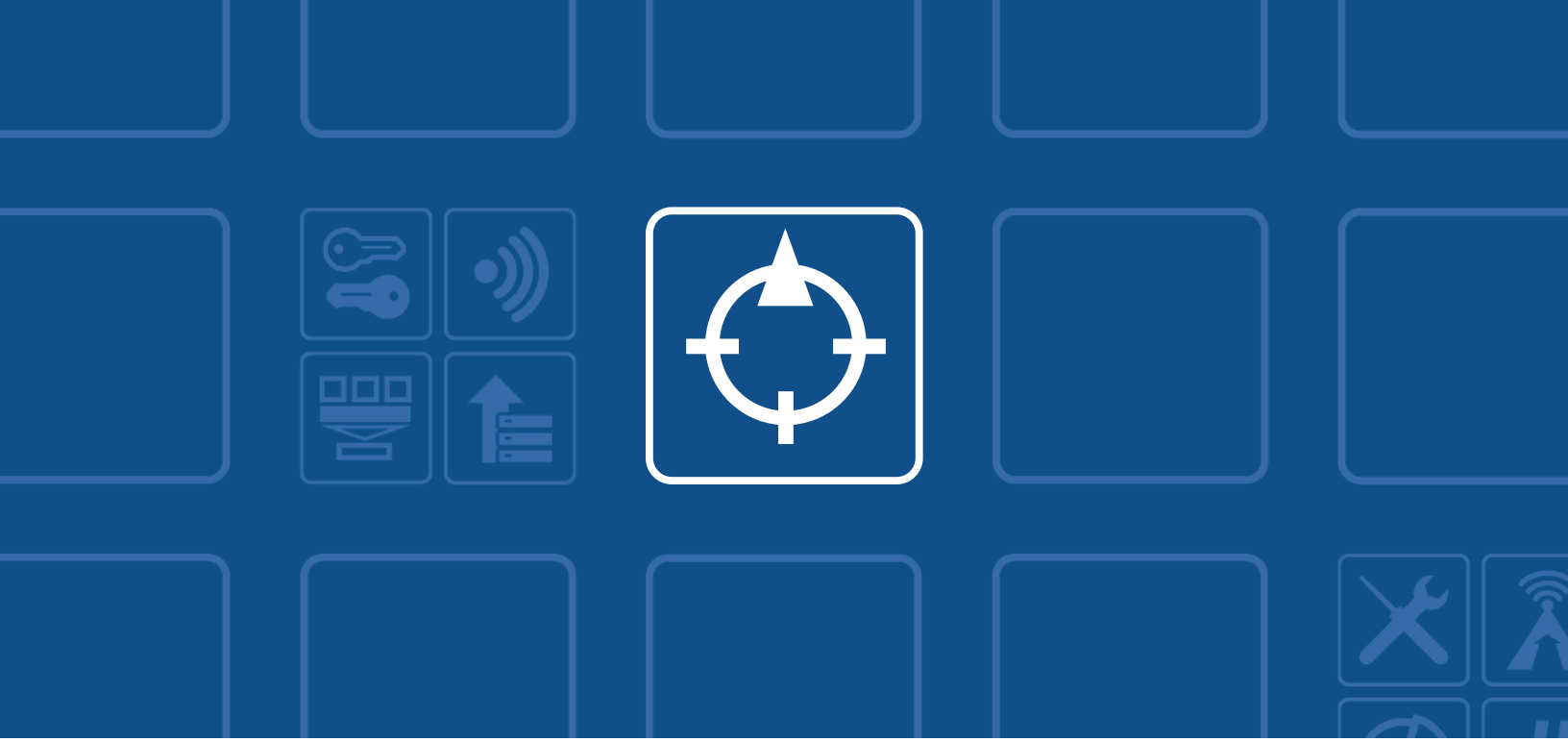
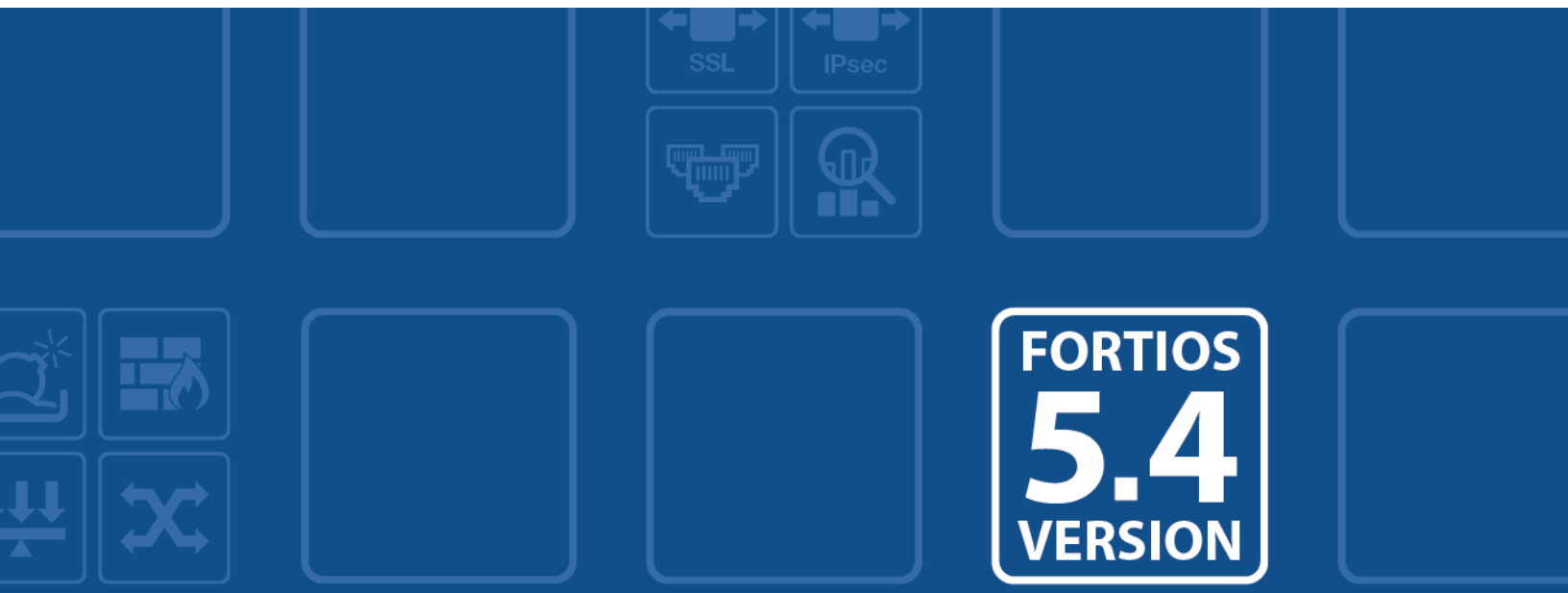


