

# FortiCore FortiCore Administration Guide v2.0.0

Version 2.0.0

## **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](mailto:techdocs@fortinet.com)

Monday, January 30, 2017

FortiCore FortiCore Administration Guide v2.0.0 Version 2.0.0

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>Introduction</b>	<b>7</b>
FortiCore models	7
How this guide is organized	7
<b>FortiCore Product Overview</b>	<b>8</b>
SDN and NFV	8
Scalability	9
Link Transection	9
Leaf-Spine Architecture	10
SDN Controllers	10
Cardinality	11
Modes of Operation	11
Configuration Example	12
Support for Packet-In and Packet-Out Messages	14
Support for VXLAN and MPLS	14
Virtualization Support	14
<b>OpenDaylight Controller</b>	<b>15</b>
<b>Getting Started</b>	<b>16</b>
Configure the Management Interface	16
Configure the Controller Channel	16
Configure DNS	17
Configure NTP	17
<b>FortiCore Web-based Interface</b>	<b>18</b>
Initial Log-in	18
Main Menu	18
Actions	18
<b>Dashboard</b>	<b>19</b>
System Reboot and Shutdown	19
Firmware Update	19
<b>System Settings</b>	<b>21</b>
Configuring System Settings	21
Maintenance Actions	21
Configuring Time-related Settings	21

Backing up and restoring the configuration.....	22
Updating Firmware using the Web UI.....	23
Services.....	24
Configuring an SMTP Email Server.....	24
<b>System Administrators.....</b>	<b>26</b>
Overview.....	26
Configuring Access Profiles.....	26
Create a Profile.....	26
Per-Profile Actions.....	27
Configuring administrator users.....	27
Per-User Actions.....	28
Using a RADIUS Server.....	28
Create a RADIUS server.....	28
Per-Server Actions.....	29
<b>SNMP Settings.....</b>	<b>30</b>
<b>Networking.....</b>	<b>33</b>
Configuring Network Interfaces.....	33
Configuring Static Routes.....	34
Link Aggregation (i.e., Port Trunking).....	34
LAG CLI Configuration.....	35
Configure Network Interface.....	36
Example: LAG Configuration.....	36
Example: Display LAG Settings.....	37
Port Format in the SDN Flow.....	37
Viewing Port Counters.....	38
<b>OpenFlow.....</b>	<b>39</b>
Configuring the SDN Controller Connection.....	39
Viewing Openflow Counters.....	40
Viewing Openflow Flows.....	40
<b>OVSDB.....</b>	<b>41</b>
OVSDB Support in Forticore.....	41
Configuring OVSDB.....	41
Example.....	42
Displaying OVSDB Channel Configurations.....	42
Example.....	42
Displaying Configuration for Individual Channels.....	43
Example.....	43
Displaying Status of Configured Channels.....	44
Example.....	44
Displaying OVSDB Protocol Counters.....	45
Example.....	45
Example Transact Request.....	46

CMDB to OVSDb Mapping .....	46
<b>Virtualization.....</b>	<b>49</b>
FortiCore Virtualization CLI Commands.....	49
Configuring a Virtual Machine.....	49
Configuring a Virtual Machine Volume.....	50
Configuration Notes.....	50
Starting a Virtual Machine.....	50
Stopping a Virtual Machine.....	50
Importing a Virtual Machine Image.....	50
Getting a List of Virtual Machines.....	50
Getting a List of Virtual Machine Images.....	50
Example Configuration.....	51
<b>VXLAN and MPLS Tunnels.....</b>	<b>52</b>
VXLAN Operation.....	52
Configuring VXLAN.....	52
VXLAN Flows.....	53
MPLS Operation.....	54
Configuring MPLS.....	54
MPLS Flows.....	54
Logical Port Types.....	55
<b>Packet-In and Packet-Out Support.....</b>	<b>56</b>
Packet-In Messages.....	56
Packet-Out Messages.....	56
Displaying Counters.....	57
<b>Logs and Reporting.....</b>	<b>58</b>
Log Browsing.....	58
Log Download.....	58
Configuring Local Log Settings.....	58
Configuring Syslog Settings.....	59
Configuring High Speed Logging.....	60
Configuring Alert Email Settings.....	61

## Change Log

Date	Change Description
2017-01-30	Published content for v2.0.0.

# Introduction

This guide provides information about FortiCore configuration and administration.

## FortiCore models

This guide is applicable to all FortiCore models:

- 3600E – 32x10G
- 3700E – 32x10G + 4x40G (QSFP)
- 3800E – 32x10G + 2x100G (QSFP28)
- 3805E - 32x10G + 2x100G (CFP4)

## How this guide is organized

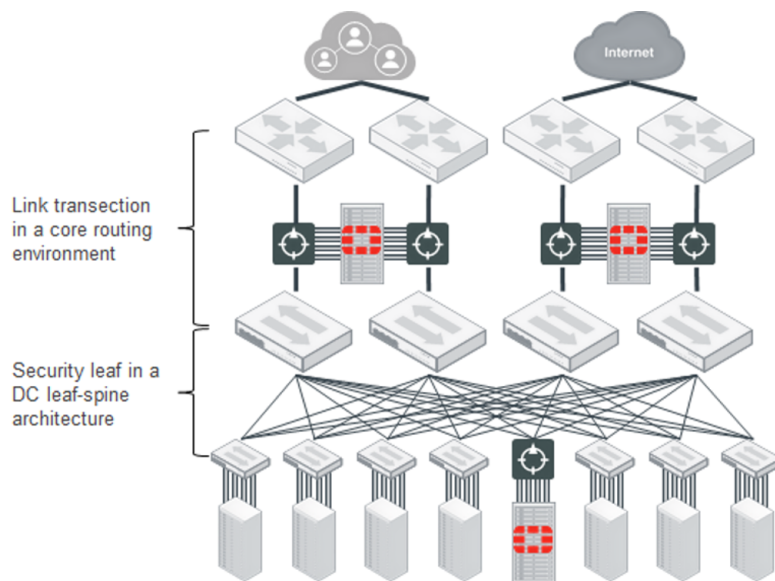
This document contains the following chapters:

- [FortiCore Product Overview](#)
- [Getting Started](#)
- [FortiCore Web-based Interface](#)
- [Dashboard](#)
- [System Settings](#)
- [System Administrators](#)
- [SNMP Settings](#)
- [Networking](#)
- [OpenFlow](#)
- [Virtualization](#)
- [VXLAN and MPLS Tunnels](#)
- [Packet-In and Packet-Out Support](#)
- [Logs and Reporting](#)
- [Troubleshooting](#)

# FortiCore Product Overview

FortiCore is an software-defined networking (SDN) security appliance that enables scalable deployment of network security functions (NSFs). You can deploy FortiCore to provide NSFs in large network topologies such as a routed core or leaf-spine data center network.

In the following diagram of a sample Data Center configuration, the FortiCore devices are highlighted with the red icons.



