and Control	Application risk, categories, bandwidth by app, ...	Every 1 week(s)	Disabled	Last 7 D
Bandwidth and Applications Report	Traffic, Bandwidth, Sessions, Destinations summ...			
Cyber-Bullying Indicators Report	Cyber-Bullying Indicators Report.			
High Bandwidth Application Usage Report	High Bandwidth Application Usage Report.			
Security 5				
Cyber Threat Assessment	Cyber Threat review of Application Visibility an...	Every 1 week(s) from 2012/10/01 03:00	Enabled	Last 7 D
Security Events and Incidents Summary	Present a brief summary of the events/Incidents...			
Threat Report	Malware, Botnets - detected, victims and source...			
VPN Report	VPN Traffic, authenticated and failed User login...			
Web Usage Report	Web usage requests, browsing and bandwidth s...			

The *Log & Report* > *Log Settings* page organizes settings into the *Global Settings*, *Local Logs*, and *Threat Weight* tabs.



Global Settings | Local Logs | Threat Weight

UUIDs in Traffic Log

Address

Log Settings

Event logging: All | Customize

Local traffic log: All | Customize

GUI Preferences

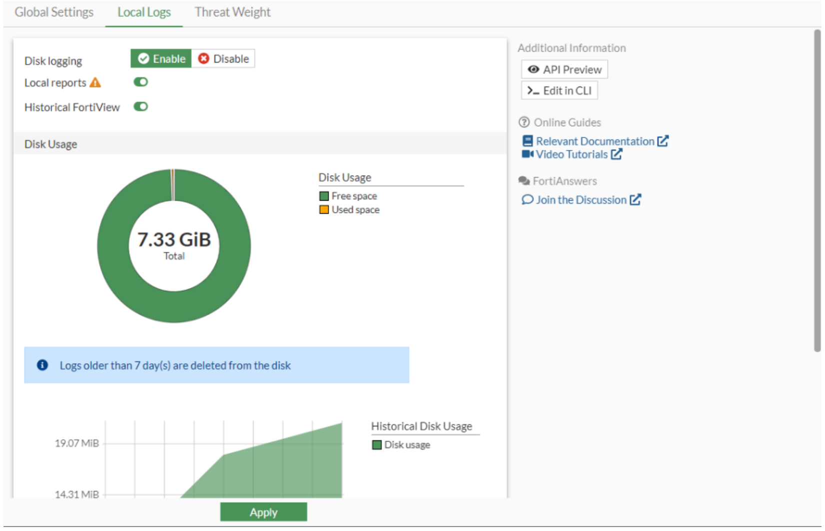
Resolve hostnames

Resolve unknown applications

Apply

Enabling local reports

The *Local Reports* toggle has been removed from the *System* > *Feature Visibility* page. *Local reports* can now only be enabled from the *Local Logs* tab of *Log & Report* > *Log Settings*.



Global Settings | Local Logs | Threat Weight

Disk logging: Enable | Disable

Local reports

Historical FortiView

Disk Usage

Logs older than 7 day(s) are deleted from the disk

Apply

Local reports are only displayed in the GUI if CSF is disabled.

Add Logs Sent Daily chart for remote logging sources - 7.2.4

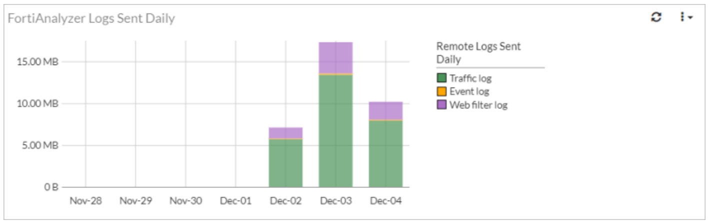
This information is also available in the FortiOS 7.2 Administration Guide:

- Viewing logs sent for remote logging source
- Logs Sent daily chart for remote logging sources

The *Logs Sent Daily* chart for remote logging sources (FortiAnalyzer, FortiGate Cloud, and FortiAnalyzer Cloud) has been added to the *Logging & Analytics* Fabric connector card within the *Security Fabric > Fabric Connectors* page, and to the *Dashboard* as a widget for a selected remote logging source.

To add the Logs Sent widget:

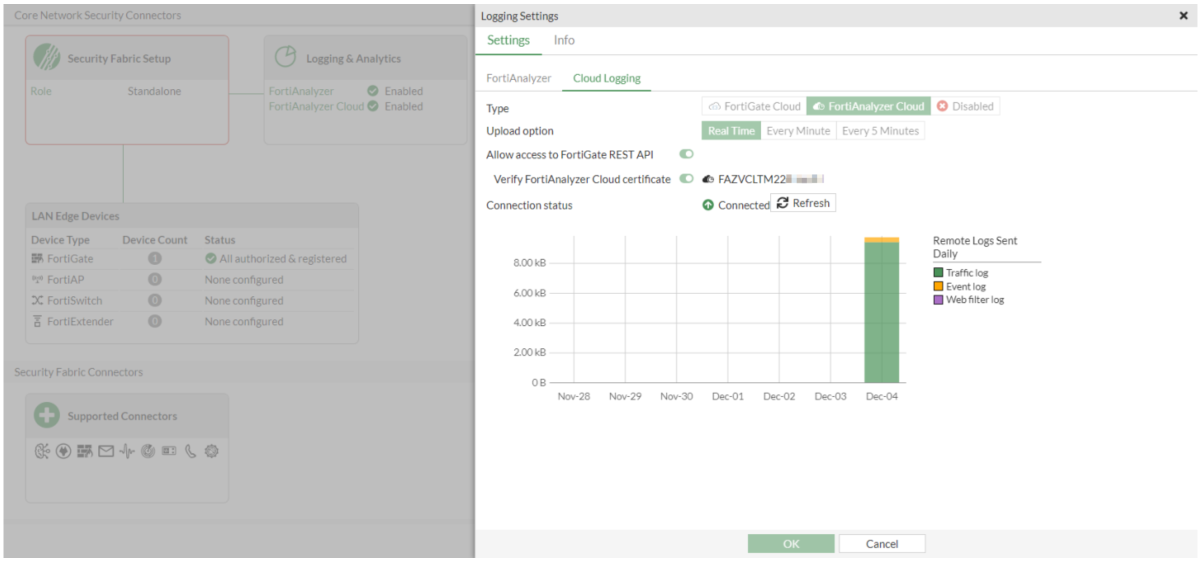
1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *Resource Usage* section, click the + beside *Logs Sent*.
3. Select a *Logging Source* (*FortiAnalyzer*, *FortiGate Cloud*, or *FortiAnalyzer Cloud*). *FortiAnalyzer* is used in this example.
4. Click *Add Widget* and click *Close*. The *FortiAnalyzer Logs Sent Daily* widget is displayed in the dashboard.



To view the chart on the Fabric Connectors page:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Logging & Analytics* Fabric connector card.

   The *Logging Settings* pane is displayed.
2. In the *Settings* tab, click either *FortiAnalyzer* or *Cloud Logging* to view the *Remote Logs Sent Daily* chart. *FortiAnalyzer Cloud* is used in this example.



Logging Settings

Settings | Info

FortiAnalyzer | Cloud Logging

Type: FortiAnalyzer Cloud

Upload option: Real Time

Allow access to FortiGate REST API: enabled

Verify FortiAnalyzer Cloud certificate: enabled — FAZVCLTM22

Connection status: Connected

3. Click *OK* to close the pane.

Cloud

This section includes information about cloud-related new features:

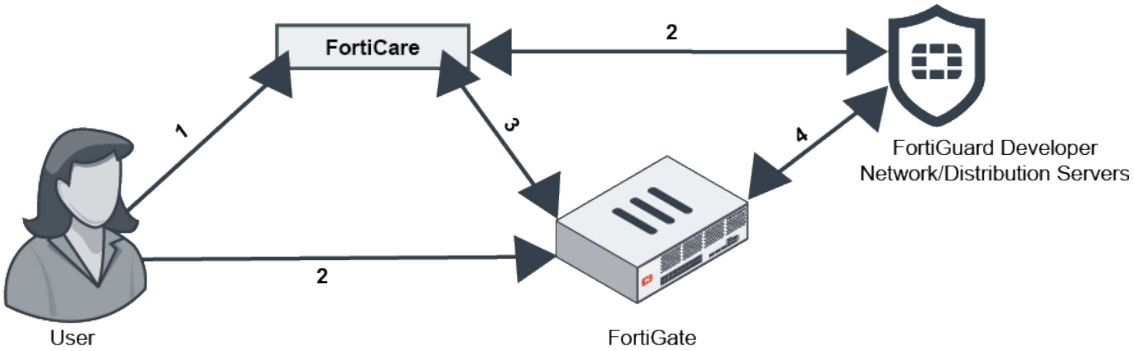
Public and private cloud

This section includes information about public and private cloud-related new features:

Allow grace period for FortiFlex to begin passing traffic upon activation

This enhancement allows for a two-hour grace period for FortiFlex to begin passing traffic upon retrieving the license from FortiCare without VM entitlement verification from FortiGuard Distribution Servers (FDS). In the past, after retrieving the license from FortiCare, traffic was not allowed to pass until the license entitlement was verified with FDS. Since FDS must communicate with FortiCare to retrieve license and entitlement updates, this delayed the entitlement check from the FortiGate. Such delays negatively impacted autoscaling and on-demand instances.

The following shows the topology for this enhancement. The topology shows two step 2s because they happen concurrently.



The topology illustrates the following process:

1. The user generates the FortiFlex license.
2. FDS pulls the registration data from FortiCare, updates the FortiGuard Developer Network (FDN) database, and pushes updates to other systems. The user immediately registers the FortiFlex token on the FortiGate.
3. The FortiGate reaches FortiCare to obtain the license. The grace period immediately starts, and the FortiFlex can pass traffic.
4. The FortiGate synchronizes entitlement from FDS. The FortiGate license becomes valid.

The following scenarios illustrate how the grace period works in production.

Scenario 1

In this scenario, the FortiGate-VM can reach FDS and FortiCare. The FortiGate-VM activates a newly generated FortiFlex license token before FDS synchronizes the license information from FortiCare. The FortiGate-VM is granted the two-hour license grace period.

1. Create a FortiGate-VM with an evaluation license. The following shows the `get system status` output at this point:
   ```
   Version: FortiGate-VM64 v7.2.0,build1115,220218 (interim)
   Serial-Number: FGVMEVVEWEABZJ10
   ```
2. Generate a new FortiFlex license on FortiCare and activate the FortiFlex license token in FortiOS immediately:
   ```
   FGT-TEMP68 # exec vm-license AC6A134D807CDA4B75F8
   This operation will reboot the system !
   Do you want to continue? (y/n)y
   ```
3. The FortiGate-VM sets the VM license status as `Grace Period` before it can validate the license with FDS. The following shows the `get system status` output at this point:

   ```
   Version: FortiGate-VM64 v7.2.0,build1115,220218 (interim)
   ...
   Serial-Number: FGVMMLTM22000386
   License Status: Grace Period
   License Expiration Date: 2022-08-03
   VM Resources: 1 CPU/4 allowed, 2007 MB RAM
   Log hard disk: Available
   ```

   The following shows the `diagnose debug vm-print-license` output at this point:

   ```
   SerialNumber: FGVMMLTM22000386
   CreateDate: Fri Feb 18 16:30:02 2022
   ```

```
License expires: Wed Aug 3 00:00:00 2022
Default Contract:
FMWR:6:20220218:20220803,ENHN:20:20220218:20220803,COMP:20:20220218:20220803,AVDB:6
:20220218:20220803,NIDS:6:20220218:20220803,FURL:6:20220218:20220803,SPAM:6:2022021
8:20220803,VMLS:6:20220218:20220803:4
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: ML (21)
CPU: 4 (subscription:4)
MEM: 2147483647
VDOM license:
  permanent: 1
  subscription: 0
Grace period: 119 min 34 sec
```

The following shows the `diagnose hardware sysinfo vm full` output at this point:

```
UUID: 4213ad10566d26bf8128bcce13ee457c
valid: 1
status: 6
code: 400
warn: 0
copy: 0
received: 4294939603
warning: 4294939603
recv: 202202181631
dup:
```

4. **FDS synchronizes the license information from FortiCare. The followwing shows the output at this point:**

```
Version: FortiGate-VM64 v7.2.0,build1115,220218 (interim)
...
Serial-Number: FGVMMLTM22000386
License Status: Valid
License Expiration Date: 2022-08-03
VM Resources: 1 CPU/4 allowed, 2007 MB RAM
Max number of virtual domains: 1
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
```

The following shows the `diagnose debug vm-print-license` output at this point:

```
SerialNumber: FGVMMLTM22000386
CreateDate: Fri Feb 18 16:30:02 2022
License expires: Wed Aug 3 00:00:00 2022
Default Contract:
FMWR:6:20220218:20220803,ENHN:20:20220218:20220803,COMP:20:20220218:20220803,AVDB:6
:20220218:20220803,NIDS:6:20220218:20220803,FURL:6:20220218:20220803,SPAM:6:2022021
8:20220803,VMLS:6:20220218:20220803:4
```

```
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: ML (21)
CPU: 4 (subscription:4)
MEM: 2147483647
VDOM license:
  permanent: 1
  subscription: 0
```

The following shows the `diagnose hardware sysinfo vm full` output at this point:

```
UUID: 4213ad10566d26bf8128bcce13ee457c
valid: 1
status: 1
code: 200
warn: 0
copy: 0
received: 4294939603
warning: 4294939603
recv: 202202181631
dup:
```

5. You can check the license logs using the following commands:

```
execute log filter category event
execute log filter field service license
execute log display
3 logs found.
3 logs returned.

1: date=2022-02-18 time=08:31:30 eventtime=1645201890437418122 tz="-0800"
logid="0100022804" type="event" subtype="system" level="critical" vd="root"
logdesc="License status changed" service="license" sn="FGVMMLTM22000386"
status="VALID" msg="License status changed to VALID"

2: date=2022-02-18 time=08:30:39 eventtime=1645201838290517060 tz="-0800"
logid="0100022804" type="event" subtype="system" level="critical" vd="root"
logdesc="License status changed" service="license" sn="FGVMMLTM22000386"
status="VALID" msg="License is in grace period"

3: date=2022-02-18 time=08:26:27 eventtime=1645201586895849932 tz="-0800"
logid="0100022804" type="event" subtype="system" level="critical" vd="root"
logdesc="License status changed" service="license" sn="FGVMEVVEWEABZJ10"
status="VALID" msg="License status changed to VALID"
```

Scenario 2

In this scenario, the FortiGate-VM cannot reach FDS but can reach FortiCare. When the FortiGate-VM receives the license file from FortiCare with the token, the two-hour grace period begins.