FORTINET
High Performance Network Security

FortiOS™ Handbook - Open Ports

VERSION 5.4.0



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, May 18, 2016

FortiOS™ Handbook - Open Ports

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-04-28	Initial release.

FortiGate Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiAuthenticator	RADIUS	TCP/1812
	FSSO	TCP/8000
FortiGate	HA Heartbeat	TCP/703, TCP/23, or ETH Layer 2/8890
FortiGuard	Management	TCP/541
	AV/IPS	UDP/9443
FortiManager	AV/IPS Push	UDP/9443
	SSH CLI Management	TCP/22
	Management	TCP/541
	SNMP Poll	UDP/161, UDP/162
	FortiGuard Queries	TCP/443
Others	Web Admin	TCP/80, TCP/443
	FSSO	TCP/8000
	Policy Override Authentication	TCP/443, TCP/8008
	FortiClient Portal	TCP/8009
	Policy Override Keepalive	TCP/1000, TCP/1003
	SSL VPN	TCP/10443
3rd-Party Servers	FSSO	TCP/8000

Outgoing Ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	IPsec Secure SNMP	UDP/500, UDP/4500
FortiAuthenticator	LDAP, PKI Authentication	TCP or UDP/389
FortiCloud	Registration, Quarantine, Log & Report, Syslog	TCP/443
	OFTP	TCP/514
	Management	TCP/541
	Contract Validation	TCP/10151
FortiGate	HA Heartbeat	TCP/703, TCP/23, or ETH Layer 2/8890
FortiGuard	AV/IPS Update	TCP/443
	Cloud App DB	TCP/9582
	FortiGuard Queries	UDP/53, UDP/8888
	DNS	UDP/53, UDP/8888
	Registration	TCP/80
	Alert Email, Virus Sample	TCP/25
	Management, Firmware, SMS, FTM, Licensing, Policy Override	TCP/443
	Central Management, Analysis	TCP/541
FortiManager	Management	TCP/541
	Log & Report	TCP or UDP/514
	Secure SNMP	UDP/161, UDP/162
	FortiGuard Queries	TCP/8890, UDP/53
FortiSandbox	OFTP	TCP/514