## SDN and NFV

To separate the network control layer software functions from the forwarding hardware, tier 1 carriers, cloud-based providers, and large data-centers are migrating towards the use of SDN.

SDN uses open protocols (mostly OpenFlow) to program forwarding instructions onto the forwarding-layer hardware. (OpenFlow is a vendor-neutral standard communications interface defined to enable interaction between the control and forwarding layers of an SDN architecture.) Management protocols (such as the OpenStack suite or NETCONF) exist to configure the device management options of the forwarding-layer hardware.

SDN complements Network Function Virtualization (NFV) where we virtualize networking services (including network-based security services) and run on virtual machines within a hypervisor environment. A common set of open protocols are available to control the SDN hardware-based network devices and NFV virtualized networking devices.

FortiCore enables integration of hardware-based and/or virtualized NSFs at a scale that meets core network and datacenter architectural requirements.



## Scalability

Deep-packet inspection of traffic on high-performance 40G & 100G links creates performance requirements that are demanding for a single network security appliance.

Clustering appliances (along with load-balancing) can increase performance compared to a single appliance. Clustering can impose functional limitations on the solution, however, and may offer only simple statistical load-balancing techniques to distribute the traffic.

FortiCore is an inline network appliance that can meet the performance requirements of high speed network links. It can intelligently-shunt traffic-of-interest to a set of associated network security devices to meet aggregate network security and performance requirements.

## Link Transection

In a Link Transection configuration, a FortiCore is inserted between two active networking devices.

FortiCore utilizes SDN-programmed flows to match packets of interest and send them to the associated network security functions (NSF).

Link Transection mode allows the deployment of scalable network-based security and monitoring solutions at any point in the network architecture. This concept of 'network instrumentation' is key to large data center architectures.

### Link Transection – Mobility Carrier GiFW

With rapid growth in the number of mobile devices supported on carrier networks, scalable Gigabit firewalls (GiFW) are necessary to combat mobile malware.

FortiCore can scale to GiFW size, placing GiFW assets near-line to the traffic to maintain low-latency data paths for latency-sensitive applications such as Voice over IP.

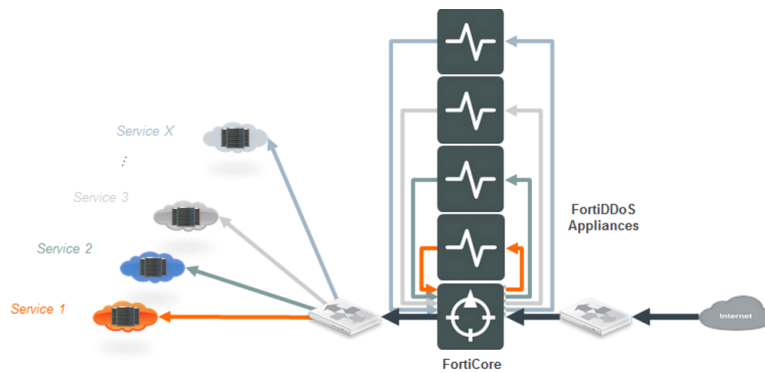
For each Access Point Name (APN), you can apply this solution to FortiGate devices as well as security devices from other vendors.

### Link Transection – DDoS

As DDoS defenses cannot use traditional load-balancing techniques, such defenses are bounded by the performance of individual appliances.

With FortiCore, you can steer the flows for each service to specific FortiDDoS devices. Multiple FortiDDoS devices can serve a common high-performance link, without affecting router configurations. Moreover, you can program exceptions to DDoS inspection to bypass the FortiDDoS devices.

The following figure shows the FortiCore solution for DDoS.

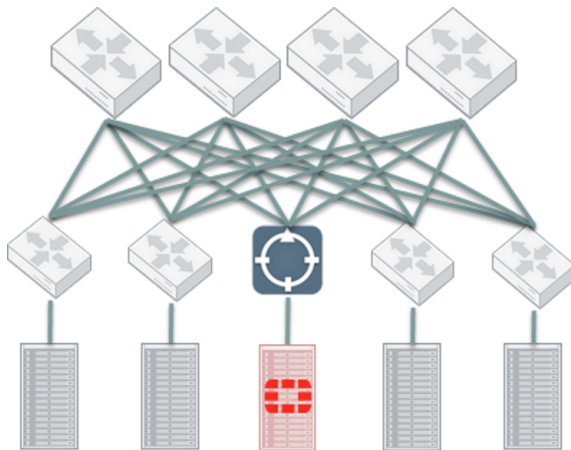


## Leaf-Spine Architecture

In datacenter design, the leaf-spine architecture ensures that all servers are one hop apart, with redundant equal-cost paths. Operating as a special leaf node, FortiCore provide network security functions for the datacenter.

It offers the following advantages in an SDN-enabled data center environment:

- Unknown flows can be forwarded to the FortiCore, rather than to the SDN Controller. The control plane is protected from the effects of DDoS attacks, which would otherwise overload the SDN controller.
- FortiCore can inspect unknown flows (associated NSF's perform the DPI functions), and send inspected flows to the destination node.



## SDN Controllers

The SDN controller is the key element of the SDN control plane.

- The controller receives data from SDN applications and services via its Northbound APIs, and generates flow data to be deployed to the SDN switches.
- The SDN controller can configure and provision the SDN switches (normally using OVSDB protocol)
- The SDN controller can also query SDN switches for operational performance and flow data

FortiCore supports any SDN controller that is compliant with OpenFlow version 1.3. For additional information, see the Open Networking Foundation web site:

<https://www.opennetworking.org/sdn-resources/openflow>

This web site also contains the [OpenFlow version 1.3 specification](#).

Fortinet product testing primarily used the OpenDaylight SDN controller, provided by the Linux Foundation.

## Cardinality

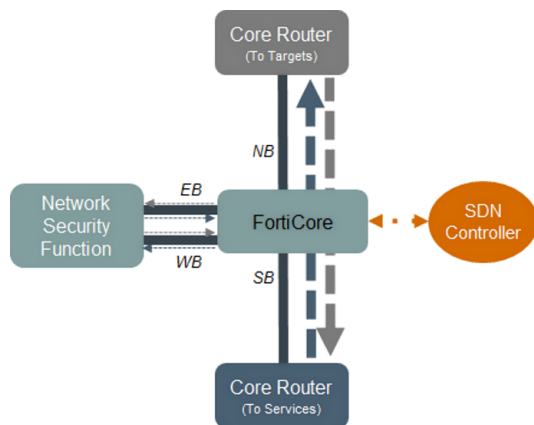
FortiCore hardware provides four flow processing units (FPGA, TCAM, DDR3 memory cache) that can each support 100G of full-duplex traffic processing.

We associate each unit with a cardinal designation (North, East, South, West), analogous to the cardinality associated with datacenter design (for example, North-South traffic and East-West traffic).

