

# Fortigate Firewalls

All about Fortinet, Firewall and other stuff of the daily work with the products.

- Design
- Operation
  - Using the save option "set cfg-save revert" to automatically reboot and revert to a previous configuration of a FortiGate
  - Backup Configuration
  - Useful CLI commands FortiOS
- Troubleshooting
  - Wrong DNS Server used by random clients
- Links & Tools
  - Access to Demo Fortinet Appliances
  - Fortinet Blog Links

# Design

# Operation

# Using the save option "set cfg-save revert" to automatically reboot and revert to a previous configuration of a FortiGate

## Description

“ This article describes the system global option "**set cfg-save revert**" that can be used during remote changes on a Fortigate and where the operator would like an automatic revert to the previous configuration in case of problems arise (if for example the connection to the FortiGate is lost).

## Solution

The global setting parameter "set cfg-save" dictates the way that configuration changes applied on the FortiGate are saved:

```
FGT# config system global
```

```
FGT# (global) # set cfg-save ?
```

automatic    automatically save config

manual       manually save config

revert       manually save config and revert the config when timeout

- The default setting is "**automatic**" : in this mode, any changes applied after an "end" or "Apply" will be saved.

- If set to "**revert**", an additional global parameter is required, which is the timeout in seconds : "**set cfg-revert-timeout**"

**Once this is applied, any new changes must be saved manually with the command "execute cfg save" within the period of the timeout, otherwise the FortiGate will reboot.**

A warning CLI message will be displayed 10s before the reboot :

```
FGT # System will reboot if no input is received in the next 10 seconds...
System will reboot if no input is received in the next 9 seconds...
System will reboot if no input is received in the next 8 seconds...
System will reboot if no input is received in the next 7 seconds...
```

Example :

This example explains the use of the **cfg-save revert** command and its associated event log Fortigate Restarted when newly added configuration is not confirmed.

```
FG100D_Primary (global) # set cfg-save
automatic   Automatically save config.
manual      Manually save config.
revert      Manually save config and revert the config when timeout.
```

```
FG100D_Primary (global) # show full-configuration | grep cfg
set cfg-save automatic
```

```
FG100D_Primary (global) # show full-configuration | grep cfg
set cfg-save revert    <<--- Changed from automatic to revert
set cfg-revert-timeout 600 <<--- (10 Minutes)
```

```
FG100D_Primary (lan) # set role
lan      Connected to local network of endpoints.
wan      Connected to Internet.
dmz      Connected to server zone.
undefined Interface has no specific role.
```