Note that, while a proxy is configured, FortiGate uses the following URLs to access the FortiGuard Distribution Network (FDN):

- update.fortiguard.net
- service.fortiguard.net
- support.fortiguard.com

FortiAnalyzer Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiAP-S	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiClient	Syslog	UDP/514
FortiManager	Syslog & OFTP	TCP/514, UDP/514
	Registration	TCP/541
Others	SSH CLI Management	TCP/22
	Web Admin	TCP/80, TCP/443
	REST	TCP/443
	DC Polling	TCP/445
	Logg Agg	TCP/3000
	MySQL	TCP/3306

Outgoing Ports table		
Purpose		**Protocol/Port**
FortiGuard	AV/IPS, SMS, FTM, Licensing, Policy Override, RVS, URL/AS Update	TCP/443

Outgoing Ports table		
Purpose		**Protocol/Port**
3rd-Party Servers	LDAP & PKI Authentication	TCP/389, UDP/389
	Log & Report	TCP/21, TCP/22
	Configuration Backups	TCP/22
	Alert Email	TCP/25
	DNS	UDP/53
	NTP	UDP/123
	SNMP Traps	UDP/162
	Report Query	TCP/389
	Syslog & OFTP	TCP OR UDP/514
	RADIUS	TCP/1812

FortiAP-S Open Ports

Outgoing Ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiCloud	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiGate	CAPWAP	UDP/527, UDP/5246
FortiGuard	FortiGuard Queries	UDP/53, UDP/8888
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246

FortiAuthenticator Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiClient	SSO Mobility Agent, FSSO	TCP/8001
FortiGate	LDAP, PKI Authentication	TCP or UDP/389
	RADIUS	TCP/1812
	FSSO	TCP/8000
Others	SSH CLI	TCP/22
	Telnet	TCP/23
	HTTP & SCEP	TCP/80
	SNMP Poll	UDP/161
	Web Admin	TCP/80, TCP/443
	LDAP	TCP/389
	LDAPS	TCP/636
	RADIUS	TCP/1812, TCP/1813
	OCSP	TCP/2560
3rd-Party Servers	FSSO & Tiers	TCP/8002, TCP/8003

Outgoing Ports		
Purpose		**Protocol/Port**
FortiGate	RADIUS	TCP/1812
	FSSO	TCP/8000

Outgoing Ports		
Purpose		**Protocol/Port**
FortiGuard	AV/IPS Updates	TCP/443
	Virus Sample	TCP/25
	SMS, FTM, Licensing, Policy Override Authentication, URL/AS Updates	TCP/443
	Registration	TCP/80
3rd-Party Servers	SMTP, Alerts, Virus Sample	TCP/25
	DNS	UDP/52
	Windows AD	TCP/88
	NTP	UDP/123
	LDAP	TCP or UDP389
	Domain Control	TCP/445
	LDAPS	TCP/636
	FSSO & Tiers	TCP/8002, TCP/8003

FortiClient Open Ports

Outgoing Ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog	UDP/514
FortiAuthenticator	SSO Mobility Agent, FSSO	TCP/8001
FortiGate	VPN Settings	TCP/8900
	Policy Override Authentication	TCP/8010
	Explicit Proxy	TCP/8080
FortiGuard	AV Update & Registration	TCP/80
	URL/AS Rating, DNS, FDN, FortiGuard Queries	UDP/53, UDP/8888
FortiManager	FortiGuard Queries	UDP/53, UDP/8888

FortiCloud Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiAP-S	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiGate	Registration, Quarantine, Log & Report, Syslog	TCP/443
	OFTP	TCP/514
	Management	TCP/541
	Contract Validation	TCP/10151