The FortiCore uses the cardinal designation to associate interfaces with each processing unit. You configure each interface to be Northbound, Eastbound, Southbound, or Westbound. The incoming flows on an interface are processed on the associated processor unit.

Based on the incoming port designation of a programmed flow, the flow is programmed only on the associated processing unit. If a programmed flow has no incoming port definition (e.g., a general flow), it is copied into all of the processing units.

The following figure shows the cardinality of each interface in a typical link-transection topology.



## Modes of Operation

FortiCore supports two modes of operation: Link Transect and Conditional Forwarding.

## Link Transect Mode

In Link Transect mode, all matching traffic is sent NB-EB and SB-WB, based on the flow table entries. Forwarding decisions are not based on session awareness.

## Conditional Forwarding Mode

For session-based Network Security Functions, FortiCore provides Conditional Forwarding mode.

Here, FortiCore applies TCP session-awareness to forwarding decisions. The FortiCore forwards only active TCP session traffic to the Network Security Function. For traffic that is not part of an active session you can configure a flow (for that traffic) to bypass the NSF.

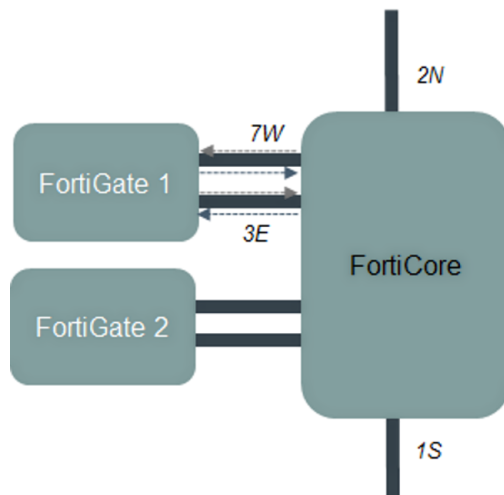
Session-awareness is necessary because a session-based Network Security Function will track the TCP sessions and discard any traffic that is not part of an active session. With Conditional Forwarding mode you avoid discarding this traffic.

The flow table provides the mappings between the external ports (N-S, S-E, N-W). In Conditional Forwarding mode, you also need to configure the association between the East and West ports for each Network Security device. This is required for TCP session tracking, performed in the East and West flow processing units.

Use the **config system network-function-group** command to specify the eas and west ports for each device.

## Configuration Example

In the following example, FortiGate 1 is providing session-based Network Security, and the FortiCore is operating in Conditional Forwarding mode.



### FortiCore Port assignments:

- Port 1: Southbound
- Port 2: Northbound

- Port 3: Eastbound to/from FortiGate 1
- Port 7: Westbound to/from FortiGate 1

### Simplified Flow table

Flow processor	Flow number	Match fields				Track?	Action	
		Ingress Port	VLAN	IP Protocol	Dest Port		Set VLAN	Out Port
South								
	1	1S	20	TCP	80	Y	200	3E
	2	1S					n/a	2N
East								
	1	3E	200	TCP	80	Y	20	1S
North								
	1	2N	20	TCP	80	Y	200	7W
	2	2N					n/a	1S
West								
	1	7W	200	TCP	80	Y	20	2N

### Flow Description:

The North and South interfaces each require two flows:

- Flow 1 directs the TCP traffic towards FortiGate 1.
- Flow 2 directs all other traffic to bypass FortiGate 1.

The East interface has one flow to direct the TCP traffic to port 1 (South)

The West interface has one flow to direct the TCP traffic to port 2 (North)

The North/South traffic uses VLAN 20.

For East/West traffic, the flow table entries (North 1 and South 1) set the VLAN to 200.

### Setting the Tracking field

The SDN controller must indicate the flow table entries that require session tracking. The FortiCore expects this information in the 8-byte cookie value in the flow entry. If the least-significant bit of the most-significant byte is

set, the FortiCore tracks the session for this flow.

## Port Pairing

Use the **config system network-function-group** command to specify the east port and the west port that are connected to FortiGate 1:

```
config system network-function-group
```

```
    edit 1
        set east-port 3
        set west-port 7
    next
end
```

## Support for Packet-In and Packet-Out Messages

FortiCore uses the Packet-In message to send a captured packet to the controller.

An Openflow controller can use the Packet-Out message to inject packets into the data plane of a particular switch. The Packet-Out message can carry a raw packet to inject into the switch, or can reference a local buffer on the switch that contains the raw packet.

## Support for VXLAN and MPLS

The FortiCore is an inline network appliance that can intelligently intercept and redirect traffic-of-interest to a set of associated network security devices.

Encapsulation protocols such as VxLAN and MPLS may not be fully supported by some network security devices. As VLANs are supported by all the security devices that will be deployed along with the FortiCore, it can map VxLAN and MPLS packets to specific VLANs. This makes it easier for the security device to analyze the traffic. The FortiCore then restores the VxLAN and MPLS headers onto the packets before they are sent towards their original destinations.

## Virtualization Support

In the Openflow architecture, switches are configured and managed by an Openflow controller. Therefore, Forticore operation depends on communication with this controller.

If an external controller is unavailable, FortiCore can run an internal Openflow controller. This controller runs on a virtual machine so that you can select any Openflow controller and the appropriate guest OS for the VM.

# OpenDaylight Controller

In the initial release, FortiCore product testing primarily focused on the OpenDaylight SDN controller, provided by the Linux Foundation. Refer to the following web site for additional information about OpenDaylight:

<http://opendaylight.org>

The OpenDaylight platform provides a set of core services, and provides a plug-in framework for other capabilities to be added as required.

For FortiCore, we use the following OpenDaylight components

- AAA
- OVSDB services
- OpenFlow

After the FortiCore connects to the controller, the controller performs 'discovery' to get information about the SDN switch ports on the FortiCore.

You configure the forwarding instructions (as flows) in the OpenDaylight controller. OpenDaylight sends the flows to the FortiCore using OpenFlow protocol.

Notes:

- FortiCore supports OpenFlow 1.3. The Open Networking Foundation web site contains the [OpenFlow version 1.3 specification](#).
- The FortiCore communication channel to the OpenDaylight controller uses TCP, or TLS if an encrypted channel is required.
- Configure the FortiCore management port as the SDN controller channel.
- FortiCore provides one SDN controller channel to the controller.

# Getting Started

This chapter describes how to perform the initial configuration for the FortiCore. This guide assumes that you have already installed the product into a hardware rack and set up console port or management port access.

## Basic steps:

1. Configure the management interface.
2. Configure the controller channel
3. Configure DNS
4. Configure NTP

## Configure the Management Interface

Configure the following settings for the management interface, so that you can access the web UI from a remote location:

Use the following command to configure the default gateway:

```
config router static
  edit 1
    set gateway <ip address>
  next
end
```

Use the following command to set the FortiCore IP address and configure the management interface:

```
config system interface
  edit mgmt
    set ip <ip&netmask>
    set allowaccess {http https ping snmp ssh telnet}
```

The system processes the update and disconnects your SSH session because the interface has a new IP address. At this point, you should be able to connect to the CLI or Web UI from a host on the management subnet that you just configured. You can verify the configuration remotely.