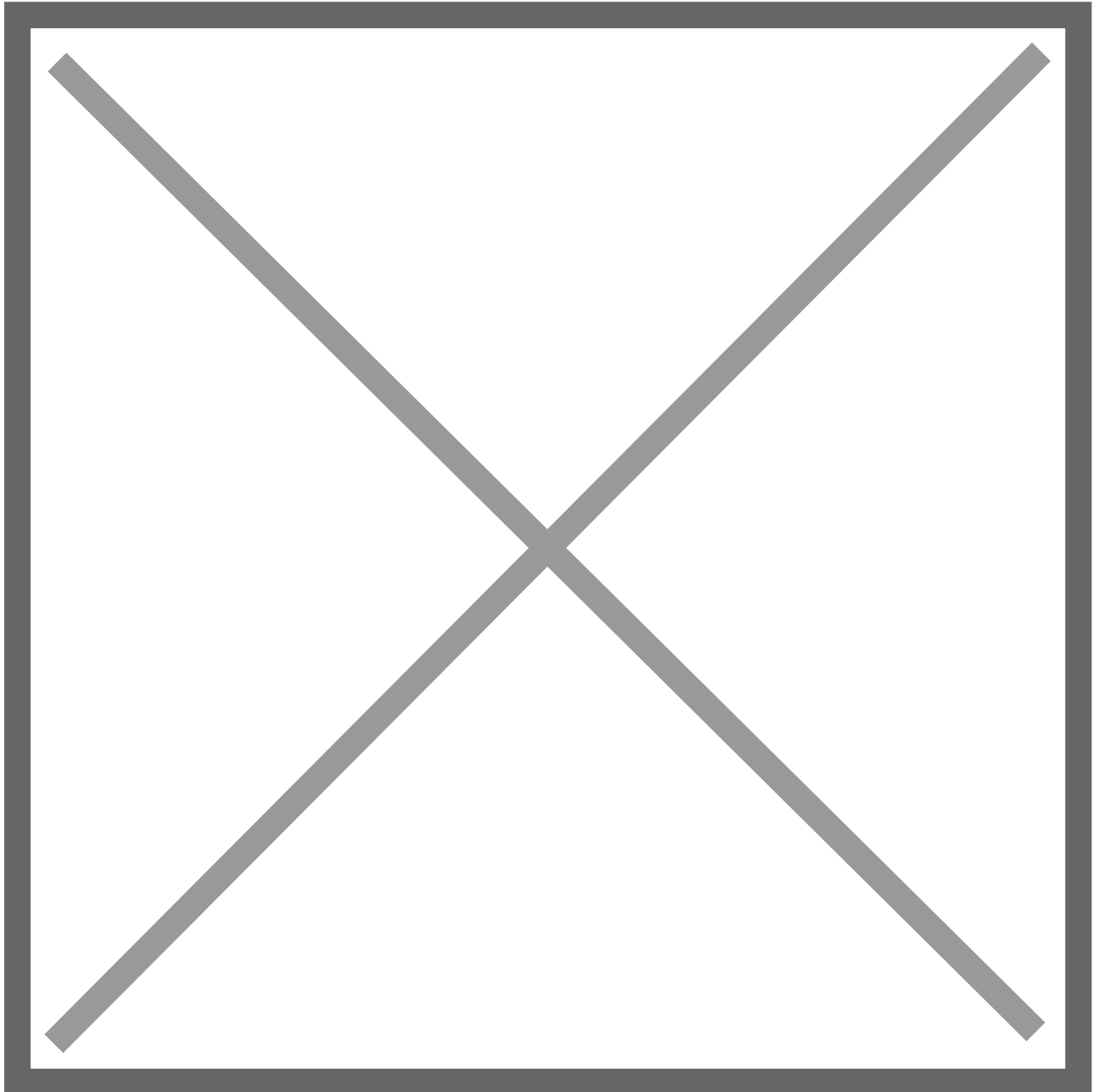
```
FG100D_Primary (lan) # set role lan <<-- Added a new role to the LAN interface configuration in order to
generate a new change in the current configuration.
FG100D_Primary (lan) # end
```

```
FG100D_Primary (lan) # show full-configuration | grep role
```

```
set role lan <<-- New configuration added to interface
```

```
FG100D_Primary (lan) # show full-configuration | grep role
```

```
set role undefined <<-- The newly added configuration of role on the interfaces was never added to the current configuration due to the "timeout" of 600 seconds, (10 Minutes) expired and the newly added configuration was never confirmed generating the event log "Fortigate Restarted" under system events.
```





# Backup Configuration

## Backing up the configuration

### Using the GUI

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Backup*.
2. Direct the backup to your *Local PC* or to a *USB Disk*.  
The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
3. If VDOMs are enabled, indicate whether the scope of the backup is the entire FortiGate configuration (*Global*) or only a specific VDOM configuration (*VDOM*).  
If backing up a VDOM configuration, select the VDOM name from the list.
4. Enable *Encryption*. Encryption must be enabled on the backup file to back up VPN certificates.
5. Enter a password, and enter it again to confirm it. This password will be required to restore the configuration.
6. Click *OK*.
7. When prompted, select a location on the PC or USB disk to save the configuration file. The configuration file will have a .conf extension.

### Using the CLI

Use one of the following commands:

```
execute backup config management-station <comment>
```

or:

```
execute backup config usb <backup_filename> [<backup_password>]
```

### FTP

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>] [<password>]
```

### TFTP

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```



# VDOM

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom  
  
edit <vdom_name>
```

## Using REST-API

REST-API user must have write access to FortiGate and VDOM

### Create access profile

```
FGT # config system accprofile  
FGT (accprofile) # edit readOnly  
new entry 'readOnly' added  
FGT (readOnly) # set sysgrp read  
FGT (readOnly) # end
```

### Create API user in FortiGate

```
FGT # config system api-user  
FGT (api-user) # edit api-admin  
new entry 'api-admin' added  
FGT (api-admin) # set accprofile "readOnly"  
FGT (api-admin) # set vdom root  
FGT (api-admin) # config trusthost  
FGT (trusthost) # edit 1  
new entry '1' added  
FGT (1) # set ipv4-trusthost 'ip_address_of_your_machine' 255.255.255.255  
FGT (1) # end  
FGT (api-admin) # end
```

### Generate API Token

```
FGT # execute api-user generate-key api-admin  
New API key: 'your_api_token'
```

NOTE: The bearer of this API key will be granted all access privileges assigned to the api-user api-admin.