This scenario is unlikely to happen in production. If a FortiGate-VM can reach FortiCare, it can also likely reach FDS. This scenario illustrates what occurs if the two-hour grace period passes without communication with FDS.

The following shows the license logs in this scenario during the two-hour grace period:

```
2: date=2022-02-17 time=22:57:43 eventtime=1645167462076672946 tz="-0800" logid="0100022804"
     type="event" subtype="system" level="critical" vd="root" logdesc="License status
     changed" service="license" sn="FGVMMLTM123123" status="VALID" msg="License is in grace
     period"
```

The following shows the license logs in this scenario after the two-hour grace period has passed and the FortiGate-VM still cannot reach FDN, and the license status changes to invalid:

```
1: date=2022-02-18 time=00:57:45 eventtime=1645174666108212880 tz="-0800" logid="0100022804"
     type="event" subtype="system" level="critical" vd="root" logdesc="License status
     changed" service="license" sn="FGVMMLTM22000351" status="INVALID" msg="License status
     changed to INVALID"
```

The following shows the output from `diagnose sys vd list | grep index` after the two-hour grace period has passed and the FortiGate-VM still cannot reach FDN, and the license status changes to invalid:

```
name=root/root index=0 disabled fib_ver=22 rpdb_ver=0 use=144 rt_num=26 asym_rt=0 sip_
     helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vsys_ha/vsys_ha index=1 enabled fib_ver=5 rpdb_ver=1 use=75 rt_num=0 asym_rt=0 sip_
     helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vsys_fgfm/vsys_fgfm index=2 enabled fib_ver=4 rpdb_ver=0 use=72 rt_num=0 asym_rt=0 sip_
     helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
```

Azure new instance type support

FortiOS 7.2.0 adds support for new Azure instance types as follows:

- DV4 and DsV4-series
- Dav4 and Dasv4-series
- Dv5 and Dsv5-series
- Dasv5 and Dadsv5-series

The DV4 and DsV4-series contain support for Intel Xeon (Ice Lake [2020] and Cascade Lake [2018]) for general purpose workloads. The DsV4 series has the option for premium storage:

Instance type	vCPU	Max NIC	Recommended BYOL license
DV4 series			
Standard_D2_v4	2	2	FG-VM02 or FG-VM02v
Standard_D4_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32_v4	32	8	FG-VM32 or FG-VM32v
DsV4 series			
Standard_D2s_v4	2	2	FG-VM02 or FG-VM02v

Instance type	vCPU	Max NIC	Recommended BYOL license
Standard_D4s_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8s_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16s_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32s_v4	32	8	FG-VM32 or FG-VM32v

The Dav4 and Dasv4-series contain support for second generation AMD EPYC 7452 (Rome 2019) for production/multithreaded workloads. The DaSV4 series has the option for premium storage:

Instance type	vCPU	Max NIC	Recommended BYOL license
DaV4 series			
Standard_D2a_v4	2	2	FG-VM02 or FG-VM02v
Standard_D4a_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8a_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16a_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32a_v4	32	8	FG-VM32 or FG-VM32v
DasV4 series			
Standard_D2as_v4	2	2	FG-VM02 or FG-VM02v
Standard_D4as_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8as_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16as_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32as_v4	32	8	FG-VM32 or FG-VM32v

The Dv5 and Dsv5-series contain support exclusively for Intel Xeon (Ice Lake [2020]) for general purpose workloads. A premium storage tier is available on Dsv5:

Instance type	vCPU	Max NIC	Recommended BYOL license
DV5 series			
Standard_D2_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32_v5	32	8	FG-VM32 or FG-VM32v

Instance type	vCPU	Max NIC	Recommended BYOL license
DsV5 Series			
Standard_D2s_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4s_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8s_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16s_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32s_v5	32	8	FG-VM32 or FG-VM32v

The Dasv5 and Dadsv5-series contain support for third generation AMD EPYC 7763v (Milan 2021) for production/multithreaded workloads:

Instance type	vCPU	Max NIC	Recommended BYOL license
DasV5 Series			
Standard_D2as_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4as_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8as_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16as_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32as_v5	32	8	FG-VM32 or FG-VM32v
DadsV5 Series			
Standard_D2ads_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4ads_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8ads_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16ads_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32ads_v5	32	8	FG-VM32 or FG-VM32v

OCI X7 and X9 instance shapes

FortiOS 7.2.0 adds support for new OCI instance shapes as follows:

AMD

Instance shape	OCPU	Memory (RAM) in GB
VM.Standard.E3.Flex	1-64	1-1024 GB
VM.Standard.E4.Flex	1-64	1-1024 GB

Intel

Instance shape	OCPU	Memory (RAM) in GB
VM.Standard.3.Flex	1-32	1-512 GB

GCP DPDK support

You can now enable DPDK on FortiGate-VMs deployed on the Google Cloud Platform (GCP). DPDK allows improved network performance.

The following example enables DPDK on a FortiGate-VM deployed on GCP, passes UDP and TCP traffic with an antivirus (AV)/IPS/application firewall policy enabled, then checks the engine and vNP statistics.

To enable DPDK on a FortiGate-VM deployed on GCP:

1. In the FortiOS CLI, enable DPDK, reboot, then check the DPDK status:

```
config dpdk global
(global) # set status enable
(global) # get
status               : enable
interface            :
multiqueue           : disable
sleep-on-idle        : disable
elasticbuffer        : disable
per-session-accounting: traffic-log-only
ipsec-offload        : disable
hugepage-percentage : 30
mbufpool-percentage : 25

(global) # set interface port1 port2 port3 port4
(global) # set multiqueue enable
(global) # set sleep-on-idle enable
(global) # set elasticbuffer enable
(global) # end
status, interface change will trigger system reboot and will take effect after the
reboot.
Enabling DPDK will adjust Tx/Rx ring size to max allowable value by PMD for the
best performance.
Do you want to continue? (y/n)y

config dpdk global
    set status enable
    set interface "port1" "port2" "port3" "port4"
    set multiqueue enable
    set sleep-on-idle enable
    set elasticbuffer enable
    set per-session-accounting traffic-log-only
    set ipsec-offload disable
    set hugepage-percentage 30
    set mbufpool-percentage 25
end
```

2. Check early initialization logs:

```
diagnose dpdk log show early-init
-----------------------------------------------------------------
    DPDK early initialization starts at 2022-03-23 04:58:00(UTC)
-----------------------------------------------------------------
Content of DPDK configuration:(Use cmdb configuration)

    config dpdk global
        set status enable
        set interface "port1" "port2" "port3" "port4"
        set multiqueue enable
        set sleep-on-idle enable
        set elasticbuffer enable
        set per-session-accounting traffic-log-only
        set ipsec-offload disable
        set hugepage-percentage 30
        set mbufpool-percentage 25
    end
    config dpdk cpus
        set rx-cpus "all"
        set vnp-cpus "all"
        set ips-cpus "all"
        set tx-cpus "all"
    end

Parse config success!

Check CPU definitions 'rx-cpus'
Check CPU definitions 'vnp-cpus'
Check CPU definitions 'ips-cpus'
Check CPU definitions 'tx-cpus'
Check CPU definitions 'isolated-cpus'
Check CPUs success!

Huge page allocation done

Ports enabled for DPDK:
    port1
    port2
    port3
    port4
Port name to device name mapping:
    port1: eth0
    port2: eth1
    port3: eth2
    port4: eth3
    port5: eth4
    port6: eth5
    port7: eth6
    port8: eth7
    port9: eth8
    port10: eth9
    port11: eth10
    port12: eth11
    port13: eth12
    port14: eth13
    port15: eth14
    port16: eth15
    port17: eth16
    port18: eth17
    port19: eth18
    port20: eth19
    port21: eth20
    port22: eth21
    port23: eth22
    port24: eth23

Start enabling DPDK kernel driver for port 'port1'...
Getting PCI device info for eth0...
reading pci dev /sys/class/net/eth0
link path: ../../devices/pci0000:00/0000:00:04.0/virtio1/net/eth0
Device info of eth0:
    dev_name: eth0
    macaddr: 42:01:0a:00:00:0f
    pci_vendor: 0x1af4
    pci_device: 0x1000
    pci_id: 0000:00:04.0
    pci_domain: 0
    pci_bus: 0
    pci_devid: 4
    pci_function: 0
    guid: n/a
Unbinding device eth0 from kernel driver...
Device eth0 unbind from kernel driver successful
Binding device eth0 to DPDK driver...
Device eth0 bind to DPDK driver successful
Creating DPDK kernel driver for device eth0...
Add VNP dev: eth0 PCI: 0000:00:04.0, Succeeded
DPDK kernel driver for eth0 successfully created
DPDK kernel driver enabled for port 'port1' (device name 'eth0')

Start enabling DPDK kernel driver for port 'port2'...
```

```
Getting PCI device info for eth1...
reading pci dev /sys/class/net/eth1
link path: ../../devices/pci0000:00/0000:00:05.0/virtio2/net/eth1
Device info of eth1:
    dev_name: eth1
    macaddr: 42:01:0a:00:01:0f
    pci_vendor: 0x1af4
    pci_device: 0x1000
    pci_id: 0000:00:05.0
    pci_domain: 0
    pci_bus: 0
    pci_devid: 5
    pci_function: 0
    guid: n/a
Unbinding device eth1 from kernel driver...
Device eth1 unbind from kernel driver successful
Binding device eth1 to DPDK driver...
Device eth1 bind to DPDK driver successful
Creating DPDK kernel driver for device eth1...
Add VNP dev: eth1 PCI: 0000:00:05.0, Succeeded
DPDK kernel driver for eth1 successfully created
DPDK kernel driver enabled for port 'port2' (device name 'eth1')

Start enabling DPDK kernel driver for port 'port3'...
Getting PCI device info for eth2...
reading pci dev /sys/class/net/eth2
link path: ../../devices/pci0000:00/0000:00:06.0/virtio3/net/eth2
Device info of eth2:
    dev_name: eth2
    macaddr: 42:01:0a:00:02:0f
    pci_vendor: 0x1af4
    pci_device: 0x1000
    pci_id: 0000:00:06.0
    pci_domain: 0
    pci_bus: 0
    pci_devid: 6
    pci_function: 0
    guid: n/a
Unbinding device eth2 from kernel driver...
Device eth2 unbind from kernel driver successful
Binding device eth2 to DPDK driver...
Device eth2 bind to DPDK driver successful
Creating DPDK kernel driver for device eth2...
Add VNP dev: eth2 PCI: 0000:00:06.0, Succeeded
DPDK kernel driver for eth2 successfully created
DPDK kernel driver enabled for port 'port3' (device name 'eth2')

Start enabling DPDK kernel driver for port 'port4'...
```

```
Getting PCI device info for eth3...
reading pci dev /sys/class/net/eth3
link path: ../../devices/pci0000:00/0000:00:07.0/virtio4/net/eth3
Device info of eth3:
    dev_name: eth3
    macaddr: 42:01:0a:00:03:0f
    pci_vendor: 0x1af4
    pci_device: 0x1000
    pci_id: 0000:00:07.0
    pci_domain: 0
    pci_bus: 0
    pci_devid: 7
    pci_function: 0
    guid: n/a
Unbinding device eth3 from kernel driver...
Device eth3 unbind from kernel driver successful
Binding device eth3 to DPDK driver...
Device eth3 bind to DPDK driver successful
Creating DPDK kernel driver for device eth3...
Add VNP dev: eth3 PCI: 0000:00:07.0, Succeeded
DPDK kernel driver for eth3 successfully created
DPDK kernel driver enabled for port 'port4' (device name 'eth3')
Bind ports success!

mknod for uio0 (254, 0) done.
mknod for uio1 (254, 1) done.
mknod for uio2 (254, 2) done.
mknod for uio3 (254, 3) done.
Make UIO nodes success!

#--------------EAL INIT----------------
#--------------------------------------

#--------------------------------------
# port  oid     dev_name       pci_id
#--------------------------------------
     0    0         eth0 0000:00:04.0
     1    1         eth1 0000:00:05.0
     2    2         eth2 0000:00:06.0
     3    3         eth3 0000:00:07.0
#--------------------------------------
DPDK sanity test passed
```