## Configure the Controller Channel

Use the following commands to configure the channel to the OpenDaylight controller. Configuring the IP address of the ODL controller is mandatory; other parameters are optional. For example, the transport protocol defaults to TCP, and the port number defaults to 6633:

```
config system open-flow-channel
  set ip <controller ipv4_addr>
  set port <integer>
end
```



## Configure DNS

Use the following commands to configure DNS:

```
config system dns
    set primary <IP Address>
    set secondary <IP Address>
end
```

## Configure NTP

Use the following commands to configure NTP:

```
config system time ntp
    set ntpsync enable
    set ntpserver <IP Address>
```

# FortiCore Web-based Interface

The FortiCore provides a web-based administrative interface to configure and manage the system. After you configure the management interface (see [Getting Started](#)), you can access the web interface remotely.

To access the interface, use following steps:

1. Navigate your web browser to: `http://<FortiCore IP address>`.
2. Enter a valid FortiCore user name and password.

After you successfully log in, the FortiCore Web Interface displays the dashboard.

## Initial Log-in

On your initial login to FortiCore, use the default credentials (user: **admin**, no password).



Note: for security reasons, you should create a new password for the admin user as soon as possible. Navigate to System > Administrator to edit the admin user.

---

## Main Menu

The main menu is common for all of the pages. The main menu contains the following selections:

- **Dashboard** - summary information about the system and the status of system resources
- **System** - system configuration and maintenance actions, user configuration, SNMP configuration
- **Networking** - interface and routing configuration. Port counter display.
- **OpenFlow** - various OpenFlow counters. Current active flows.
- **Log and Report** - configuration for log reporting and log servers. Browse the logs.

## Actions

On many pages, the following actions are available:

- **Add** - open a new page with the form to add a profile.
- **Refresh** - refreshes the page.

## Dashboard

The dashboard displays information about the system and the status of system resources (CPU, RAM, and Disk).

Field	Description
<b>System Information</b>	
Host Name	The host name
Current Time	Current system time
System Uptime	The duration of time since the last reboot, shutdown or reset
Serial Number	Serial number of the chassis
Firmware Version	Current version of firmware
<b>System Resources</b>	
CPU	Current CPU utilization as a percentage
RAM	Current RAM space used, as a percentage
Disk	Current disk space used, as a percentage

## System Reboot and Shutdown

From the dashboard page, you can initiate the following actions:

- **Reboot** - reboot the operating system
- **Shutdown** - power down the system
- **Reset** - reset the configuration to the factory default settings

## Firmware Update

To load the system with a new version of firmware:

1. Download the desired firmware version from the Fortinet support site to your local hard drive.
2. Click the **update** button next to the current firmware version.

3. Select the firmware file and click **OK**.
4. The system automatically loads the firmware and performs a system restart.

# System Settings

Use this page to configure system settings and to perform system maintenance actions.

The page contains three tabs:

- **Basic** - basic system settings
- **Maintenance** - time-related settings and to perform maintenance actions
- **Services** - settings for the mail server

## Configuring System Settings

You can update any of the basic settings. The important fields are the host name and the DNS servers.

Click the **Save** button before you navigate to a different tab or page.

The following table describes the basic settings:

Field	Description	Default
Host Name	The host name	n/a
Language	Language to display in the UI. Currently, only English is supported.	English
Idle Timeout	The duration (in minutes) before an idle active session will be logged out.	30 minutes
HTTP port	Port for the HTTP service	80
HTTPS port	Port for the HTTPS service	443
SSH Port	Port for the SSH service	22
Telnet Port	Port for the Telnet service	23

## Maintenance Actions

### Configuring Time-related Settings

You can update the time-related maintenance settings.

Click the **Save** button before you navigate to a different tab or page.

The following table describes the time-related settings:

Field	Description	Default
System Time	Local time of the system	n/a
Daylight Saving Time	Enable if this locale implements daylight savings time.	enabled
Time Zone	Local time zone	Pacific Time
NTP	Enable if you will use NTP to set and maintain the correct time for the system.	enabled
NTP Server	Specify a space-separated list of Fully-Qualified Domain Names or IP addresses of the NTP server pool.	n/a
Synchronizing Interval	How often the system synchronizes its time with the NTP server. The valid range is 1-1440.	60 minutes

## Backing up and restoring the configuration

If the system experiences hardware failure, being able to restore the entire backup configuration minimizes the time to reconfigure a replacement.

Configuration backups do *not* include data such as logs and reports.




Back up files include sensitive information, such as HTTPS certificate private keys. We strongly recommend that you password-encrypt backup files and store them in a secure location.

If you are restoring a configuration, you must know its management interface configuration to access the web UI after the restore procedure completes. Open the configuration file and record the IP address and network requirements for the management interface. Also, research the administrator username and password.

### To backup or restore the system configuration:

1. Go to **System>Settings**.
2. Click the **Maintenance** tab.
3. Scroll to the Backup & Restore section, and complete the actions described in the table below:

Actions	Guidelines
<b>Backup</b>	
Back Up	Select this option to back up the configuration. This backup is a text file.

Actions	Guidelines
Entire Configuration	Select this option to include error page files, script files, and ISP address book files. This backup is a tar file.
<b>Restore</b>	
Restore (option)	Select this option to restore a previous configuration. This restore file must be a text file.
Restore File	Click <b>Browse</b> to locate the file. After you select the file, the system displays the <b>Restore</b> button.
Restore (  button)	Click the <b>Restore</b> button to start the restore procedure. Your web browser uploads the configuration file and the system restarts with the new configuration.  Time required to restore varies by the size of the file and the speed of your network connection. Your web UI session is terminated when the system restarts. To continue using the web UI, refresh the web page and log in again.  If the restored system has a different management interface configuration than the previous configuration, you must access the web UI using the new management interface IP address.

## Updating Firmware using the Web UI

The maintenance tab includes the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: active and alternate. The upgrade procedure updates the firmware on the inactive partition and then makes it the active partition. In other words, if partition 2 is active, and you perform the upgrade procedure, partition 1 is upgraded and becomes the active partition; partition 2 becomes the alternate partition. The reason for this is to preserve the working system state in the event upgrade fails or is aborted.


Before you begin:

- Download the firmware file from the Fortinet Customer Service & Support website: <https://support.fortinet.com/>
- Read the release notes for the version you plan to install.
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.

**Boot Alternate Firmware** - reboot the system using the firmware in the non-active partition

**Upgrade** - upgrade the system from a file on the local hard drive

**To update firmware:**

1. Go to **System>Settings**.
2. Click the **Maintenance** tab.
3. Scroll to the Upgrade section.
4. Click **Browse** to locate and select the file.
5. Click  to upload the firmware and reboot.