## Get the backup

```
HOSTNAME=<hostname>
API_TOKEN=<api-token>
DATE=`date +%F_%T%S`
curl -k -o $HOSTNAME_$DATE.conf -H "Authorization: Bearer $API_TOKEN" \
"https://$HOSTNAME/api/v2/monitor/system/config/backup/?scope=global&access_token=$API_TOKEN"
```

# Restoring a configuration

## Using the GUI

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Restore*.
2. Identify the source of the configuration file to be restored: your *Local PC* or a *USB Disk*. The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
3. Click Upload, locate the configuration file, and click *Open*.
4. Enter the password if required.
5. Click *OK*.

## Using the CLI

```
execute restore config management-station normal 0
```

or:

```
execute restore config usb <filename> [<password>]
```

## FTP

```
execute restore config ftp <backup_filename> <ftp_server> [<port>] [<user_name>] [<password>]
```

## TFTP

```
execute restore config tftp <backup_filename> <tftp_server> <password>
```

The FortiGate will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

# Useful CLI commands

## FortiOS

### Cheatsheets

- FortiOS 6.2 CheatSheet (<https://blog.boll.ch/cheatsheet-fortios-version-6-2/>)
- FortiOS 7.0 CheatSheet (<https://blog.boll.ch/cheatsheet-fortios-7-0/>)
- FortiOS 7.2 CheatSheet (<https://blog.boll.ch/cheatsheet-fortios-v7-2/>)

### CLI Commands

To start a transaction in CLI use ***execute config-transaction start.***

A workspace mode transaction times out in five minutes if there is no activity. When a transaction times out, all changes are discarded

Commit config changes with ***execute config-transaction commit.***  
Abort with ***execute config-transaction abort.***

### Generic Commands

#### Default Device Information

<b>admin / no password</b>	Default login
<b>192.168.1.99</b>	Default IP on port1, internal or management port
<b>9600/8-N-1, hw flow control disabled</b>	Default serial console settings

#### General system commands

<b>get system status</b>	General system information
--------------------------	----------------------------

<b>exec tac support</b>	Generates report for support
<b>tree</b>	List all commands
<b>&lt;command&gt; ? / tab</b>	Use ? or tab in CLI for help
<b>&lt;command&gt;   grep [filter]</b>	Grep commands to filter output

## Fortigate most used ports

<b>UDP/53, UDP/8888</b>	Fortiguard Queries
<b>TCP/389, UDP/389</b>	LDAP, PKI Authentication
<b>TCP/443</b>	Contract Validation, FortiToken, Firmware Updates
<b>TCP/443, TCP/8890</b>	AV and IPS Update
<b>UDP/500, ESP</b>	IPSEC VPN
<b>UDP/500, UDP/4500</b>	IPSEC VPN with NAT-Traversal
<b>TCP/514</b>	FortiManager, FortiAnalyzer
<b>TCP/1812, TCP/1813</b>	RADIUS Auth & Accounting
<b>UDP/5246, UDP/5247</b>	CAPWAP
<b>TCP/8001</b>	FSSO
<b>TCP/8013</b>	Compliance and Security Fabric
<b>ETH Layer 0x8890, 0x8891 and 0x8893</b>	HA Heartbeat For HA The virtual MAC address is determined based on following formula: 00-09-0f-09-<group-id_hex>-(<vcluster_integer> + <idx>)

## Network commands

### Interface information

<b>diag ip address list</b>	List of IP addresses on FortiGate interfaces
<b>diag firewall iplist list</b>	List of IP addresses on VIP and IP-Pools

## Security Fabric

<b>diag sys csf upstream / downstream</b>	List of up/downstream devices
<b>diag sys csf neighbor list</b>	MAC/IP list of connected FG devices
<b>diag automation test &lt;stich_name&gt;</b>	Test stitches in the CLI
<b>diag test appl csfd 1 ...</b>	Display security fabric statistics
<b>diag debug appl csfd -1</b>	Real-time debugger

## Switch Controller

<b>diag switch-controller switch-info mac-table</b>	Managed FortiSwitch MAC address list
<b>diag switch-controller switch-info port-stats</b>	Managed FortiSwitch port statistics
<b>diag switch-controller switch-info trunk</b>	Trunk information
<b>diag switch-controller switch-info mclag</b>	Dumps MCLAG related information from FortiSwitch
<b>execute switch-controller get-conn-status</b>	Get FortiSwitch connection status
<b>execute switch-controller diagnose-connection</b>	Get FortiSwitch connection diagnostics