Outgoing Ports		
Purpose		**Protocol/Port**
FortiGuard	Registration	TCP/443

FortiDB Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
Others	SSH CLI Management	TCP/22
	Telnet CLI Management	TCP/23
	Web Admin	TCP/80, TCP/443
	SNMP Traps	UDP/161
	Agent Communication	TCP/9116, TCP/9117

Outgoing Ports		
Purpose		**Protocol/Port**
FortiGuard (FortiDB will use a random port picked by the kernel)	FortiGuard Updates	TCP/80
FortiMonitor	SSH, SFTP	TCP/22
3rd-Party Servers	Email Notifications/Reports	TCP/25
	SNMP Traps	UDP/162
	Syslog	UDP/514

FortiGuard Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiAnalyzer	AV/IPS Updates, SMS, FTM, Licensing, Policy Overrides, RVS, URL/AS Update	TCP/443
FortiAP-S	FortiGuard Queries	UDP/53, UDP/8888
	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
	Event Logs	UDP/5246
FortiAuthenticator	AV/IPS Updates	TCP/443
	Virus Sample	TCP/25
	SMS, FTM, Licensing, Policy Override Authentication, URL/AS Updates	TCP/443
	Registration	TCP/80
FortiClient	AV Update & Registration	TCP/80
	URL/AS Rating, DNS, FDN, FortiGuard Queries	UDP/53, UDP/8888
FortiCloud	Registration	TCP/443
FortiGate	AV/IPS Update, Management, Firmware, SMS, FTM, Licensing, Policy Override	TCP/443
	Cloud App DB	TCP/9582 (flow.fortinet.net)
	FortiGuard Queries, DNS	UDP/53, UDP/8888
	Registration	TCP/80
	Alert Emails, Virus Sample	TCP/25
	Central Management, Analysis	TCP/541

Incoming Ports		
Purpose		**Protocol/Port**
FortiManager	AV/IPS Updates, URL/AS Update, Firmware, SMS, FTM, Licensing, Policy Override Authentication	TCP/443
	Registration	TCP/80
FortiSandbox (FortiSandbox will use a random port picked by the kernel)	FortiGuard Distribution Servers	TCP/8890
	FortiGuard Web Filtering Servers	UDP/53, UDP/8888

Outgoing Ports		
Purpose		**Protocol/Port**
FortiGate	Management	TCP/541
	AV/IPS	UDP/9443
FortiManager	AV/IPS	UDP/9443

FortiManager Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiClient	FortiGuard Queries	UDP/53, UDP/8888
FortiGate	Management	TCP/541
	Log & Report	TCP or UDP/514
	Secure SNMP	UDP/161, UDP/162
	FortiGuard Queries	TCP/8890, UDP/53
FortiGuard	AV/IPS	UDP/9443
FortiManager	FortiClient Manager	TCP/6028
Others	SSH CLI Management	TCP/22
	Telnet CLI Management	TCP/23
	SNMP Traps	UDP/162
	Web Admin	TCP/80, TCP/443

Outgoing Ports		
Purpose		**Protocol/Port**
FortiAnalyzer	Syslog & OFTP	TCP/514, UDP/514
	Registration	TCP/541
FortiGate	AV/IPS Push	UDP/9443
	SSH CLI Management	TCP/22
	Management	TCP/541
	SNMP Poll	UDP/161, UDP/162
	FortiGuard Queries	TCP/443

Outgoing Ports		
Purpose		**Protocol/Port**
FortiGuard	AV/IPS Updates, URL/AS Update, Firmware, SMS, FTM, Licensing, Policy Override Authentication	TCP/443
	Registration	TCP/80
FortiManager	FortiClient Manager	TCP/6028
3rd-Party Servers	DNS	UDP/53
	NTP	UDP/123
	SNMP Traps	UDP/162
	Proxied HTTPS Traffic	TCP/443
	RADIUS	TCP/1812

Note that, while a proxy is configured, FortiManager uses the following URLs to access the FortiGuard Distribution Network (FDN):

- update.fortiguard.net
- service.fortiguard.net
- support.fortiguard.com

FortiSandbox Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiGate	OFTP	TCP/514
Others	SSH CLI Management	TCP/22
	Telnet CLI Management	TCP/23
	Web Admin	TCP/80, TCP/443
	OFTP Communication with FortiGate & FortiMail	TCP/514