The system replaces the firmware on the alternate partition and reboots. The alternate (upgraded) partition becomes the active, and the active becomes the alternate.



When you update software, you are also updating the web UI. To ensure the web UI displays the updated pages correctly:

- Clear your browser cache.
- Refresh the page.

In most environments, press Ctrl-F5 to force the browser to get a new copy of the content from the web application. See the Wikipedia article on browser caching issues for a summary of tips for many environments:

[https://en.wikipedia.org/wiki/Wikipedia:Bypass\\_your\\_cache](https://en.wikipedia.org/wiki/Wikipedia:Bypass_your_cache).

## Services

The services tab provides the fields to configure an SMTP Email Server.

### Configuring an SMTP Email Server

Configure an SMTP email server if you want to send alerts by email. See [Logs and Reporting](#) for information on configuring alerts.

**To configure SMTP:**

1. Go to **System>Settings**.
2. Click the **Services** tab.
3. Complete the configuration as described in the following table.
4. Save the configuration.

Settings	Guidelines
SMTP Server	IP address or FQDN of an SMTP server (such as FortiMail) or email server that the appliance can connect to in order to send alerts and/or generated reports.
Port	Listening port number of the server. Usually, SMTP is 25.



Settings	Guidelines
Authentication	Enable if the SMTP server requires authentication
Username	Username for authentication to the SMTP server
Password	Password for authentication to the SMTP server

# System Administrators

Use the system administrator page to configure admin users for the system.

## Overview

By default, the system has one administrator account named **admin**, which has permissions to grant Read-Write access to all system functions.

Unlike other administrator accounts, the **admin** account cannot be deleted. It is similar to a root administrator account. The admin account always has full permission to view and change all system configuration options, including viewing and changing *all* other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.

You can use the **admin** account to configure more administrator accounts for other people. Accounts can be made with different scopes of access using access profiles. For example, you can create an account for a security auditor who must only be able to view the configuration and logs, but *not* change them.

### Basic steps for configuring users

1. Configure access profiles to provision the permissions for each role.
2. Optional. Create RADIUS server configurations if you want to use a RADIUS server to authenticate administrators. Otherwise, you can use local authentication.
3. Create administrator user accounts and assign access profiles based on user roles.

## Configuring Access Profiles

The access profile determines the user's level of access to various parts of the system. The following levels can be assigned:

- Read (view access)
- Read-Write (view, change, and execute access)
- No access

When an administrator has only read access to a feature, the administrator can access the web UI page for that feature, and can use the `get` and `show` CLI command for that feature, but cannot make changes to the configuration.

### Create a Profile

1. Go to **System>Administrator**.
2. Click the **Access Profile** tab.
3. Click the **Add** button

4. Input the fields, as described in the table below.
5. Click the **Save** button.

Field	Description
Profile Name	The profile name
For each of the categories listed below, you set the permission: <ul style="list-style-type: none"> <li>• None - no access to CLI or GUI provisioning commands.</li> <li>• Read Only - ready-only access.</li> <li>• Read-Write - can make changes to the configuration, using CLI or GUI commands.</li> </ul>	
System	controls access to the following commands: <pre>config system diagnose hardware diagnose sniffer diagnose system execute date execute ping execute ping-options execute traceroute</pre>
Router	controls access to the following commands: <pre>config router</pre>
Log & Report	controls access to the following commands: <pre>config log config report execute formatlogdisk</pre>



The **super\_admin\_prof** access profile, a special access profile assigned to the **admin** account and required by it, appears in the list of access profiles. It exists by default and cannot be changed or deleted. The profile has permissions similar to the UNIX root account.

## Per-Profile Actions

Each entry in the profiles list contains the following icons in the Action column:

- **Edit** - opens a new page with the form to edit the data for this profile.
- **Delete** - deletes this profile.

## Configuring administrator users

We recommend that only network administrators—and if possible, only a single person—use the **admin** account. You can configure additional accounts with different access profiles, as required.

**To create administrator users:**

1. Go to **System>Administrator**.  
**The configuration page displays the Admin tab.**
2. Click **Add** to display the configuration editor.
3. Complete the configuration as described in the table below
4. Save the configuration.

The following table lists the settings for each user:

Field	Description
Name	The user name
Authentication Server	<ul style="list-style-type: none"><li>• Local—Use the local administrator authentication server.</li><li>• RADIUS—Use a RADIUS authentication server. Select the RADIUS server configuration.</li></ul>
Password	Enter a password for the user
Trusted Hosts	Source IP address and netmask from which the administrator is allowed to log in. For multiple addresses, separate each entry with a space. You can specify up to three trusted areas. They can be single hosts, subnets, or a mixture.
Profile	Access Profile

## Per-User Actions

Each entry in the users list contains the following icons in the Action column:

- **Edit** - opens a new page with the form to edit the data for this user
- **Lock** - prevents the user from being updated or deleted
- **Delete** - deletes this user

## Using a RADIUS Server

You can use a RADIUS authentication server to authenticate administrator credentials.

### Create a RADIUS server

**To create a RADIUS server configuration:**

1. Go to **System>Administrator**.
2. Click the **RADIUS** tab.
3. Click **Add** to display the configuration editor.

4. Complete the configuration as described in the table below
5. Save the configuration.

Field	Description
Name	The user name
Server	IP address for the server
Port	Port number for the server. The commonly used port for RADIUS is 1812.
Shared Secret	Enter the shared secret used when connecting to the server.
Authentication Protocol	<ul style="list-style-type: none"><li>• PAP—Password authentication protocol.</li><li>• CHAP—Challenge-Handshake Authentication Protocol.</li><li>• MS-CHAP—Microsoft version of CHAP.</li><li>• MS-CHAPv2—Microsoft CHAP, version 2.</li></ul>

## Per-Server Actions

Each entry in the profiles list contains the following icons in the Action column:

- **Edit** - opens a new page with the form to edit the data for this RADIUS server
- **Delete** - deletes this RADIUS server

# SNMP Settings

Many organizations use *SNMP* (simple network management protocol) to track the health of their systems. FortiCore supports SNMP v1 and v2c,

SNMP relies on network devices that maintain standard management information bases (MIBs). *MIBs* describe the structure of the management data maintained on the device. Some MIB definitions are standard for all network devices, and some are vendor and product-family specific.

The FortiCore system runs an *SNMP agent* to communicate with the *SNMP manager*. The agent enables the system to respond to *SNMP queries* for system information and to send *SNMP traps* (alarms or event messages) to the SNMP manager.