## SD-WAN

<b>diag sys virtual-wan-link member</b>	Provide interface details
<b>diag sys virtual-wan-link health-check &lt;name&gt;</b>	State of SLAs
<b>diag sys virtual-wan-link service &lt;rule-id&gt;</b>	SD-WAN rule state
<b>diag sys virtual-wan-link intf-sla-log &lt;intf-name&gt;</b>	Link Traffic History
<b>diag sys virtual-wan-link sla-log &lt;sla&gt; &lt;link_id&gt;</b>	SLA-Log on specific interface
<b>diag test application lnmtd 1/2/3</b>	Statistics of link-monitor
<b>diag debug application link- monitor -1</b>	Real-time debugger of link-monitor

## Network Troubleshooting

<b>get hardware nic [port]</b>	Interface information
<b>get system arp</b> <b>get system arp   grep x.x.x.x</b> <b>diag ip arp list</b>	ARP table
<b>exec clear system arp table</b>	Clears ARP table
<b>exec ping x.x.x.x</b> <b>exec ping-options [option]</b>	Ping utility
<b>exec traceroute x.x.x.x</b> <b>exec traceroute-options [option]</b>	Traceroute utility
<b>exec telnet x.x.x.x [port]</b>	Telnet utility
<b>exec dhcp lease-list</b>	Show DHCP Leases
<b>diag traffictest server-intf</b> <b>diag traffictest client-intf</b> <b>diag traffictest port [port]</b> <b>diag traffictest run -c [public_iperf_server_ip]</b>	Iperf test directly run from FortiGate

## Transparent Mode

<b>diag netlink brctl</b>	Bridge MAC table
---------------------------	------------------

## Routing

### Routing troubleshooting

<b>get router info routing-table all</b>	Show routing table
<b>get router info routing-table details x.x.x.x</b>	Show routing decision for specified destination-IP
<b>get router info routing-table database</b>	Routing table with inactive routes
<b>get router info kernel</b>	Forwarding information base
<b>diag firewall proute list</b>	List of policy-based routes
<b>diag ip rtcache list</b>	List of route cache
<b>exec router restart</b>	Restart of routing process
<b>diag sys link-monitor status/interface/launch</b>	Show link monitor status / per interface / for WAN LB

## BGP

<b>get router info bgp summary</b>	BGP summary of BGP status
<b>get router info bgp neighbors</b>	Information of BGP neighbors
<b>diag ip router bgp all enable</b> <b>diag ip router bgp level info</b>	Real-time debugging for BGP protocol
<b>exec router clear bgp all</b>	Restart of BGP session

## OSPF

<b>get router info ospf status</b>	OSPF status
<b>get router info ospf interface</b>	Information on OSPF interfaces
<b>get router info ospf neighbor</b>	Information on OSPF neighbors
<b>get router info ospf database brief / router lsa</b>	Summary / Details of all LSDB entries
<b>get router info ospf database self-originate</b>	Information on LSAs originating from FortiGate
<b>diag ip router ospf all enable</b> <b>diag ip router ospf level info</b>	Real-time debugging of OSPF protocol
<b>exec router clear ospf process</b>	Restart of OSPF session

## VPN

<b>diag debug appl ike 63</b>	Debugging of IKE negotiation
-------------------------------	------------------------------

<b>diag vpn ike log filter</b>	Filter for IKE negotiation output
<b>diag vpn ike gateway list</b>	Phase 1 state
<b>diag vpn ike gateway flush</b>	Delete Phase 1
<b>diag vpn tunnel list</b>	Phase 2 state
<b>diag vpn tunnel flush</b>	Delete Phase 2
<b>get vpn ike gateway</b>	Detailed gateway information
<b>get vpn ipsec tunnel details</b>	Detailed tunnel statistics
<b>get vpn ipsec tunnel summary</b>	Detailed tunnel information
<b>diag vpn ipsec status</b>	Shows IPSEC crypto status
<b>show full vpn certificate local</b>	Export all keys and certs

# Troubleshooting



# Wrong DNS Server used by random clients

## Problem

Fortigate VPN users reporting that they cannot connect to internal resources anymore. When you check the client the internal host is reachable by IP but it appears that windows isn't using the internal DNS server to resolve the host name. A check with nslookup was working when testing this on the VPN client.

## Solution

the clients having issues were using IPV6 and learned about this feature in Windows call "Smart Multi-Homed Name Resolution". It sounds like Windows will forward a DNS query to both the IPV6 and IPV4 DNS servers and use the first response.