Outgoing Ports		
Purpose		**Protocol/Port**
FortiGuard (FortiSandbox will use a random port picked by the kernel)	FortiGuard Distribution Servers	TCP/8890
	FortiGuard Web Filtering Servers	UDP/53, UDP/8888
FortiSandbox Community Cloud (FortiSandbox will use a random port picked by the kernel)	Upload detected malware information	TCP/443

3rd-Party Servers Open Ports

Incoming Ports		
Purpose		**Protocol/Port**
FortiAnalyzer	LDAP & PKI Authentication	TCP/389, UDP/389
	Log & Report	TCP/21, TCP/22
	Configuration Backups	TCP/22
	Alert Emails	TCP/25
	DNS	UDP/53
	NTP	UDP/123
	SNMP Traps	UDP/162
	Report Query	TCP/389
	Syslog & OFTP	TCP or UDP/514
	RADIUS	TCP/1812
FortiAuthenticator	SMTP, Alerts, Virus Sample	TCP/25
	DNS	UDP/52
	Windows AD	TCP/88
	NTP	UDP/123
	LDAP	TCP or UDP/389
	Domain Control	TCP/445
	LDAPS	TCP/636
	FSSO & Tiers	TCP/8002, TCP/8003
FortiManager	DNS	UDP/53
	NTP	NTP/123
	SNMP Traps	UDP/162

Incoming Ports		
Purpose		**Protocol/Port**
	Proxied HTTPS Traffic	TCP/443
	RADIUS	TCP/1812

Outgoing Ports		
Purpose		**Protocol/Port**
FortiAuthenticator	FSSO & Tiers	TCP/8002, TCP/8003
FortiGate	FSSO	TCP/8000

CLI Syntax

This section contains commands to control protocols and ports under various CLI options.

firewall/ldb-monitor

The following command will set the load balancing ports per protocol.

```
config firewall ldb-monitor
   edit <name_str>
      set name <string>
      set type [ping | tcp | http | passive-sip]
      set port <integer>
   end
```

firewall/profile-protocol-options

The following command will set the proxy option profile ports per protocol.

```
config firewall profile-protocol-options
   edit <name_str>
      set name <string>
      config [http | ftp | imap | mapi | pop3 | smtp | nntp | dns | mail-signature]
         edit <name_str>
         set ports <integer>
   end
```

firewall/sniffer

The following command will set the sniffer profile port.

```
config firewall sniffer
   edit <name_str>
      set port <string>
      set protocol <string>
   end
```

firewall/ssl-server

The following command will set and map the SSL server ports.

```
config firewall ssl-server
   edit <name_str>
      set port <integer>
      set mapped-port <integer>
   end
```

firewall/ssl-ssh-profile

The following command will set the SSL-SSH profile ports per protocol.

```
config firewall ssl-ssh-profile
   edit <name_str>
      set name <string>
      config [ssl | https | ftps | imaps | pop3s | smtps | ssh]
         edit <name_str>
```

```
            set ports <integer>   (ssl protocol excluded)
    end
```

firewall/vip

The following command will set the ports to map public and private IP addresses for Destination NAT (DNAT) per protocol.

```
config firewall vip
   edit <name_str>
      set name <string>
      set protocol [tcp | udp | sctp | icmp]
      set mappedport <user>
      set portmapping-type [1-to-1 | m-to-n]
      config realservers
         edit <name_str>
            set port <integer>
         end
   end
```

icap/server

The following command will set the ICAP server port. Note that further configuration is required to add an ICAP profile to an existing security policy.

```
config icap server
   edit <name_str>
      set port <integer>
   end
```

log.syslogd/override-setting

The following command will set the port by which logs can be sent to a remote computer running a syslog server. This command is to be used within a VDOM to override the global configuration created in `config log.syslogd setting`.

```
config log.syslogd override-setting
   edit <name_str>
      set port <integer>
   end
```

log.syslogd/setting

The following command will set the port by which logs can be sent to multiple remote computers running a syslog server.

```
config [log.syslogd | log.syslogd2 | log.syslogd3 | log.syslogd4] setting
   edit <name_str>
      set port <integer>
   end
```

system.autoupdate/push-update

The following command will set the FDN push update port.

```
config system.autoupdate push-update
   edit <name_str>
      set port <integer>
   end
```