## To configure SNMP:

1. Go to **System>SNMP**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

Settings	Guidelines
<b>System Information</b>	
SNMP Agent	Enable to activate the SNMP agent, so that the system can send traps and receive queries.
Description	A description or comment about the system. The description can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens ( - ) and underscores ( _ ).
Contact	Contact information for the administrator or other person responsible for this system. The contact information can be up to 35 characters long.
Location	Physical location of the appliance, such as <code>floor2</code> . The location can be up to 35 characters long.
<b>Threshold</b>	
CPU	<ul style="list-style-type: none"> <li>• Trigger—The default is 80% utilization.</li> <li>• Threshold—The default is 3, meaning the event is reported when the condition has been triggered 3 times in a short period.</li> <li>• Sample Period—The default is 600 seconds.</li> <li>• Sample Frequency—The default is 30 seconds.</li> </ul>

Settings	Guidelines
Memory	<ul style="list-style-type: none"> <li>• Trigger—The default is 80% utilization.</li> <li>• Threshold—The default is 3, meaning the event is reported when the condition has been triggered 3 times in a short period.</li> <li>• Sample Period—The default is 600 seconds.</li> <li>• Sample Frequency—The default is 30 seconds.</li> </ul>
Disk	<ul style="list-style-type: none"> <li>• Trigger—The default is 90% utilization.</li> <li>• Threshold—The default is 1, meaning the event is reported each time the condition is triggered.</li> <li>• Sample Period—The default is 7200 seconds.</li> <li>• Sample Frequency—The default is 3600 seconds.</li> </ul>
<b>Community (SNMP v1 and v2c)</b>	
Name	<p>Name of the SNMP community to which the FortiCore system and at least one SNMP manager belongs, such as <code>management</code>.</p> <p>You must configure the FortiCore system to belong to at least one SNMP community so that community's SNMP managers can query system information and receive SNMP traps.</p> <p>You can add up to three SNMP communities. Each community can have a different configuration for queries and traps, and the set of events that trigger a trap.</p> <p>You can also add the IP addresses of up to eight SNMP managers to each community to designate the destination of traps and which IP addresses are permitted to query the FortiCore system.</p>
Status	Select to enable the configuration.
Queries	<p>Port number on which the system listens for SNMP queries from the SNMP managers in this community. The default is 161.</p> <p>Enable queries for SNMP v1, SNMP v2c, or both.</p>
Traps	<p>Source (Local) port number and destination (Remote) port number for trap packets sent to SNMP managers in this community. The default is 162.</p> <p>Enable traps for SNMP v1, SNMP v2c, or both.</p>
Events	<p>Select to enable SNMP event reporting for the following thresholds:</p> <ul style="list-style-type: none"> <li>• CPU— CPU usage has exceeded 80%.</li> <li>• Memory—Memory (RAM) usage has exceeded 80%.</li> <li>• Disk—Disk space usage for the log partition or disk has exceeded 90%.</li> </ul>

Settings	Guidelines
Host	<p>IP address of the SNMP manager to receive traps and be permitted to query the FortiADC system. SNMP managers have read-only access. You can add up to 8 SNMP managers to each community. To allow any IP address using this SNMP community name to query the FortiCore system, enter 0 . 0 . 0 . 0. For security best practice reasons, however, this is not recommended.</p> <p><b>Caution:</b> The system sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative equipment.</p> <p><b>Note:</b> If there are no other host IP entries, entering only 0 . 0 . 0 . 0 effectively disables traps because there is no specific destination for trap packets. If you do not want to disable traps, you must add at least one other entry that specifies the IP address of an SNMP manager.</p>



# Networking

Use the networking page to configure network interfaces, configure static routes, and view port statistics.

## Configuring Network Interfaces

You can edit the configuration for a physical interface but you cannot create or delete it.

### To configure a network interface:

1. Go to **Networking>Interface**.
2. Double-click the row for a physical interface to edit its configuration.
3. Complete the configuration as described in the table below.
4. Save the configuration.

Settings	Guidelines
<b>Common Settings</b>	
Name	Configuration name. Valid characters are A-Z, a-z, 0-9, _, and -. No spaces. After you initially save the configuration, you cannot edit the name
Status	The Status column is not the detected physical link status; it is the administrative status (Up/Down) that indicates whether you permit the network interface to receive and/or transmit packets.
Speed	The interface speed. Speed options vary for different models and interfaces. Port speeds must be configured as follows: <ul style="list-style-type: none"><li>- Management port must be set to auto, 1Gfull or 1Ghalf (on all models)</li><li>- Ports 1-32 must be set to 1Gfull or 10Gfull (on all models)</li><li>- Ports 33-36 must be set to 40Gfull on 3700E</li><li>- Ports 33-34 must be set to 100Gfull on 3800E</li></ul>
Type	The interface type. Physical or ??
Direction	Values: eastbound, northbound, southbound, westbound  The direction assigned to the interface determines which processing unit will process the interface's ingress traffic. Flows received from the SDN controller will be populated onto the unit associated with the incoming port value of the flow. If the flow has no incoming port value, the flow is programmed on all four processing units.

## Configuring Static Routes

### To configure a static route:

1. Go to **Networking>Routing**.
2. Click **Add** to display the configuration editor.
3. Complete the configuration as described in the table below
4. Save the configuration.

Settings	Guidelines
Destination	Address/mask notation to match the destination IP in the packet header.  It is a best practice to include a default route. If there is no other, more specific static route defined for a packet's destination IP address, a default route will match the packet, and pass it to a gateway router so that any packet can reach its destination.
Gateway	Specify the IP address of the next-hop router where the system will forward packets for this static route. This router must know how to route packets to the destination IP addresses that you have specified, or forward packets to another router with this information.
Distance	The default administrative distance is 10, which makes it preferred to OSPF routes that have a default of 110. We recommend you do not change these settings unless your deployment has exceptional requirements.

## Link Aggregation (i.e., Port Trunking)

We use Link Aggregation to combine multiple physical ports so that they appear as a single higher capacity port. Doing this provides:

- Connection/Link reliability
- Traffic load sharing among member ports

With FortiCore Release 2.0.0, we provide this feature to enable you to aggregate multiple physical ports into one LAG group. (Two or more member (physical) ports can comprise a multiple LAG group.)

Within an LAG group, you can set most of the typical parameters (like speed, mac-addr, ip address etc.). You can also set the Forticore-specific parameter “direction”, which binds a port to a cardinality (NORTH/SOUTH/EAST/WEST). However, some LAG-specific parameters like “member” and “algorithm” are available only if the interface type is LAG.