Adding a regkey to disable the parallel queries and the issue cleared.

Go to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

- If the Dword value DisableParallelAandAAAA exists already, make sure its value is set to 1.
- If the value does not exist, right-click on Parameters, and select New > Dword (32-bit) Value.
- Name it DisableParallelAandAAAA.
- Set the value of the Dword to 1. You can turn the feature back on by setting the value to 0, or by deleting the value.

## Link

<https://forum.fortinet.com/tm.aspx?m=190334>

# Links & Tools

# Access to Demo Fortinet Appliances

Fortinet offers for most appliances a demo access.

You can use the following as an example:

Product	URL	Login
Authenticator	<a href="https://fortiauthenticator.fortidemo.com">https://fortiauthenticator.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
WEB Security	<a href="https://fortiweb.fortidemo.com">https://fortiweb.fortidemo.com</a>	demo / demo
MAIL Security	<a href="https://fortimail.fortidemo.com/admin">https://fortimail.fortidemo.com/admin</a>	demo / demo
Firewall	<a href="https://fortigate.fortidemo.com">https://fortigate.fortidemo.com</a>	demo / demo
FortiGate SD-WAN Demo	<a href="https://fortigate-sdwan.fortidemo.com">https://fortigate-sdwan.fortidemo.com</a>	demo / demo
Switching LAN	<a href="https://fortiswitch.fortidemo.com">https://fortiswitch.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
FortiSwitch as Standalone	<a href="https://lanedge.fortidemo.com">https://lanedge.fortidemo.com</a>	demo / demo
FortiSwitch managed by FortiGate	<a href="https://lanedge.fortidemo.com">https://lanedge.fortidemo.com</a>	demo / 40Network!
VoIP Switching	<a href="https://fortivoice.fortidemo.com">https://fortivoice.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
DDOS Protection	<a href="https://fortiddos.fortidemo.com">https://fortiddos.fortidemo.com</a>	demo / demo
Device Management	<a href="https://fortimanager.fortidemo.com">https://fortimanager.fortidemo.com</a>	demo / demo

Log Analyzer	<a href="https://fortianalyzer.fortidemo.com">https://fortianalyzer.fortidemo.com</a>	demo / demo
FortiPortal (MSSP Solution for FortiManager / FortiAnalyzer)	<a href="https://fortiportal.fortidemo.com">https://fortiportal.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
FortiEMS (FortiClient Endpoint Management Server)	<a href="https://fctems.fortidemo.com">https://fctems.fortidemo.com</a>	corp\demo / Fortinet1
Recorder and Surveillance	<a href="https://fortirecorder.fortidemo.com">https://fortirecorder.fortidemo.com</a>	demo / demo
Sandbox	<a href="https://fortisandbox.fortidemo.com">https://fortisandbox.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
Security Information and Event Management (SIEM)	<a href="https://fortisiem.fortidemo.com">https://fortisiem.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
Wireless Access Point	<a href="https://fortiap.fortidemo.com">https://fortiap.fortidemo.com</a>	demo / demo
Proxy	<a href="https://fortiproxy.fortidemo.com">https://fortiproxy.fortidemo.com</a>	demo / demo
Application Delivery Controller (ADC)	<a href="https://fortiadc.fortidemo.com">https://fortiadc.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
Virtual Security Analyst	<a href="https://fortiai.fortidemo.com">https://fortiai.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>
Deception-based Solution	<a href="https://fortideceptor.fortidemo.com">https://fortideceptor.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>

Security, Orchestration, Automation and Response Solution	<a href="https://fortisoar.fortidemo.com">https://fortisoar.fortidemo.com</a>	demo / demo But it shows error: "FSR-Auth-043: Login denied as all concurrent user seats are currently in use. Please wait or contact the administrator for access."
Network Tester	<a href="https://fortitester.fortidemo.com">https://fortitester.fortidemo.com</a>	demo / demo
Wireless Manager	<a href="https://fortiwlm.fortidemo.com">https://fortiwlm.fortidemo.com</a>	demo / demo
Carrier Grade NAT (CGN)	<a href="https://forticarrier.fortidemo.com">https://forticarrier.fortidemo.com</a>	Unknown Request credentials here: <a href="https://www.fortinet.com/demo-center">https://www.fortinet.com/demo-center</a>

# Fortinet Blog Links

## Fortigate Blog

<https://yurisk.info/category/fortigate.html>

## Fortinet Blog

- <https://yurisk.info/category/fortinet.html>
- <https://troublenet.de/category/fortinet/>