system.autoupdate/tunneling

The following command will set the proxy server port that the FortiGate will use to connect to the FortiGuard Distribution Network (FDN).

```
config system.autoupdate tunneling
   edit <name_str>
      set port <integer>
   end
```

system/email-server

The following command will set the SMTP server port that the FortiGate uses to send out alert emails.

```
config system email-server
   edit <name_str>
      set port <integer>
   end
```

system/fortiguard

The following command will set the port by which scheduled FortiGuard service updates will be received.

```
config system fortiguard
   edit <name_str>
      set port [53 | 8888 | 80]
   end
```

system/link-monitor

The following command will set the health link monitor port per protocol.

```
config system link-monitor
   edit <name_str>
      set protocol [ping | tcp-echo | udp-echo | http | twamp]
      set port <integer>
   end
```

system/probe-response

The following command will set the server probe mode that will be used on an interface and its port.

```
config system probe-response
   edit <name_str>
      set mode [none | http-probe | twamp]
      set port <integer>
   end
```

system/session-helper

The following command will set the session helper port per protocol. A session helper binds a service to a TCP or UDP port.

```
config system session-helper
   edit <name_str>
      set protocol <integer>
      set port <integer>
   end
```

system/virtual-wan-link

The following command will set the virtual WAN link health check port per protocol.

```
config system virtual-wan-link
   edit <name_str>
      config health-check
         edit <name_str>
            set protocol [ping | tcp-echo | udp-echo | http | twamp]
            set port <integer>
   end
```

user/fsso

The following command will set the server address, port, and password for multiple FSSO agents.

```
config user fsso
   edit <name_str>
      set name <string>
      set [server | server2 | server3 | server4 | server5] <string>
      set [port | port2 | port3 | port4 | port5] <integer>
      set [password | password2 | password3 | password4 | password5] <password>
   end
```

user/fsso-polling

The following command will set the Active Directory server port.

```
config user fsso-polling
   edit <name_str>
      set port <integer>
   end
```

user/ldap

The following command will set the LDAP server port.

```
config user ldap
   edit <name_str>
      set port <integer>
   end
```

user/pop3

The following command will set the POP3 service port.

```
config user pop3
   edit <name_str>
      set port <integer>
   end
```

user/radius

The following command will set the RADIUS service port and ports for additional accounting servers.

```
config user radius
   edit <name_str>
      set radius-port <integer>
      config accounting-server
         edit <name_str>
```

```
            set port <integer>
        end
    end
```

user/setting

The following command will set the authentication port table for users per protocol.

```
config user setting
   edit <name_str>
      config auth-ports
         edit <name_str>
            set type [http | https | ftp | telnet]
            set port <integer>
         end
   end
```

user/tacacs+

The following command will set the TACACS+ server port.

```
config user tacacs+
   edit <name_str>
      set port <integer>
   end
```

vpn.ssl/settings

The following command will set the SSL VPN access HTTPS port. You can also enable or disable SSL VPN port precedence over the admin GUI HTTPS port.

```
config vpn.ssl settings
   edit <name_str>
      set port <integer>
      set port-precedence [enable | disable]
   end
```

vpn.ssl.web/portal

The following command will set bookmarks for groups of users and their ports.

```
config vpn.ssl.web portal
   edit <name_str>
      config bookmark-group
         edit <name_str>
            config bookmarks
               edit <name_str>
                  set port <integer>
         end
   end
```

vpn.ssl.web/user-bookmark

The following command will set RDP user bookmark ports.

```
config vpn.ssl.web user-bookmark
   edit <name_str>
      config bookmarks
         edit <name_str>
```

```
            set port <integer>
        end
    end
```

wanopt/profile

The following command will set WAN optimization ports per protocol.

```
config wanopt profile
   edit <name_str>
      config [http | cifs | mapi | ftp | tcp]
         edit <name_str>
            set port <integer>
   end
```

web-proxy/forward-server

The following command will set the forward server port.

```
config web-proxy forward-server
   edit <name_str>
      set port <integer>
   end
```

webfilter/fortiguard

The following command will close ports used for HTTPS/HTTP override authentication and disable user overrides:

```
config webfilter fortiguard
   edit <name>
      set close-ports [enable | disable]
   end
```

FORTINET®

High Performance Network Security