## LAG CLI Configuration

```
(interface) # edit aggl
(aggl) # set
algorithm <dst-ip/dst-mac/src-dst-ip/src-dst-mac/src-ip/src-mac>
direction <northbound/southbound/eastbound/westbound>
ip <ipaddr/netmask>
ip6 <ipv6addr/netmask>
mac-addr <xx:xx:xx:xx:xx:xx>
member <portx, porty, ...>
mode <static>
mtu <integer>
status <up/down>
*vdom <root>
next-hop-mac-addr <xx:xx:xx:xx:xx:xx>
```

Configuration attribute	Function
algorithm	Sets the LAG algorithm
direction	Direction associated with this port
ip	ipv4 address of the interface
ip6	ipv6 address of the interface
mac-add	Hardware address of the interface
member	Sets the port members of LAG
mode	Mode of LAG. Only 'static' option in this release
mtu	Maximum transportation unit of the LAG interface
status	Interface status
vdom	vdom name
next-hop-mac-addr	Next hop hardware address to used in case of VxLAN

## Configure Network Interface

```
FortiCore-3700E # config system interface
FortiCore-3700E (interface) # edit agg1
FortiCore-3700E (agg1) # set
allowaccess    Allow access with the interface
direction     direction associated with this port
ip            ip address of interface
ip6           ipv6 address of interface
lacp-mode     Set LAG(Link Aggregation Groups) mode
member        Set port members of LAG
mode          static
mtu           maximum transportation unit
status        interface status
*type         interface type
*vdom         vdom name
```

**NOTE:** You might notice the slight difference between “Configuring Network Interfaces” and “LAG CLI Configuration”. They are very similar as they are both system interfaces. For interfaces starting with “port,” we assume a physical interface. For interfaces starting with “agg,” we must specify the attribute **type = aggregate**. When we do this, the lag-specific attributes (aggregate-algorithm, lacp-mode, and member) become visible. These attributes are not visible for physical ports. All other attributes are common for both types.

## Example: LAG Configuration

Here is an illustrative aggregate/lag port configuration:

```
FortiCore-3700E # config system interface
FortiCore-3700E (interface) # edit agg2
Add new entry 'agg2' for node 1

FortiCore-3700E (agg2) # set
allowaccess    Allow access with the interface
direction     direction associated with this port
ip            ip address of interface
ip6           ipv6 address of interface
mtu           maximum transportation unit
status        interface status
*type         interface type
*vdom         vdom name

FortiCore-3700E (agg2) # set vdom root

FortiCore-3700E (agg2) # set type
physical      physical
aggregate     aggregate

FortiCore-3700E (agg2) # set type aggregate
```

```

FortiCore-3700E (agg2) # set
aggregate-algorithm    aggregate interface slave selection algorithm
allowaccess            Allow access with the interface
direction              direction associated with this port
ip                     ip address of interface
ip6                    ipv6 address of interface
lACP-mode              Set LAG(Link Aggregation Groups) mode
member                 Set port members of LAG
mtu                    maximum transportation unit
status                 interface status
*type                  interface type
*vdom                  vdom name

FortiCore-3700E (agg2) # set member port8 pr <Enter>

FortiCore-3700E (agg2) # set member port8 port9

FortiCore-3700E (agg2) # set aggregate-algorithm
dst-ip                 dst-ip
dst-mac                dst-mac
port-flow              port-flow
src-dst-ip             src-dst-ip
src-dst-mac            src-dst-mac
src-ip                 src-ip
src-mac                src-mac

FortiCore-3700E (agg2) # set aggregate-algorithm src-dst-ip <Enter>

FortiCore-3700E (agg2) # set aggregate-algorithm src-dst-ip

FortiCore-3700E (agg2) # end

```



## Example: Display LAG Settings

```

FortiCore-3700E # show system interface agg1
config system interface
edit "agg1"
set type aggregate
set vdom root
set direction northbound
set member port2
next
end

```

## Port Format in the SDN Flow

To program a LAG port in a flow (as input or output), observe the following format:

Match Field: Inport  
port encoding: 0xFCDDXYZZ

Action: Outport  
port encoding: 0xFCDDXYZZ

- DD = port direction
  - 01 = North
  - 02 = South
  - 03 = East
  - 04 = West
- X = Logical port type
  - 0 = Physical
  - 1 = Vxlan
  - 2 = MPLS
  - 3 = **LAG**
- Y = Port speed
  - 1 = 1G
  - 2 = 10G
  - 3 = 40G
  - 4 = 100G
- ZZ = Physical/logical port number

e.g. FC023205 (hex) represents a southbound LAG port of value 5.

## Viewing Port Counters

To view the port counters:

1. Go to **Networking**>**Port Counter**.

The configuration page displays the statistics for each port.

# OpenFlow

Use the OpenFlow page to configure the connection to an SDN controller, and to view OpenFlow counters and flows.

## Configuring the SDN Controller Connection

**To create an SDN controller connection:**

1. Go to **Openflow>Controller**.  
The Openflow page displays the Controller connection fields.
2. Complete the configuration as described in the table below
3. Save the configuration.

Field	Description
Version Supported	OpenFlow version
Transport Type	Select TCP or TLS
IP address	IP address of the SDN controller
Port Number	Port number of the SDN controller
Cert	The OpenFlow certificate
CACert	The OpenFlow CA certificate
Probe Interval	Interval in seconds at which idle controller is probed
Max Backoff	Maximum time interval (in seconds) that the system will wait before retrying a connection to the controller
Connection Status	Status of the connection to the SDN controller. Read-only field
Datapath Id	Read-only field
Connection Uptime	Time duration (in minutes) that the current connection has up. Read-only field

## Viewing Openflow Counters

To view the port counters:

1. Go to **Openflow>Counters**.

The configuration page displays the RX and TX counters related to Openflow.

## Viewing Openflow Flows

To view the Openflow flows:

1. Go to **Openflow>Flows**.
2. The configuration page displays the current field values of active OpenFlow flows.
3. (Optional) Click the **preview** icon for any of the rows to view detailed information about that flow.



# OVSDB

OVSDB (Open vSwitch Database) is a management protocol used to manipulate the configuration of Open vSwitches. We use Openflow to configure the forwarding path, whereas we use OVSDB to configure the switch itself.

OVSDB uses JSON for its wire format and is based on JSON-RPC version 1.0. (Schema is also in JSON format.)

Forticore supports OVSDB for remote configuration by either OVSDB client or manager.

## OVSDB Support in Forticore

Forticore supports 2 OVSDB channels, each configurable as active or passive.

In passive mode, FortiCore listens for connections and OVSDB clients can connect to Forticore on the default port or configured port.

In active mode, FortiCore connects to the OSVDB manager which is listening on the specified port.

Configuration objects are supported and configurable thru OVSDB: port, vxlan tunnel and openflow channel.

We support the RPC methods: list databases, get schema, echo, transact and cancel.

Supported OVSDB database operations as components of the “transact” RPC include: insert, select, update, mutate, delete, commit, abort, comment, and assert.

## Configuring OVSDB

We use the following CLI to configure a OVSDB channel:

```
config system ovbdb-channel
edit 1
set transport <tcp/tls>
set ip <ovbdb client/manager ip addr>
set port <ovbdb listening port>
set probe-interval <seconds>
set max-backoff <seconds>
set passive-connection <enable/disable>
end
```

Configuration Attribute	Description
transport	Transport protocol. TCP (Default) and TLS are supported.
ip	OVSDB client or manager's IP address

Configuration Attribute	Description
port	Port on which the OVSDb is listening. In passive mode, Forticore will listen on this port. In active mode, Forticore connects to the OVSDb manager on this port. Default is 6640.
passive-connection	Specifies OVSDb channel mode. Enable makes the channel passive. Disable makes it active. Default is disable.
max-backoff	Maximum time (in seconds) between retries. Default is 8 secs.
probe-interval	Maximum time (in seconds) between liveness check probes. Default 5 secs.