3. Pass UDP and TCP traffic with AV/IPS/application firewall policy enabled, then check engine and vNP statistics:

```
diagnose dpdk statistics show engine

----------------------------------------------------------------------------
FortiOS DPDK Helper Engine Stats
----------------------------------------------------------------------------
```

```
                                     Total         Engine  0         Engine  1
   Engine  2         Engine  3
CPU ID:                                                    0                 1
           2                 3

---------- DPDK RX Stage -------------------------------------------------------
dpdkrx_rx_pkts:                    2610346             87916           2521121
           5              1304
dpdkrx_tx_pkts:                    2610346             87916           2521121
           5              1304
dpdkrx_drop_pkts:                        0                 0                 0
           0                 0
dpdkrx_drop_multiseg_pkts:               0                 0                 0
           0                 0
dpdkrx_elstcbuf_in_num:                  0                 0                 0
           0                 0
dpdkrx_elstcbuf_out_num:                 0                 0                 0
           0                 0
dpdkrx_monitor_rx_cnt:                   0                 0                 0
           0                 0

---------- VNP Stage -----------------------------------------------------------
vnp_rx_from_kernel_pkts:             30974              6260              6161
       10159              8394
vnp_rx_pkts:                       2610346            720505            793687
      654737            441417
vnp_tx_pkts:                       2608246            723777            788462
      653882            442125
vnp_tx_drop_pkts:                        0                 0                 0
           0                 0
vnp_to_ips_pkts:                      2738               885               656
         652               545
vnp_to_ips_drop_pkts:                     0                 0                 0
            0                 0
vnp_to_vnp_pkts:                         0                 0                 0
           0                 0
vnp_to_vnp_drop_pkts:                    0                 0                 0
           0                 0
vnp_to_kernel_pkts:                  30289              2090             10709
       10342              7148
ipsec_dec_pkts:                          0                 0                 0
           0                 0
ipsec_enc_pkts:                          0                 0                 0
           0                 0
ipsec_sa_add:                            0                 0                 0
           0                 0
ipsec_sa_upd:                            0                 0                 0
```

```
           0                 0
ipsec_sa_del:                            0                 0                 0
           0                 0
ipsec_spi_add:                           0                 0                 0
           0                 0
ipsec_spi_add_fail:                      0                 0                 0
           0                 0
ipsec_spi_del:                           0                 0                 0
           0                 0
ipsec_spi_del_fail:                      0                 0                 0
           0                 0
ipsec_spi_lookup:                        0                 0                 0
           0                 0
ipsec_spi_lookup_fail:                   0                 0                 0
           0                 0
ipsec_spi_reclaim:                       0                 0                 0
           0                 0
ipsec_ib_sa_hit:                         0                 0                 0
           0                 0
ipsec_ib_sa_miss:                        0                 0                 0
           0                 0
ipsec_ib_headroom_err:                   0                 0                 0
           0                 0
ipsec_ib_cryptodev_err:                  0                 0                 0
           0                 0
ipsec_ib_post_proc_err:                  0                 0                 0
           0                 0
ipsec_ib_uesp_dport_err:                 0                 0                 0
           0                 0
ipsec_ib_uesp_not_enabled:               0                 0                 0
           0                 0
ipsec_ob_sa_hit:                         0                 0                 0
           0                 0
ipsec_ob_sa_miss:                        0                 0                 0
           0                 0
ipsec_ob_headroom_err:                   0                 0                 0
           0                 0
ipsec_ob_cryptodev_err:                  0                 0                 0
           0                 0
ipsec_ob_post_proc_err:                  0                 0                 0
           0                 0

---------- IPS Stage -----------------------------------------------------------
ips_rx_pkts:                          2738               657               698
         705               678
ips_tx_pkts:                          2738               657               698
         705               678
ips_drop_pkts:                           0                 0                 0
```

```
           0                 0
ips_vdct_pkts:                           0                 0                 0
           0                 0
ips_inv_pkts:                            0                 0                 0
           0                 0
from_ips_rx_pkts:                        0                 0                 0
           0                 0
from_ips_tx_pkts:                        0                 0                 0
           0                 0
from_ips_drop_pkts:                      0                 0                 0
           0                 0
from_ips_fallback_pkts:                  0                 0                 0
           0                 0

---------- DPDK TX Stage -------------------------------------------------------
dpdktx_rx_pkts:                    2610984           2522231             86925
         893               935
dpdktx_tx_pkts:                    2610984           2522231             86925
         893               935
dpdktx_drop_pkts:                        0                 0                 0
           0                 0
dpdktx_drop_oversized_pkt:               0                 0                 0
           0                 0


diagnose dpdk statistics show vnp

--------------------------------------------------------------------------------
FortiOS DPDK Helper VNP Stats
--------------------------------------------------------------------------------

                                     Total         Engine  0         Engine  1
   Engine  2         Engine  3
CPU ID:                                                    0                 1
           2                 3

---------- VNP Internal --------------------------------------------------------
ctr_sse:                            224038             68362             49639
       50015             56022
ctr_sse_cmd:                           168                62                34
          39                33
ctr_sse_delmiss:                         0                 0                 0
           0                 0
ctr_sse_msg:                           113                48                11
          17                37
ctr_sse_pruned:                          0                 0                 0
           0                 0
```

```
vnp_st_rx_from_dpdkrx:            2610531            720527            793688
     654804            441512
vnp_st_sse_proc:                  2582749            718835            783299
     644776            435839
vnp_st_tx_to_kernel:                30474              2112             10710
      10409              7243
vnp_st_ipsec_ib:                        0                 0                 0
          0                 0
vnp_st_ipsec_ob:                        0                 0                 0
          0                 0
vnp_st_fpath_proc:                2580170            718463            782989
     644412            434306
vnp_st_tx_to_dpdktx:              2608486            723802            788463
     653996            442225
vnp_st_tx_to_ips:                    2738               885               656
        652               545
vnp_st_rx_from_kernel:              31222              6286              6164
      10275              8497
vnp_st_sse_cmd:                       168                62                34
         39                33
vnp_st_final:                       33380              3059             11400
      11100              7821

ctr_sse_entries:                         8                 2                 2
           3                 1

err_sse_batch_size:                      0                 0                 0
           0                 0
err_sse_unknown_cmd:                     0                 0                 0
           0                 0
err_sse_full:                            0                 0                 0
           0                 0
err_sse_tbl_alloc_fail:                  0                 0                 0
           0                 0
err_sse_inv_oid:                         0                 0                 0
           0                 0
err_fp_no_act:                           0                 0                 0
           0                 0
err_fp_no_port:                          0                 0                 0
           0                 0
drop_inv_l3:                             0                 0                 0
           0                 0
drop_inv_l4:                             0                 0                 0
           0                 0
drop_fp_act:                             0                 0                 0
           0                 0
drop_inv_port:                           0                 0                 0
           0                 0
```

```
drop_inv_ip_cksum:                       0                 0                 0
           0                 0
drop_oversized_pkt:                      0                 0                 0
           0                 0
drop_unsupported:                        0                 0                 0
           0                 0
drop_looping_pkt:                        0                 0                 0
           0                 0
drop_ipsec_ob_fail:                      0                 0                 0
           0                 0
--------------------------------------------------------------------------------
```

External ID support in STS for AWS SDN connector - 7.2.1

This enhancement builds on the AWS SDN connector, which can use the AWS security token service (STS) to connect to multiple AWS accounts concurrently. To enhance security, the SDN connector now supports using an external ID, which allows the target account owner to permit the source account to assume the role only under specific circumstances.

See How to use an external ID when granting access to your AWS resources to a third party for details.

The example demonstrates a source account, the AWS account that FortiOS is connected to, accessing a target account. The target account must explicitly allow an external ID string in its role definition. The role definition has a trust policy that allows the source account on the condition that it connects with the specified external ID. You can configure these definitions on the target account in AWS.

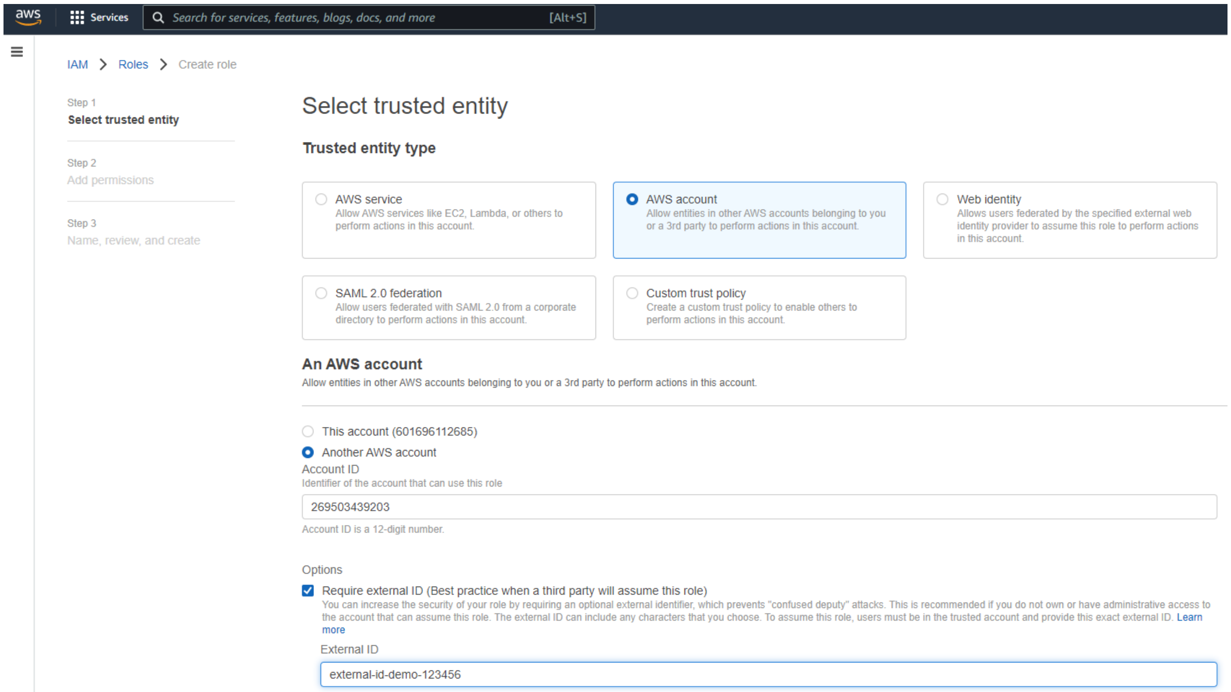
This example uses two AWS accounts:

- **Target account**: 601xxxxxx685
- **Source account**: 269xxxxxx203

The example demonstrates that a FortiGate-VM in the source account can retrieve dynamic objects from the target account if it has the specified external ID.

To configure SDN connector support for AWS STS with an external ID:

1. Log in to the AWS console using the target account.
2. Create an IAM role on the target account:
   a. Go to *IAM* > *Roles* > *Create role* > *AWS account.*
   b. Select *Another AWS account*.
   c. In the *Account ID* field, enter the source account. In this example, the source account is 269xxxxxx203.
   d. Enable *Require external ID (Best practice when a third party will assume this role)*.
   e. In the *External ID* field, enter the desired external ID. In this example, the external ID is external-id-demo-123456.



Select trusted entity

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

● AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ This account (601696112685)
● Another AWS account

Account ID
Identifier of the account that can use this role
269503439203
Account ID is a 12-digit number.

Options

☑ Require external ID (Best practice when a third party will assume this role)
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more

External ID
external-id-demo-123456

f. Click *Next*.

g. Continue with the configuration until the *Review* step. In the *Role name* field, enter the desired role name. In this example, the role name is cross-account-with-external-id-demo.

3. Create an inline policy on the target account:

   a. Go to *IAM* > *Roles*.

   b. Select the role that you created.

   c. Click *Add inline policy* > *JSON*.

   d. Paste the following in to the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

   e. Continue to create the policy. Name the policy as desired. In this example, the policy name is CrossAccountPolicy.

You can also create a standalone policy in *IAM* > *Policies*, and attach the policy to the IAM role, instead of adding an inline policy as this procedure describes.

4. Log in to the AWS console using the source account.
5. Create an IAM role on the source account:
    a. Go to *IAM* > *Roles* > *Create role* > *AWS service* > *EC2*..
    b. Under *Permissions*, configure the desired permissions. In this example, this role is configured with AmazonEC2FullAccess.
    c. Click *Next*.
    d. Continue with the configuration until the *Review* step. In the *Role name* field, enter the desired role name.
6. Create an inline policy on the source account:
    a. Go to *IAM* > *Roles*.
    b. Select the role that you created.
    c. Click *Add inline policy* > *JSON*.
    d. Paste the following in to the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::601xxxxxx685:role/cross-account-with-external-id-
demo"
            ]
        }
    ]
}
```

    e. Continue to create the policy. Name the policy as desired. The resource should be the Amazon resource name (ARN) of the IAM role that you created in the target account. You can find the ARN by logging in to the AWS portal under the target account and going to the IAM web portal.

You can also create a standalone policy in *IAM* > *Policies*, and attach the policy to the IAM role, instead of adding an inline policy as this procedure describes.

7. Launch a FortiGate-VM under the source account.
8. Assign the IAM role that you created in step 5 to the FortiGate-VM.
9. Configure FortiOS:
    a. Configure the AWS SDN connector to be able to access the target account:

```
config system sdn-connector
    edit "aws1"
        config external-account-list
            edit "arn:aws:iam::601xxxxxx685:role/cross-account-with-external-id-
demo"
                set external-id "external-id-demo-123456"
                set region-list "us-east-1"
            next
        end
    next
end
```

b. Configure a dynamic address. This address checks whether the FortiGate-VM can retrieve the instance address in the target account:

```
config firewall address
    edit "sdn1"
        set type dynamic
        set sdn "aws1"
        set filter "InstanceId=i-02c5141c75e6aed4f"
    next
end
```

c. Confirm that the FortiGate-VM can retrieve the dynamic IP address from the target account:

```
show firewall address sdn1
config firewall address
    edit "sdn1"
        set type dynamic
        set sdn "aws1"
        set filter "InstanceId=i-02c5141c75e6aed4f"
        set sdn-addr-type all
        config list
            edit "172.31.24.149"
            next
            edit "54.172.135.95"
            next
        end
    next
end
```

Permanent trial mode for FortiGate-VM - 7.2.1

A permanent evaluation VM license replaces the 15 day evaluation period for FortiGate-VM. The evaluation VM license applies to all private cloud (VMware ESXi, KVM, and so on) and all bring your own license public cloud instances.

When spinning up a new FortiGate-VM, you choose to log in to FortiCare to activate the VM trial or upload a new license.

Limitations of the evaluation VM license include the following:

- Maximum of one free evaluation copy per FortiCare account
- Support for low encryption operation only, except for GUI management access and FortiManager communications
- Maximum of 1 CPU and 2 GB of memory
- Maximum of three interfaces, firewall policies, and routes
- No FortiCare support
- No FortiGuard support
- Support for a maximum of two virtual domains (VDOM). When using multi-VDOM mode, the root VDOM must be an admin type and the other can be a traffic VDOM. See VDOM types.

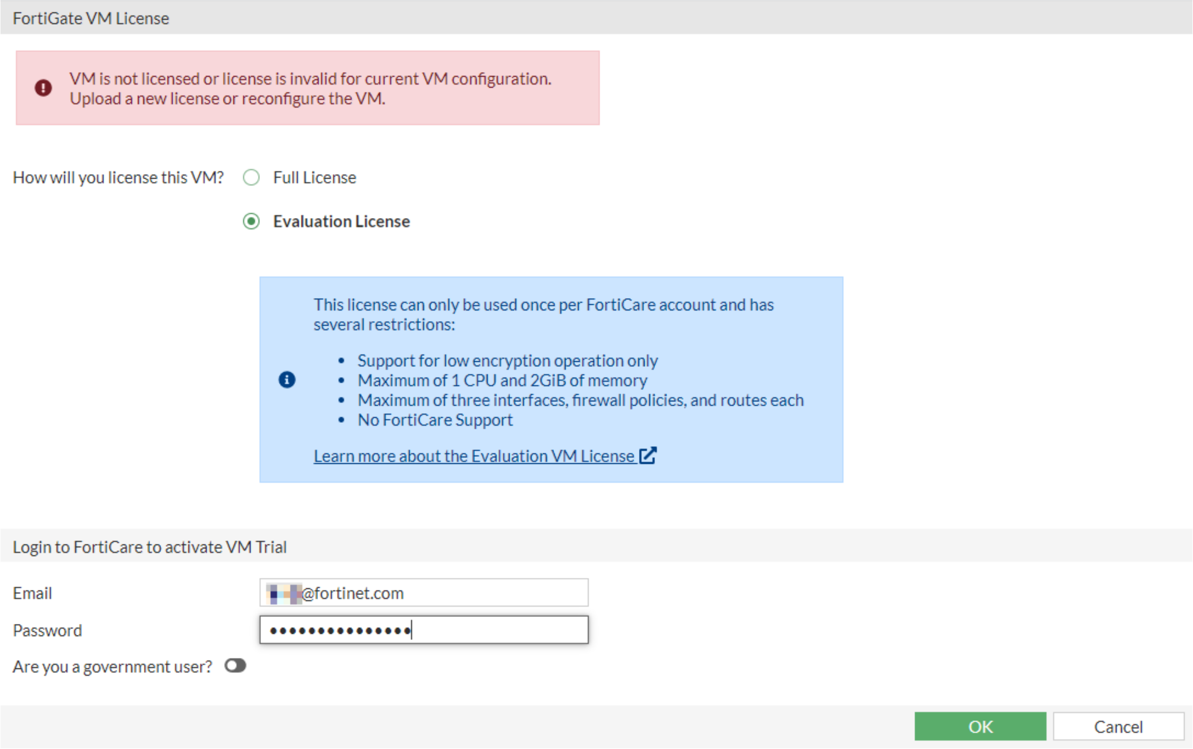
To obtain the permanent VM trial license from FortiCare using the CLI:

1. A newly deployed FortiGate-VM no longer has a valid evaluation license, even if the instance has only 1 CPU and 2 GB of memory. Run `get system status`. The following output is expected:
   ```
   Version: FortiGate-VM64 v7.2.1,build1242,220715 (interim)
   ...
   Serial-Number: FGVMEVNXFLTGKOBC
   License Status: Invalid
   VM Resources: 1 CPU/1 allowed, 2007 MB RAM/2048 MB allowed
   ```
2. Obtain the permanent VM trial license from FortiCare:
   ```
   exec vm-license-options account-id xxxx@fortinet.com
   ```
   ```
   exec vm-license-options account-password xxxxxxx
   ```
   ```
   exec vm-license
   This VM is using the evaluation license. This license does not expire.
   Limitations of the Evaluation VM license include:
     1.Support for low encryption operation only
     2.Maximum of 1 CPU and 2GiB of memory
     3.Maximum of three interfaces, firewall policies, and routes each
     4.No FortiCare Support
   This operation will reboot the system !
   Do you want to continue? (y/n)y

   Connection to 10.6.30.74 closed.
   ```
3. You can run the following commands to check that the permanent VM trial license is valid:
   - `get sys stat`. The following output is expected:
     ```
     Version: FortiGate-VM64 v7.2.1,build1242,220715 (interim)
     ...
     Serial-Number: FGVMEVNXFLTGKOBC
     License Status: Valid
     VM Resources: 1 CPU/1 allowed, 2007 MB RAM/2048 MB allowed
     ```
   - `diagnose hardware sysinfo vm full`. The following output is expected:
     ```
     UUID:     4213dbbc94f2520b0d75eeafe1b319c7
     valid:    1
     status:   1
     code:     0
     warn:     0
     copy:     0
     received: 4294939472
     warning:  4294939472
     recv:     202207162014
     dup:
     ```
   - `diagnose debug vm-print-license`. The following output is expected:
     ```
     SerialNumber: FGVMEVNXFLTGKOBC
     CreateDate: Sat Jul 16 20:11:15 2022
     UUID: 4213dbbc94f2520b0d75eeafe1b319c7
     ```

```
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: EVAL (1)
CPU: 1
MEM: 2048
VDOM license:
  permanent: 2
  subscription: 0
```

To obtain the permanent VM trial license from FortiCare using the GUI:

1. When unlicensed, the FortiOS GUI allows you to download the permanent VM trial license from FortiCare with your FortiCare account credentials. In the FortiGate VM License page, for *How will you license this VM?*, select *Evaluation License*.



FortiGate VM License

VM is not licensed or license is invalid for current VM configuration.
Upload a new license or reconfigure the VM.

How will you license this VM? ○ Full License ● Evaluation License

This license can only be used once per FortiCare account and has several restrictions:

- Support for low encryption operation only
- Maximum of 1 CPU and 2GiB of memory
- Maximum of three interfaces, firewall policies, and routes each
- No FortiCare Support

Learn more about the Evaluation VM License

Login to FortiCare to activate VM Trial

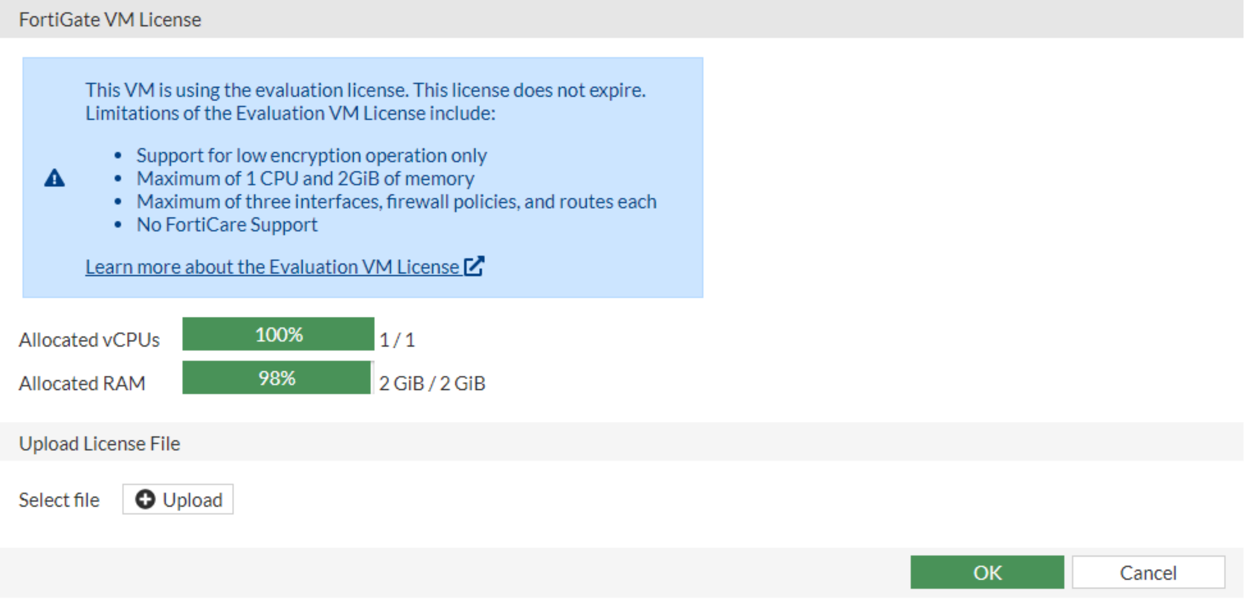
Email: [redacted]@fortinet.com

Password: •••••••••••••••

Are you a government user?

2. In the *Email* field, enter your FortiCare account email address.
3. In the *Password* field, enter your FortiCare account password.
4. Click *OK*. When a permanent VM trial license is applied, the FortiOS, the GUI shows a summary of the license

limitations and allows you to upload a paid VM license.



FortiGate VM License

This VM is using the evaluation license. This license does not expire.
Limitations of the Evaluation VM License include:

- Support for low encryption operation only
- Maximum of 1 CPU and 2GiB of memory
- Maximum of three interfaces, firewall policies, and routes each
- No FortiCare Support

Learn more about the Evaluation VM License

Allocated vCPUs: 100% 1 / 1

Allocated RAM: 98% 2 GiB / 2 GiB

Upload License File

Select file

To allow FortiManager to apply a license to an unlicensed FortiGate-VM instance:

1. Confirm that the FortiGate is unlicensed by running `get system status` in the FortiOS CLI. The following shows expected output for this command:

```
Version: FortiGate-VM64-AZURE v7.2.1,build1252,220728 (interim)
...
Serial-Number: FGVMEVTN8UP4KIA6
License Status: Invalid
VM Resources: 1 CPU/1 allowed, 1945 MB RAM/2048 MB allowed
```

2. In the FortiOS CLI, configure the FortiManager as central management:

```
config system central-management
       set type fortimanager
       set fmg "<FortiManager IP address>"
end
```

3. In FortiManager, configure the VM license as Installing VM licenses describes.

Allow FortiManager to apply license to a BYOL FortiGate-VM instance - 7.2.1

This enhancement allows FortiManager to apply a license to a bring your own license (BYOL) FortiGate-VM instance. For example, when launching a BYOL FortiGate-VM on Azure, the FortiGate receives a serial number (SN) with the FGVMEV prefix and a VM license with an invalid status by default. This unlicensed FortiGate-VM can register to a FortiManager for authorization and management. Subsequently, the FortiManager can apply a VM license to the FortiGate-VM instance.

To allow FortiManager to apply license to a BYOL FortiGate-VM instance:

1. Confirm that the FortiGate is unlicensed by running `get system status` in the FortiOS CLI. The following shows expected output for this command:

```
Version: FortiGate-VM64-AZURE v7.2.1,build1252,220728 (interim)
...
Serial-Number: FGVMEVTN8UP4KIA6
License Status: Invalid
VM Resources: 1 CPU/1 allowed, 1945 MB RAM/2048 MB allowed
```

2. In the FortiManager CLI, enable `allow_register`:

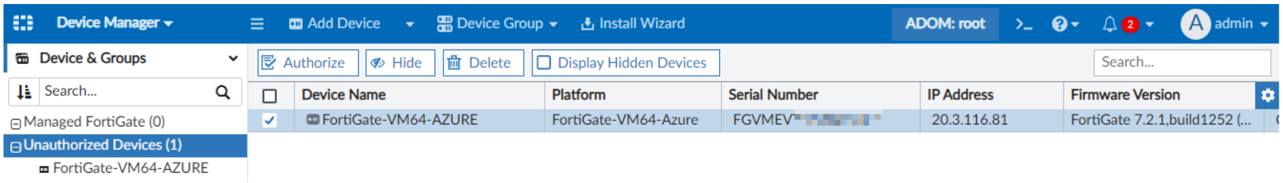
```
config system admin setting
    set allow_register enable
    set register_passwd xxxxxx
end
```

3. In the FortiOS CLI, configure the FortiManager:

```
config system central-management
    set type fortimanager
    set fmg "<FortiManager IP address>"
end
```

4. In the FortiOS CLI, confirm that the FortiGate-VM can connect to FortiManager by running `diagnose fdsm central-mgmt-status`. The following shows expected output for this command:

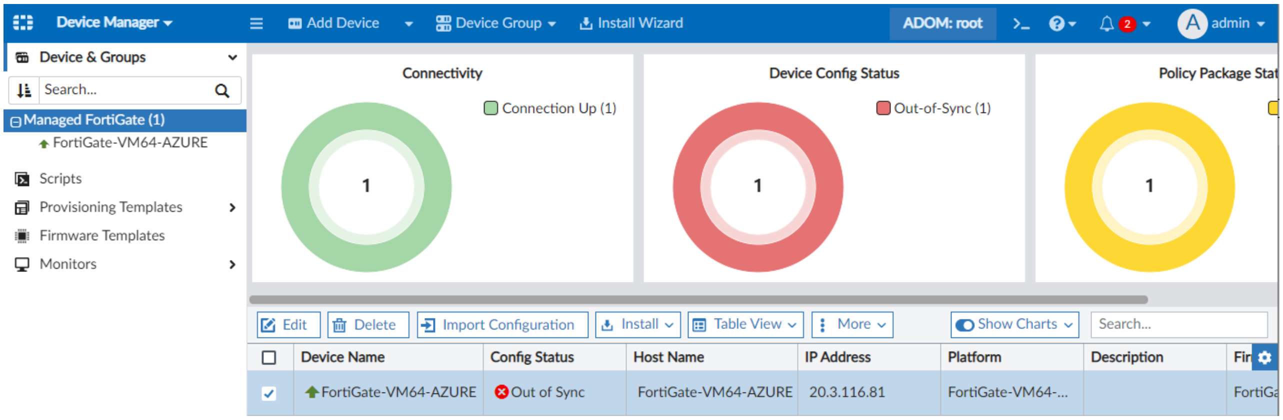
```
Connection status: Handshake
Registration status: Unknown
```



☐	Device Name	Platform	Serial Number	IP Address	Firmware Version
☑	FortiGate-VM64-AZURE	FortiGate-VM64-Azure	FGVMEV[redacted]	20.3.116.81	FortiGate 7.2.1,build1252 (...

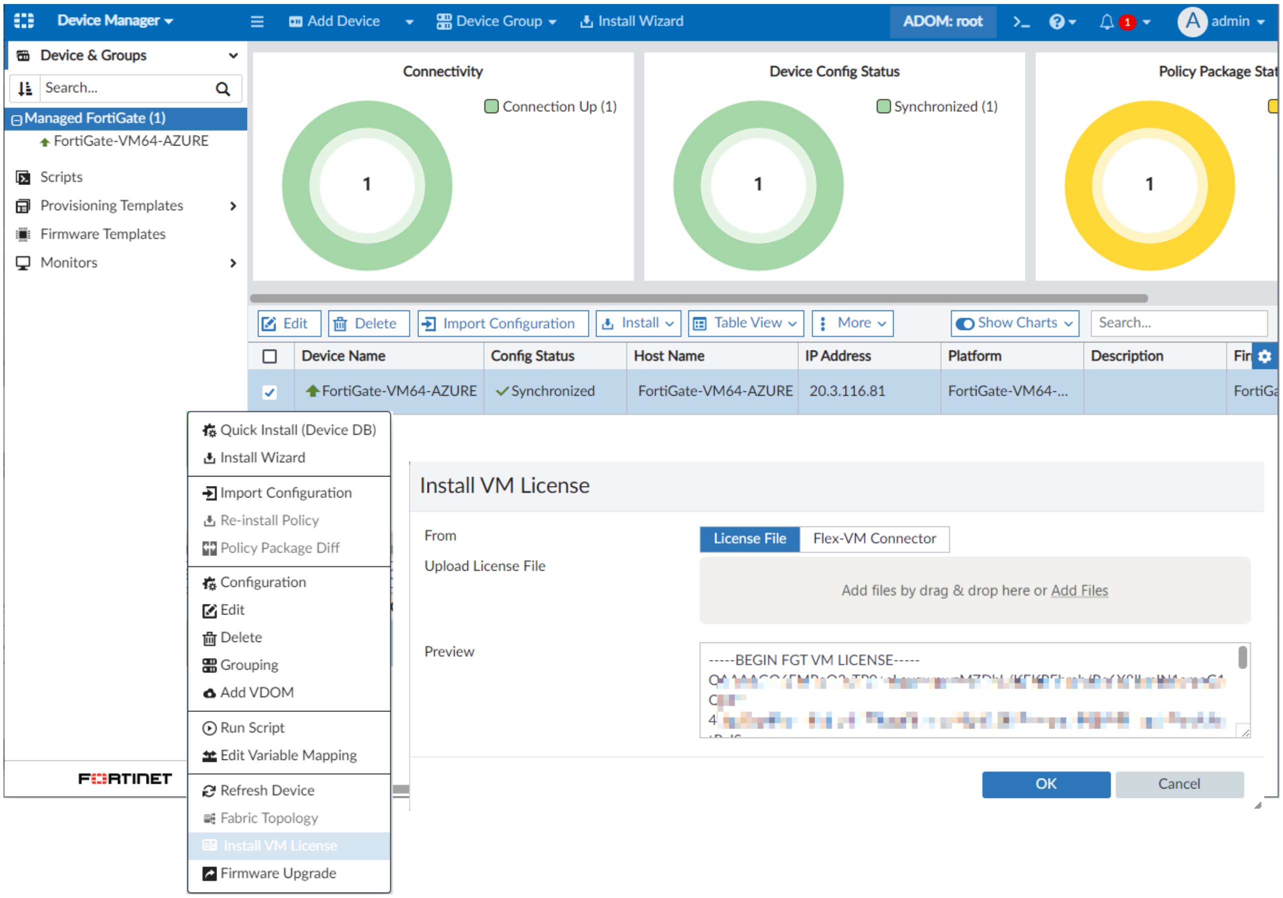
5. Register the FortiGate to FortiManager by running `execute central-mgmt register-device <FortiManager SN> xxxxxx` in the FortiOS CLI. Use the password that you configured in step 2.
6. In the FortiOS CLI, confirm that the FortiGate-VM registered to FortiManager by running `diagnose fdsm central-mgmt-status`. The following shows expected output for this command:

```
Connection status: Up
Registration status: Registered
```



☐	Device Name	Config Status	Host Name	IP Address	Platform	Description	Fir
☑	FortiGate-VM64-AZURE	Out of Sync	FortiGate-VM64-AZURE	20.3.116.81	FortiGate-VM64-...		FortiGa

7. In FortiManager, right-click the FortiGate, then select *Install VM License*.



☐	Device Name	Config Status	Host Name	IP Address	Platform	Description	Fir
☑	FortiGate-VM64-AZURE	✓ Synchronized	FortiGate-VM64-AZURE	20.3.116.81	FortiGate-VM64-...		FortiGa

Install VM License

From: License File | Flex-VM Connector

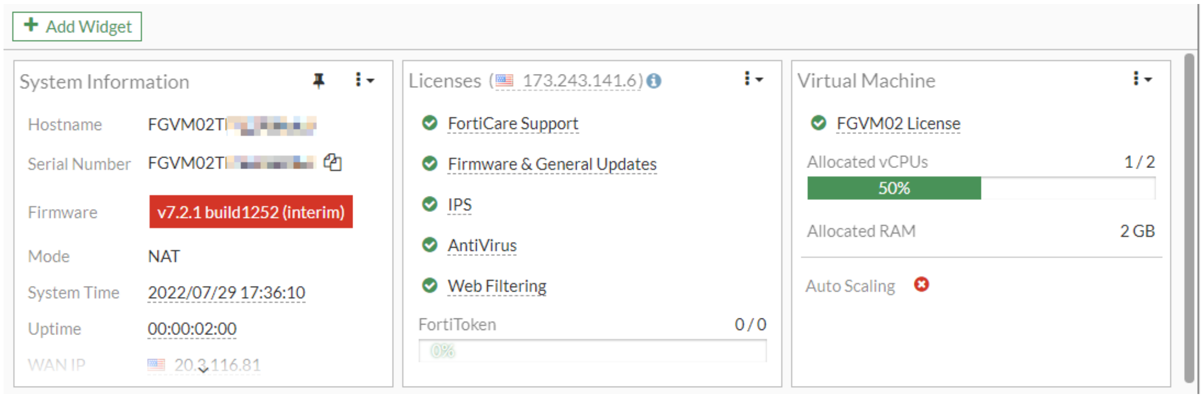
Upload License File: Add files by drag & drop here or Add Files

Preview:

```
-----BEGIN FGT VM LICENSE-----
[redacted]
```

OK Cancel

8. In the FortiOS GUI, confirm that the FortiGate-VM has received a license from the FortiManager.



System Information

Hostname FGVM02T[redacted]

Serial Number FGVM02T[redacted]

Firmware v7.2.1 build1252 (interim)

Mode NAT

System Time 2022/07/29 17:36:10

Uptime 00:00:02:00

WAN IP 20.3.116.81

Licenses (173.243.141.6)

✓ FortiCare Support

✓ Firmware & General Updates

✓ IPS

✓ AntiVirus

✓ Web Filtering

FortiToken 0 / 0

0%

Virtual Machine

✓ FGVM02 License

Allocated vCPUs 1 / 2

50%

Allocated RAM 2 GB

Auto Scaling ✗

Enable high encryption on FGFM protocol for unlicensed FortiGate-VMs - 7.2.1

For FortiManager to manage unlicensed FortiGate-VMs, FortiOS enables high encryption on the FortiGate to FortiManager (FGFM) protocol for secure connection between the FortiGate and FortiManager. In this context, a FortiGate-VM is considered unlicensed if it does not have any license applied, including evaluation licenses. After adding the FortiGate-VMs to device manager, FortiManager can install VM licenses to the managed FortiGate-VMs.

For example, in a situation where you deployed five unlicensed FortiGate-VMs, you can configure the CLI to point to the FortiManager for central management for all five VMs. FortiManager can then communicate with these VMs over high encryption and manage them.

The example below demonstrates that after configuring central management from the unlicensed VM's CLI (in this case a VM with an invalid license), FortiOS can initiate a secure TLS 1.3 session to the FortiManager and establish a connection. Subsequently, FortiManager can add this device to device management and install a VM license to it.

To allow FortiManager to apply license to an unlicensed FortiGate-VM instance:

1. Confirm that the FortiGate is unlicensed by running `get system status` in the FortiOS CLI. The following shows expected output for this command:

```
Version: FortiGate-VM64 v7.2.1,build1242,220715 (interim)
...
Serial-Number: FGVMEVNXFLTGKOBC
License Status: Invalid
VM Resources: 2 CPU/1 allowed, 3963 MB RAM/2048 MB allowed
```

2. In the FortiOS CLI, configure the FortiManager:

```
config system central-management
    set type fortimanager
    set fmg "<FortiManager IP address>"
end
```

3. In the FortiOS CLI, confirm that the FortiGate-VM can connect to FortiManager by running `diagnose fdsm central-mgmt-status`. The following shows expected output for this command:

```
Connection status: Handshake
Registration status: Unknown
```

```
FGFMs: Create session 0x114988a0.
FGFMs: setting session 0x114988a0 exclusive=0
FGFMs: Connect to 10.6.30.239:541, local 10.6.30.74:22055.
FGFMs: cert_id<0>, sni<support.>FGFMs: set_fgfm_sni SNI<support.fortinet.com>
FGFMs: Load Cipher [ALL:!RC4:!EXPORT:@STRENGTH]
FGFMs: before SSL initialization
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS read server hello
FGFMs: SSLv3/TLS write change cipher spec
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS read server hello
FGFMs: TLSv1.3 read encrypted extensions
FGFMs: SSLv3/TLS read server certificate request
FGFMs: SSLv3/TLS read server certificate
FGFMs: Remote issuer is /C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=support/emailAddress=support@fortinet.com.
FGFMs: issuer matching...try next if not match... localissuer(support),
remoteissuer(support)
FGFMs: Root issuer matched, local=remote=support
FGFMs: TLSv1.3 read server certificate verify
FGFMs: SSLv3/TLS read finished
FGFMs: SSLv3/TLS write client certificate
FGFMs: SSLv3/TLS write certificate verify
FGFMs: SSLv3/TLS write finished
FGFMs: SSL negotiation finished successfully
FGFMs: client:send:
get auth
serialno=FGVMEVNXFLTGKOBC
mgmtid=00000000-0000-0000-0000-000000000000
platform=FortiGate-VM64
fos_ver=700
minor=2
patch=1
build=1242
branch=1242
maxvdom=2
fg_ip=10.6.30.74
hostname=FGT-ESXi-REGR
harddisk=yes
biover=04000002
harddisk_size=30720
logdisk_size=30235
mgmt_mode=normal
enc_flags=0
mgmtip=10.6.30.74
```

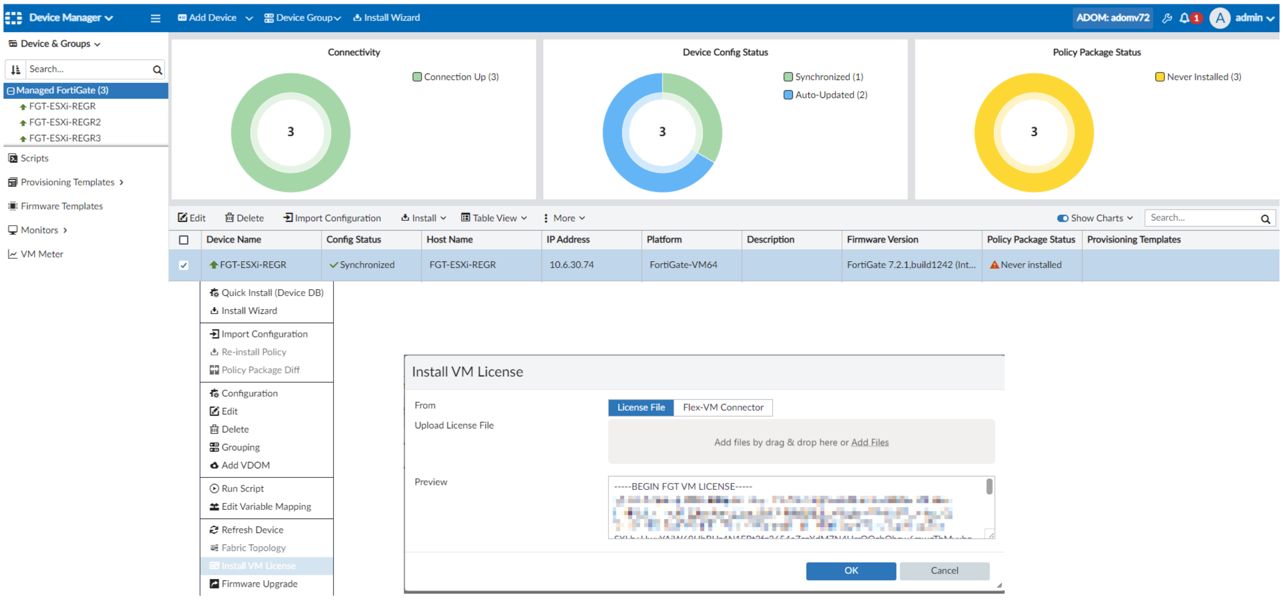
```
mgmtport=443


FGFMs: SSL negotiation finished successfully
FGFMs: SSL negotiation finished successfully
FGFMs: SSLv3/TLS read server session ticket
FGFMs: SSL negotiation finished successfully
FGFMs: SSL negotiation finished successfully
FGFMs: SSLv3/TLS read server session ticket
FGFMs: client:
reply 200
request=auth
serialno=FMG-VMTM21011759
user=
passwd=
mgmtport=443
keepalive_interval=120
chan_window_sz=32768
sock_timeout=360
mgmtid=2016070622


FGFMs: [__chg_by_fgfm_msg] set keepalive_interval: 120
FGFMs: [__chg_by_fgfm_msg] set channel buffer/window size to 32768 bytes
FGFMs: [__chg_by_fgfm_msg] set sock timeout: 360
FGFMs: client:send:
reply 501
request=auth


FGFMs: serial no FMG-VMTM21011759 saved to FMG detect file
FGFMs: Entering __cmdb_event_centmgmt_handler 1364.
FGFMs: Entering fgfm_clt_restart 373.
FGFMs: Cleanup session 0x114988a0, 10.6.30.239.
FGFMs: Destroy session 0x114988a0, 10.6.30.239.
FGFMs: Create session 0x114a0e40.
FGFMs: setting session 0x114a0e40 exclusive=0
FGFMs: Connect to 10.6.30.239:541, local 10.6.30.74:22056.
FGFMs: cert_id<0>, sni<support.>FGFMs: set_fgfm_sni SNI<support.fortinet.com>
FGFMs: Load Cipher [ALL:!RC4:!EXPORT:@STRENGTH]
FGFMs: before SSL initialization
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS read server hello
FGFMs: SSLv3/TLS write change cipher spec
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS write client hello
FGFMs: SSLv3/TLS read server hello
```

```
FGFMs: TLSv1.3 read encrypted extensions
FGFMs: SSLv3/TLS read server certificate request
FGFMs: SSLv3/TLS read server certificate
FGFMs: Remote issuer is /C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=support/emailAddress=support@fortinet.com.
FGFMs: issuer matching...try next if not match... localissuer(support),
remoteissuer(support)
FGFMs: Root issuer matched, local=remote=support
FGFMs: TLSv1.3 read server certificate verify
FGFMs: SSLv3/TLS read finished
FGFMs: SSLv3/TLS write client certificate
FGFMs: SSLv3/TLS write certificate verify
FGFMs: SSLv3/TLS write finished
FGFMs: SSL negotiation finished successfully
FGFMs: client:send:
get auth
serialno=FGVMEVNXFLTGKOBC
mgmtid=00000000-0000-0000-0000-000000000000
platform=FortiGate-VM64
```

4. Register the FortiGate to FortiManager by running `execute central-mgmt register-device <FortiManager SN> xxxxxx` in the FortiOS CLI. Use the password that you configured in step 2.
5. In FortiManager, authorize the unlicensed FortiGate-VM from the *Unregistered Devices* list.
6. In the FortiOS CLI, confirm that the FortiGate-VM registered to FortiManager by running `diagnose fdsm central-mgmt-status`. The following shows expected output for this command:

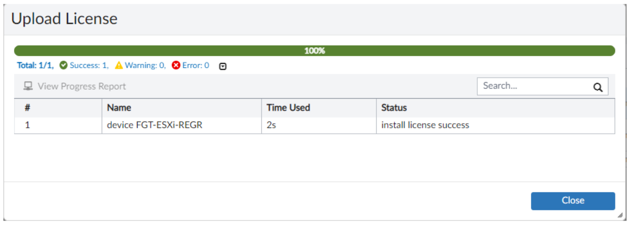
```
Connection status: Up
Registration status: Registered
```

7. In FortiManager, right-click the FortiGate, then select *Install VM License*.



☐	Device Name	Config Status	Host Name	IP Address	Platform	Description	Firmware Version	Policy Package Status	Provisioning Templates
☑	FGT-ESXi-REGR	✓ Synchronized	FGT-ESXi-REGR	10.6.30.74	FortiGate-VM64		FortiGate 7.2.1,build1242 (Int...	Never installed	

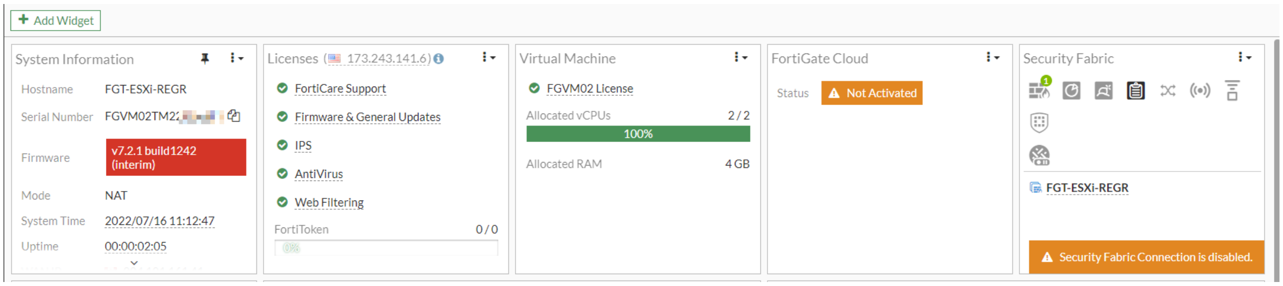
```
-----BEGIN FGT VM LICENSE-----
[redacted]
```



Total: 1/1, Success: 1, Warning: 0, Error: 0

#	Name	Time Used	Status
1	device FGT-ESXi-REGR	2s	install license success

8. In the FortiOS GUI, confirm that the FortiGate-VM has received a license from the FortiManager.



Hostname	FGT-ESXi-REGR
Serial Number	FGVM02TM2[redacted]
Firmware	v7.2.1 build1242 (interim)
Mode	NAT
System Time	2022/07/16 11:12:47
Uptime	00:00:02:05

Licenses: ✓ FortiCare Support; ✓ Firmware & General Updates; ✓ IPS; ✓ AntiVirus; ✓ Web Filtering; FortiToken 0 / 0 (0%)

Virtual Machine: ✓ FGVM02 License; Allocated vCPUs 2 / 2 (100%); Allocated RAM 4 GB

FortiGate Cloud: Status Not Activated

Support Ampere A1 Compute instances on OCI - 7.2.4

This enhancement allows FortiGate-VM for OCI to work on ARM-based Oracle Cloud Ampere A1 Compute instances.

For more information about this feature, see Support Ampere A1 Compute instances on OCI.

Implement sysrq for kernel crash - 7.2.4

In some scenarios where it is necessary to simulate a system crash, these new commands allow a super administrator to safely trigger a kernel crash using the `sysrq` key. A kernel crash dump is outputted to the console, and FortiOS reboots and recovers without function loss. Only FortiGate-VM supports this feature.

Following are the new commands for this feature:

Command	Description
`diagnose debug kernel sysrq status`	Verify if the feature is enabled or disabled.
`diagnose debug kernel sysrq enable | disable`	Enable or disable the feature.
`diagnose debug kernel sysrq command crash`	Trigger the safe kernel crash.

Scenarios where you may need to simulate a system crash without a reboot include high availability failover tests, virtual network function (VNF) healing tests, and third party VNF certification tests.

The following shows a sample kernel crash dump:

```
fgt01 # diagnose debug kernel sysrq status
Magic SysRq is disable
fgt01 #
fgt01 # diagnose debug kernel sysrq command
crash    Perform a system crash.

fgt01 # diagnose debug kernel sysrq command crash
Magic SysRq is disable!

fgt01 #
fgt01 # diagnose debug kernel sysrq enable

fgt01 #
fgt01 # diagnose debug kernel sysrq status
Magic SysRq is enabled (val=0x8)
fgt01 #
fgt01 # diagnose debug kernel sysrq command crash
This operation will generate a kernel crash and cause the firewall to reboot.
Do you want to continue? (y/n)y

BUG: unable to handle kernel NULL pointer dereference at 0000000000000000
PGD 28989a067 P4D 28989a067 PUD 28989b067 PMD 0
Oops: 0002 [#1] SMP
CPU: 2 PID: 2111 Comm: newcli Tainted: P                  4.19.13 #1
Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS 090008
12/07/2018
RIP: 0010:sysrq_handle_crash+0xd/0x16
Code: 89 f7 e8 d6 15 dd ff eb d2 45 89 ec eb f1 41 bc fb ff ff ff eb c5 e8 ca 06 c6 ff 90 90
c7 05 7e 04 19 01 01 00 00 00 0f ae f8 <c6> 04 25 00 00 00 00 01 c3 55 48 89 e5 bf 02 00 00
00 e8 44 89 c8
RSP: 0018:ffffc9000480fd58 EFLAGS: 00010246
RAX: ffffffff8068fe00 RBX: 0000000000000001 RCX: 0000000000000006
RDX: 0000000000000000 RSI: 0000000000000092 RDI: 0000000000000063
RBP: ffffc9000480fd80 R08: 0000000000000233 R09: 0000000000000004
R10: 0000000000000000 R11: 0000000000000001 R12: 0000000000000063
R13: 0000000000000004 R14: ffffffff81673560 R15: 0000000000000000
FS:  00007f0177113fc0(0000) GS:ffff8882b7b00000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000000000 CR3: 0000000289899001 CR4: 00000000003606e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
```

```
Call Trace:
 ? __handle_sysrq.cold+0x48/0xf7
 write_sysrq_trigger+0x26/0x35
 proc_reg_write+0x36/0x74
 __vfs_write+0x36/0x16c
 ? __se_sys_newfstat+0x89/0xa5
 ? _cond_resched+0x15/0x3c
 vfs_write+0xa0/0x198
 ksys_write+0x4f/0xad
 __x64_sys_write+0x15/0x17
 do_syscall_64+0x66/0x281
 entry_SYSCALL_64_after_hwframe+0x44/0xa9
RIP: 0033:0x7f017a341fa3
Code: 8b 15 f1 ce 0c 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b7 0f 1f 00 64 8b 04 25 18 00
00 00 85 c0 75 14 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 55 c3 0f 1f 40 00 48 83 ec 28
48 89 54 24 18
RSP: 002b:00007ffe608b46d8 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
RAX: ffffffffffffffda RBX: 0000000000000001 RCX: 00007f017a341fa3
RDX: 0000000000000001 RSI: 000000001138a000 RDI: 0000000000000007
RBP: 000000001138a000 R08: 0000000000000000 R09: 0000000000000001
R10: 00000000000001b6 R11: 0000000000000246 R12: 0000000000000001
R13: 000000001137f2a0 R14: 0000000000000001 R15: 00007f017a40b880
Modules linked in: filter4(P)
CR2: 0000000000000000
---[ end trace 1a3b9e86e8978153 ]---
RIP: 0010:sysrq_handle_crash+0xd/0x16
Code: 89 f7 e8 d6 15 dd ff eb d2 45 89 ec eb f1 41 bc fb ff ff ff eb c5 e8 ca 06 c6 ff 90 90
c7 05 7e 04 19 01 01 00 00 00 0f ae f8 <c6> 04 25 00 00 00 00 01 c3 55 48 89 e5 bf 02 00 00
00 e8 44 89 c8
RSP: 0018:ffffc9000480fd58 EFLAGS: 00010246
RAX: ffffffff8068fe00 RBX: 0000000000000001 RCX: 0000000000000006
RDX: 0000000000000000 RSI: 0000000000000092 RDI: 0000000000000063
RBP: ffffc9000480fd80 R08: 0000000000000233 R09: 0000000000000004
R10: 0000000000000000 R11: 0000000000000001 R12: 0000000000000063
R13: 0000000000000004 R14: ffffffff81673560 R15: 0000000000000000
FS:  00007f0177113fc0(0000) GS:ffff8882b7b00000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000000000 CR3: 0000000289899001 CR4: 00000000003606e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Kernel panic - not syncing: Fatal exception
Kernel Offset: disabled
Rebooting in 5 seconds..

System is starting...
Starting system maintenance...
Scanning /dev/sda1... (100%)
Scanning /dev/sda2... (100%)
Serial number is FGT123456
```

Support various AWS endpoint ENI IP addresses in AWS SDN Connector - 7.2.4

This enhancement allows the FortiGate AWS SDN connector to resolve various AWS endpoint ENI IP addresses:

- API Gateway Private Endpoint
- VPC endpoint for Data API for Aurora
- AWS PrivateLink for S3
- VPC endpoints for Lamdba

Support automatic vCPU hot-add in FortiGate-VM for S-series and FortiFlex licenses - 7.2.4

FortiGate-VM supports automatic vCPU hot-add/hot-remove to the limit of the license entitlement after activating an S-series license or a FortiFlex license. This enhancement removes the requirement for the CLI command `execute cpu add <number_of_new_vCPUs>` to be run or a reboot to be performed when the FortiGate-VM has a lower number of vCPUs allocated than the licensed number of vCPUs.

The following example spins up a new FortiGate-VM assigned with four vCPU:

```
FGT-CPU-Demo # get system status
Version: FortiGate-VM64 v7.2.4,build1371,221129 (interim)
...
Serial-Number: FGVM123456
License Status: Invalid
VM Resources: 1 CPU/1 allowed, 1993 MB RAM/2048 MB allowed
Log hard disk: Available
Hostname: FGT-CPU-Demo
FGT-CPU-Demo # execute cpu show
Active CPU number: 1
Total CPU number: 4
```

When activating an S-series license with four vCPU seats on the FortiGate-VM, you do not need to run `execute cpu add <number_of_new_vCPUs>` or reboot the FortiGate-VM. The FortiGate-VM automatically consumes four vCPUs out of four vCPUs allowed:

```
FGT-CPU-Demo # get system status
Version: FortiGate-VM64 v7.2.4,build1371,221129 (interim)
...
Serial-Number: FGVM123456
License Status: Valid
License Expiration Date: 2023-05-05
VM Resources: 4 CPU/4 allowed, 1993 MB RAM <===before this spec, without a reboot or "exec
     cpu add x" manually, FGT v7.2.3 shows "VM Resources: 1 CPU/4 allowed, 2007 MB RAM"
Log hard disk: Available
Hostname: FGT-CPU-Demo
FGT-CPU-Demo # execute cpu show
Active CPU number: 4
Total CPU number: 4
```

Support for GCP ARM CPU-based T2A instance family - 7.2.4

FortiGate-VM supports the GCP T2A instance family. See Deploying a FortiGate-VM using a GCP ARM CPU-based T2A instance.

Support for GCP shielded and confidential VM service - 7.2.4

FortiGate-VM for GCP supports shielded and confidential VM modes where a UEFI VM image is used for secure boot and data-in-use is encrypted during processing. These flavors use AMD EPYC Rome CPUs with vTPM. Using UEFI support with a signed bootloader ensures that the FortiGate-VM for GCP can be validated and verified to use the confidential and shielded VM flavors and modes. This allows you to encrypt your data during CPU processing. See What is Shielded VM? and Confidential Computing concepts.

You can directly deploy a FortiGate-VM in shielded or confidential VM mode by using the premade marketplace image onto cvm and shielded-vm flavors/modes. Running `get hardware cpu` on an instance in shielded or confidential mode outputs the following:

```
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 23
model           : 49
model name      : AMD EPYC 7B12
stepping        : 0
microcode       : 0x1000065
cpu MHz         : 2249.998
cache size      : 512 KB
physical id     : 0
siblings        : 8
core id         : 0
cpu cores       : 4
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 13
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
clflush mmx fxsr sse sse2 ht syscall nx mmxext fxsr_opt pdpe1gb rdtscp lm constant_tsc rep_
good nopl xtopology nonstop_tsc cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 fma
cx16 sse4_1 sse4_2 movbe popcnt aes xsave avx f16c rdrand hypervisor lahf_lm cmp_legacy cr8_
legacy abm sse4a misalignsse 3dnowprefetch osvw topoext ssbd ibrs ibpb stibp vmmcall
fsgsbase tsc_adjust bmi1 avx2 smep bmi2 rdseed adx smap clflushopt clwb sha_ni xsaveopt
xsavec xgetbv1 clzero xsaveerptr arat npt nrip_save umip rdpi
```

VMware ESXi FortiGate-VM as ZTNA gateway - 7.2.5

FortiOS supports deploying a VMware ESXi FortiGate-VM directly as a zero trust application gateway using the OVF template (.vapp). You can configure zero trust network access (ZTNA)-related parameters such as the EMS server, external and internal interface IP addresses, and the application server mapping, during OVF deployment. The deployment also bootstraps ZTNA policy, authentication scheme, rules, and user group configurations.

For more information about this feature, see VMware ESXi FortiGate-VM as ZTNA gateway.

Support the new AWS c7gn instance family - 7.2.6

FortiGate-VM supports the new AWS c7gn instance family using the FGT-ARM64-AWS image.

For more information about this feature, see Instance type support.

Add OVF template support for VMware ESXi 8 - 7.2.6

This feature introduces compatibility between the FortiGate-VM64.ovf and FortiGate-VM65.vapp.ovf templates with VMware ESXi 8, virtual hardware version 20.

For more information about this feature, see Add OVF template support for VMware ESXi 8.

Operational Technology

This section includes information about Operational Technology new features:

- GUI on page 636
- System on page 639

GUI

This section includes information about GUI related Operational Technology new features:

- Add OT asset visibility and network topology to Asset Identity Center page on page 636

Add OT asset visibility and network topology to Asset Identity Center page

Tabs are added in the *Asset Identity Center* page to view the OT asset list and OT network topology using Purdue Levels. This feature is available regardless of whether a Security Fabric is enabled.

To enable the OT features in the GUI:

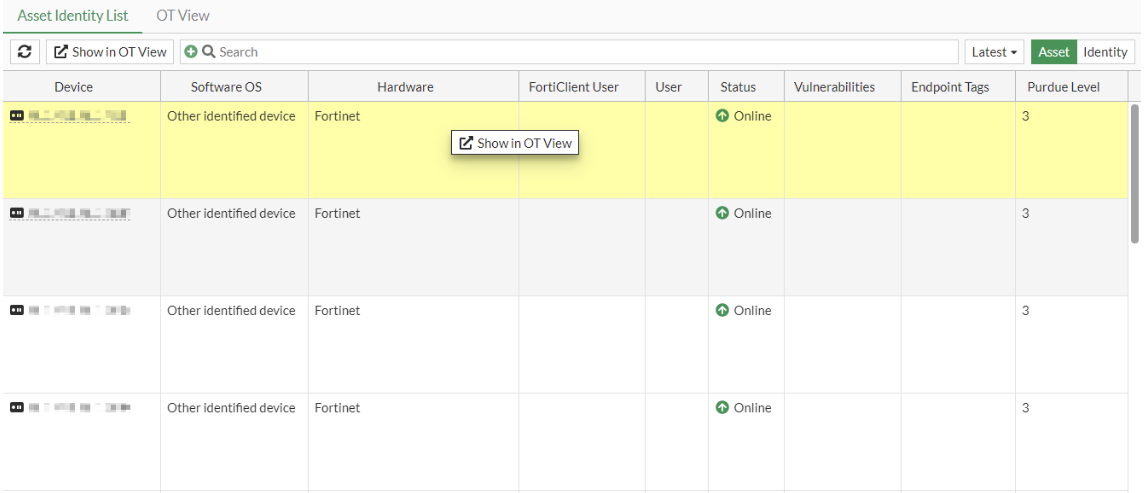
1. Go to *System* > *Feature Visibility*.
2. In the *Additional Features* section, enable *Operational Technology (OT)*.
3. Click *Apply*.

To enable the OT features in the CLI:

```
config system settings
    set gui-ot enable
end
```

Once enabled, the *Security Fabric* > *Asset Identity Center* page displays an *Asset Identity List* tab and an *OT View* tab.

- The *Asset Identity List* tab includes a configurable *Purdue Level* column and a *Show in OT View* option for selected devices in the table.

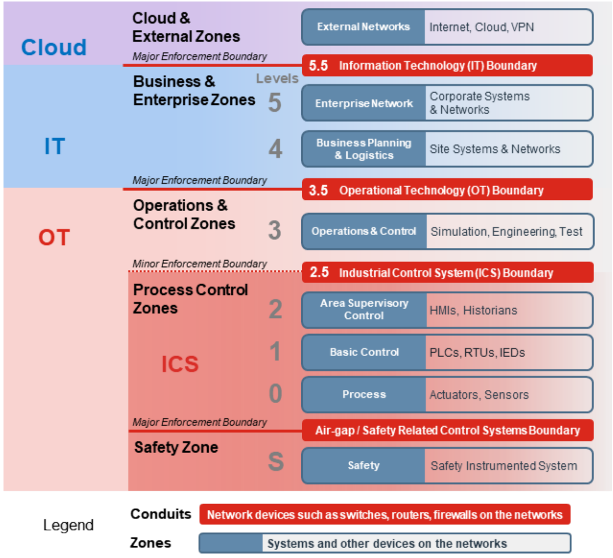


Device	Software OS	Hardware	FortiClient User	User	Status	Vulnerabilities	Endpoint Tags	Purdue Level
[redacted]	Other identified device	Fortinet			Online			3
[redacted]	Other identified device	Fortinet			Online			3
[redacted]	Other identified device	Fortinet			Online			3
[redacted]	Other identified device	Fortinet			Online			3

- The *OT View* tab shows a topology of detected components and connections mapped to Purdue Levels. The default view is locked, but devices can be dragged and dropped to other Purdue Levels if the view is unlocked.

FortiGates and managed FortiSwitches are statically assigned Purdue Level 2 and cannot be changed. Other detected devices are assigned Purdue Level 3 by default and can be changed (except to level S, 0, or external).

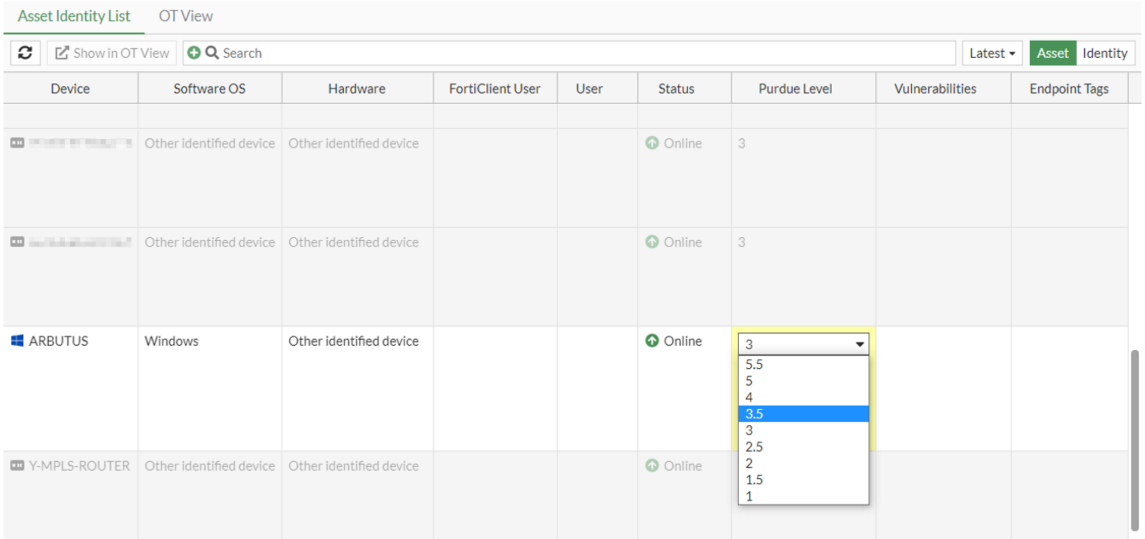
The following diagram lists the Purdue Levels based on OT network topologies:


Cloud
Cloud & External Zones
External Networks
Internet, Cloud, VPN
Major Enforcement Boundary
5.5 Information Technology (IT) Boundary
IT
Business & Enterprise Zones
Levels
5
Enterprise Network
Corporate Systems & Networks
4
Business Planning & Logistics
Site Systems & Networks
Major Enforcement Boundary
3.5 Operational Technology (OT) Boundary
OT
Operations & Control Zones
3
Operations & Control
Simulation, Engineering, Test
Minor Enforcement Boundary
2.5 Industrial Control System (ICS) Boundary
Process Control Zones
ICS
2
Area Supervisory Control
HMIs, Historians
1
Basic Control
PLCs, RTUs, IEDs
0
Process
Actuators, Sensors
Major Enforcement Boundary
Air-gap / Safety Related Control Systems Boundary
Safety Zone
S
Safety
Safety Instrumented System
Legend
Conduits
Network devices such as switches, routers, firewalls on the networks
Zones
Systems and other devices on the networks

To change the Purdue Level in the Asset Identity List tab:

1. Go to *Security Fabric > Asset Identity Center* and select the *Asset Identity List* tab.
2. Add the *Purdue Level* column to the table:
   a. Hover over the table header and click the gear icon (*Configure Table*).
   b. Select *Purdue Level*.
   c. Click *Apply*.
3. Select a device and hover over the *Purdue Level* value.
4. Click the pencil icon to edit the level.

5. Select a value from the dropdown.

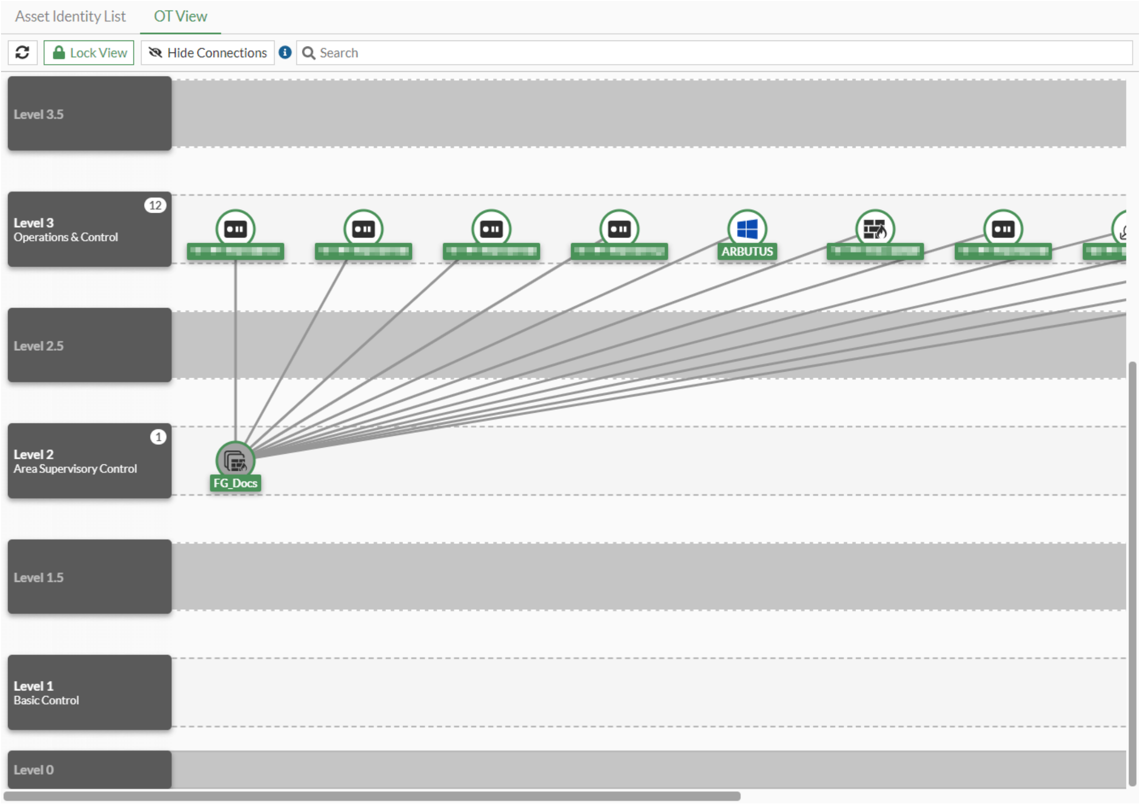


Device	Software OS	Hardware	FortiClient User	User	Status	Purdue Level	Vulnerabilities	Endpoint Tags
[redacted]	Other identified device	Other identified device			Online	3		
[redacted]	Other identified device	Other identified device			Online	3		
ARBUTUS	Windows	Other identified device			Online	3 5.5 5 4 3.5 3 2.5 2 1.5 1		
Y-MPLS-ROUTER	Other identified device	Other identified device			Online			

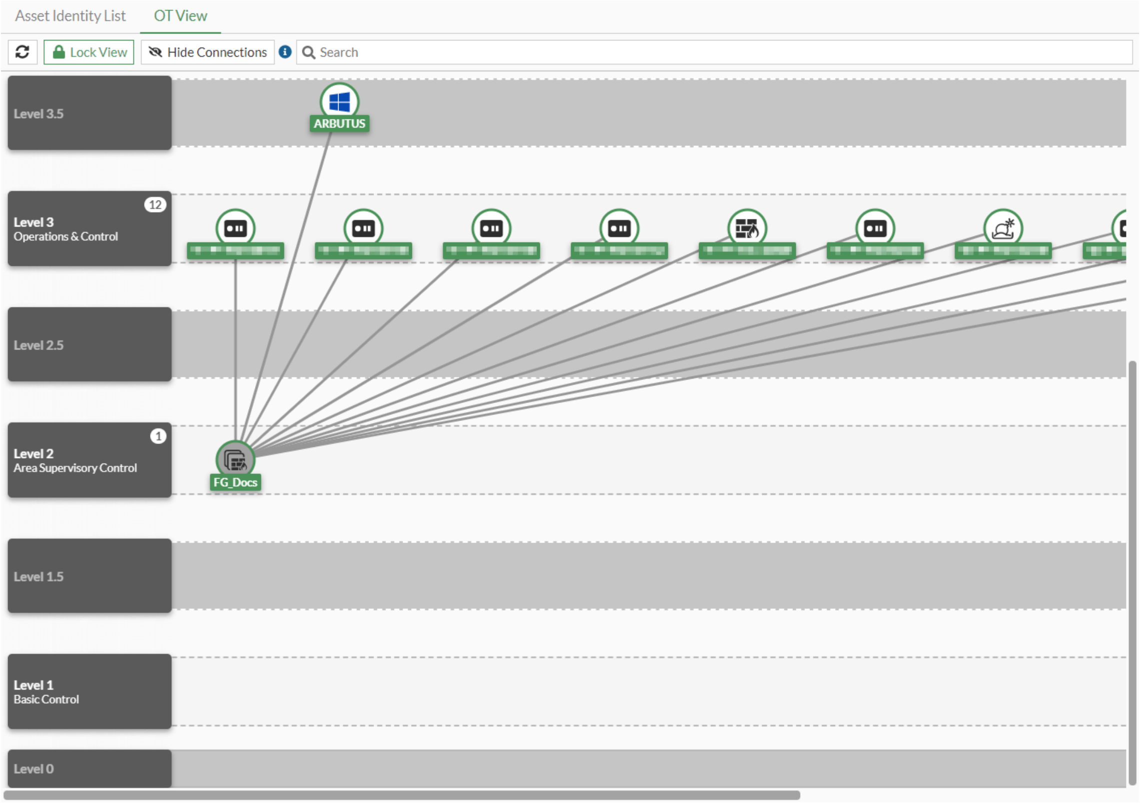
6. Click *Apply*.

To change the Purdue Level in the OT View tab:

1. Go to *Security Fabric* > *Asset Identity Center* and select the *OT View* tab.
2. Click *Unlock View*.
3. Select a device.



4. Drag the device icon to another level row.



5. Optionally, click *Lock View* to revert to the locked view.

To change the Purdue Level in the CLI:

```
# diagnose user-device-store device memory ot-purdue-set <mac> <ip> <level>
```

`mac`	Enter the MAC address of the device.
`ip`	Enter the IPv4 address of the device.
`level`	Enter the Purdue Level: 1, 1.5, 2, 2.5, 3, 3.5, 4, 5, 5.5.

System

This section includes information about system related Operational Technology new features:

- Allow manual licensing for FortiGates in air-gap environments on page 639

Allow manual licensing for FortiGates in air-gap environments

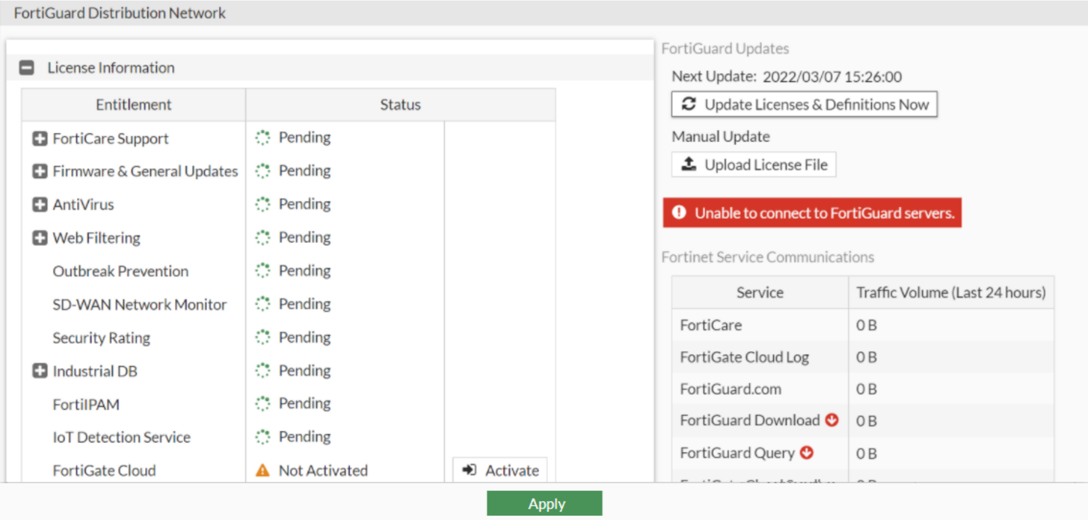
In the Operational Technology industry, industrial equipment is critical and must not be connected to the internet. However, the equipment is still required to be protected by a firewall in this air-gap environment. Without a gateway to

FortiGuard in air-gap environments, FortiGuard packages, such as AntiVirus and IPS, must be manually uploaded to the FortiGate. FortiGate licenses can be downloaded from FortiCloud and uploaded manually to the FortiGate.

Manual licensing for air-gap environments is supported only on FortiGate hardware appliances, for both rugged and non-rugged models running FortiOS 7.2.0 or later. Manual licensing is currently not supported on FortiGate virtual machine (VM) appliances.

To manually upload FortiGate licenses in the GUI:

1. Register the FortiGuard license on FortiCloud. See Registration in the FortiOS Administration Guide for more information.
2. Download the product entitlement file in FortiCloud:
   a. Go to *Products > Product List*.
   b. Select the serial number of the FortiGate. The product page opens.
   c. In the *License & Key* section, click *Get The License File*. The file downloads to your device in the format `FG201E*********ProductEntitlement.lic`.
3. In FortiOS, go to *System > FortiGuard*. Currently, the status for all services is *Pending*.


FortiGuard Distribution Network
License Information
FortiGuard Updates
Update Licenses & Definitions Now
Manual Update
Upload License File
Fortinet Service Communications
Activate
Apply

Next Update: 2022/03/07 15:26:00

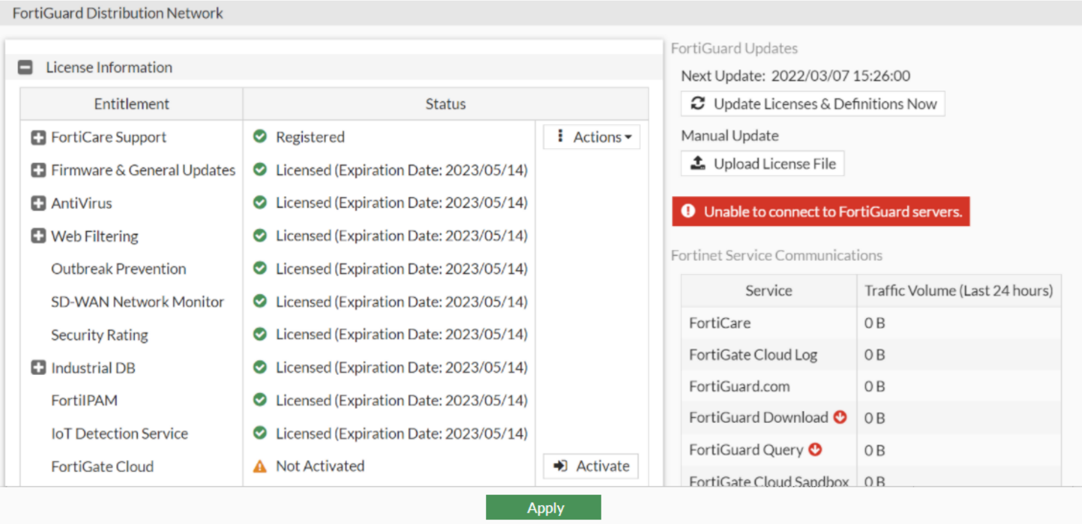
Unable to connect to FortiGuard servers.

Entitlement	Status	
FortiCare Support	Pending	
Firmware & General Updates	Pending	
AntiVirus	Pending	
Web Filtering	Pending	
Outbreak Prevention	Pending	
SD-WAN Network Monitor	Pending	
Security Rating	Pending	
Industrial DB	Pending	
FortiIPAM	Pending	
IoT Detection Service	Pending	
FortiGate Cloud	⚠ Not Activated	Activate

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiGate Cloud Log	0 B
FortiGuard.com	0 B
FortiGuard Download	0 B
FortiGuard Query	0 B

4. Click *Upload License File*. The file explorer opens.
5. Navigate to the product entitlement file and click *Open*.

   The license file uploads to the FortiGate. Once the upload is complete, the FortiGate shows that it is registered and licensed.


FortiGuard Distribution Network
License Information
Actions
Activate
FortiGuard Updates
Update Licenses & Definitions Now
Manual Update
Upload License File
Unable to connect to FortiGuard servers.
Fortinet Service Communications
Apply

Entitlement	Status
FortiCare Support	Registered
Firmware & General Updates	Licensed (Expiration Date: 2023/05/14)
AntiVirus	Licensed (Expiration Date: 2023/05/14)
Web Filtering	Licensed (Expiration Date: 2023/05/14)
Outbreak Prevention	Licensed (Expiration Date: 2023/05/14)
SD-WAN Network Monitor	Licensed (Expiration Date: 2023/05/14)
Security Rating	Licensed (Expiration Date: 2023/05/14)
Industrial DB	Licensed (Expiration Date: 2023/05/14)
FortiIPAM	Licensed (Expiration Date: 2023/05/14)
IoT Detection Service	Licensed (Expiration Date: 2023/05/14)
FortiGate Cloud	Not Activated

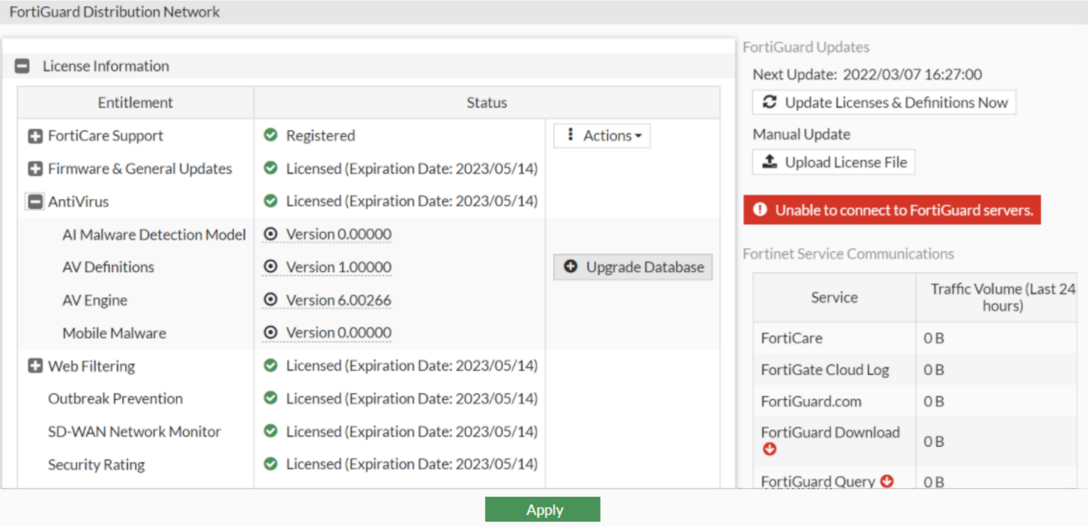
Next Update: 2022/03/07 15:26:00

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiGate Cloud Log	0 B
FortiGuard.com	0 B
FortiGuard Download	0 B
FortiGuard Query	0 B
FortiGate Cloud Sandbox	0 B

6. Click *Apply*.

To manually upgrade the AntiVirus Database in the GUI:

1. Download the static upgrade file from FortiCloud:
   a. Go to support.fortinet.com.
   b. Go to *Download > Download FortiGuard Service Updates > FortiGate*.
   c. Select the FortiOS version from the *OS Version* dropdown.
   d. Select the file from the appropriate FortiGate product model section. The file downloads to your device.
2. In FortiOS, go to *System > FortiGuard* and expand the *AntiVirus* section to view the current licenses.


FortiGuard Distribution Network
License Information
Actions
Upgrade Database
FortiGuard Updates
Update Licenses & Definitions Now
Manual Update
Upload License File
Unable to connect to FortiGuard servers.
Fortinet Service Communications
Apply

Entitlement	Status
FortiCare Support	Registered
Firmware & General Updates	Licensed (Expiration Date: 2023/05/14)
AntiVirus	Licensed (Expiration Date: 2023/05/14)
AI Malware Detection Model	Version 0.00000
AV Definitions	Version 1.00000
AV Engine	Version 6.00266
Mobile Malware	Version 0.00000
Web Filtering	Licensed (Expiration Date: 2023/05/14)
Outbreak Prevention	Licensed (Expiration Date: 2023/05/14)
SD-WAN Network Monitor	Licensed (Expiration Date: 2023/05/14)
Security Rating	Licensed (Expiration Date: 2023/05/14)

Next Update: 2022/03/07 16:27:00

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiGate Cloud Log	0 B
FortiGuard.com	0 B
FortiGuard Download	0 B
FortiGuard Query	0 B

3. Click *Upgrade Database*. The *Anti-Virus Database Upgrade* pane opens.
4. Click *Upload*. The file explorer opens.
5. Navigate to the static upgrade file and click *Open*.
6. Click *OK*.
7. Click *Apply*.

   The AntiVirus Database is upgraded.

To manually upload FortiGate licenses in the CLI:

```
# execute restore manual-license {ftp | tftp} <license file name> <server> [args]
```

Index

The following index provides a list of all new features added to FortiOS 7.2. The index allows you to quickly identify the version where the feature first became available in FortiOS.

Select a version number to navigate in the index to the new features available for that patch:

7.2.0

GUI

Security Fabric

Network

System

Policy & Objects

Security Profiles

VPN

User & Authentication

Secure Access

Log & Report

Cloud

Operational Technology

7.2.1

GUI

Security Fabric

Network

System

Policy & Objects

Security Profiles

User & Authentication

Secure Access

Log & Report

Cloud

7.2.4

Security Fabric

Network

System

Policy & Objects

Security Profiles

User & Authentication

Secure Access

Log & Report

Cloud

7.2.5

Network

System

Security Profiles

VPN

Secure Access

Cloud

www.fortinet.com