## Example

```

FortiCore-3800E # config system ovldb-channel
FortiCore-3800E (ovldb-channel) # edit 1
FortiCore-3800E (1) # set
ip                ovldb manager ip address
max-backoff       Maximum interval in seconds to wait before retrying connection
passive-connection passive connection disable|enable
port              ovldb manager port number
probe-interval    Interval in seconds at which idle manager is probed
transport         transport type
FortiCore-3800E (1) # end

```

## Displaying OVSDb Channel Configurations

We use the following CLI to view the OVSDb channel:

```
# show system ovldb-channel
```

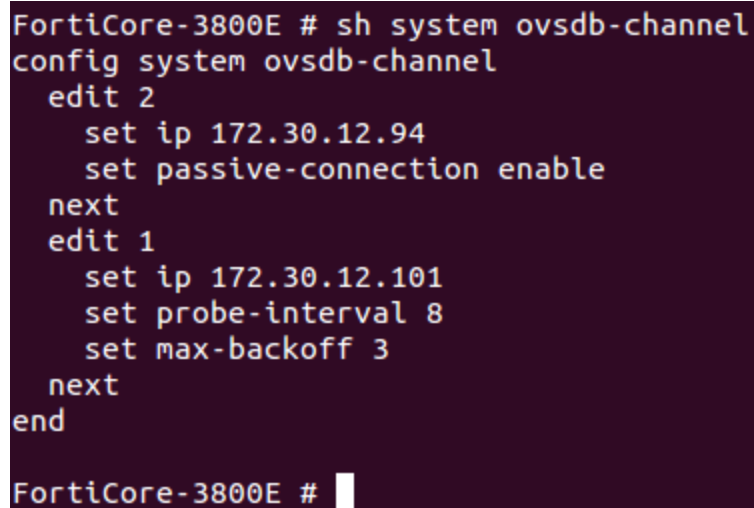
## Example

```

FortiCore-3800E # sh system ovldb-channel
configur system ovldb-channel
edit 2

```

```
    set ip 172.30.12.94
    set passive-connection enable
next
edit 1
    set ip 172.30.12.101
    set probe-interval 8
set max-backoff 3
next
end
```



```
FortiCore-3800E # sh system ovldb-channel
config system ovldb-channel
edit 2
    set ip 172.30.12.94
    set passive-connection enable
next
edit 1
    set ip 172.30.12.101
    set probe-interval 8
    set max-backoff 3
next
end
FortiCore-3800E #
```

## Displaying Configuration for Individual Channels

We use the following CLI to view the OVSDb channel:

```
# get system ovldb-channel <1|2>
```

### Example

This **get** command shows configuration of the OVSDb channel including the default values.

```
FortiCore-3800E # get system ovbdb-channel 1
transport      : tcp
ip             : 172.30.12.101
port          : 6640
probe-interval : 8
max-backoff    : 3
passive-connection : disable

FortiCore-3800E # get system ovbdb-channel 2
transport      : tcp
ip             : 172.30.12.94
port          : 6640
probe-interval : 5
max-backoff    : 8
passive-connection : enable

FortiCore-3800E #
```

## Displaying Status of Configured Channels

```
# get ovbdb channel status
```

### Example

This **get** command displays additional dynamic state information of the OVSDb channel (like connection-uptime):

```
FortiCore-3800E # get ovldb channel status
manager-id          : 1
channel-type        : tcp
ovldb-manager ip    : 172.30.12.101
ovldb-manager port   : 6640
connection-status    : up
connection-uptime    : 14 days 23 hours 58 minutes 50 seconds
probe interval       : 8
maximum backoff interval : 3
passive-connection   : disable

manager-id          : 2
channel-type        : tcp
ovldb-manager ip    : 172.30.12.94
ovldb-manager port   : 6640
connection-status    : down
connection-uptime    : 0 seconds
probe interval       : 5
maximum backoff interval : 8
passive-connection   : enable
```

**NOTE:** Channels configured as active will only have “connection-uptime,” which is only applicable to active connection. It is not applicable to passive connection.

## Displaying OVSDB Protocol Counters

```
# get ovldb counters
```

### Example

```
FortiCore-3800E # get ovldb counters
ovldb-to-cmdb-add-success      : 253
ovldb-to-cmdb-add-fail         : 0
ovldb-to-cmdb-update-success   : 0
ovldb-to-cmdb-update-fail      : 31
ovldb-to-cmdb-delete-success   : 0
ovldb-to-cmdb-delete-fail      : 0
ovldb-to-cmdb-invalid          : 1
cmdb-to-ovldb-add-success      : 44
cmdb-to-ovldb-add-fail         : 0
cmdb-to-ovldb-update-success   : 2
cmdb-to-ovldb-update-fail      : 0
cmdb-to-ovldb-delete-success   : 0
cmdb-to-ovldb-delete-fail      : 0
```

## Example Transact Request

Here is an example transact RPC method with data operations coming from the Manger to FortiCore.

```
[
  "Open_vSwitch",
  {
    "op": "mutate",
    "table": "Open_vSwitch",
    "where" : [
      [
        "next_cfg",
        "==",
        0
      ]
    ],
    "mutations" : [
      [
        "manager_options",
        "insert",
        [
          "set",
          [
            [
              "named-uuid",
              "this_manager"
            ]
          ]
        ]
      ],
      {
        "op": "insert",
        "table": "Manager",
        "row": {
          "target": "tcp:172.30.12.101:6640",
          "inactivity_probe": 5100,
          "max_backoff" : 2801
        },
        "uuid-name": "this_manager"
      },
      {
        "op" : "comment",
        "comment" : "Add manager"
      }
    ]
  }
]
```

## CMDB to OVSDB Mapping

One-on-one mapping is defined for each supported CMDB parameter to the corresponding column in OVSDB. For example "name" under config system interface is mapped to "name" in the Interface Table.

The following table shows the mapping between CMDB and OVSDDB configuration parameters:

CMDB	OVSDDB
<del>config system openflow-channel</del> <del>transport</del> <del>ip</del> <del>port</del> <del>probe-interval</del> <del>max-backoff</del> <del>status (get only)</del>	Controller Table: <del>target (tcp:ip:port or ssl:ip:port)</del> <del>target</del> <del>target</del> <del>inactivity_probe</del> <del>max_backoff</del> <del>is_connected</del>
<del>config system openflow-channel</del> <del>cert</del> <del>cacert</del>	SSL Table: <del>cert</del> <del>ca_cert</del>
<del>config system interface</del> <del>name</del> <del>type</del> <del>ip</del> <del>ip6</del> <del>direction</del> <del>next-hop-mac-addr</del> <del>mtu</del> <del>speed</del> <del>status</del> <del>mac-addr</del> <del>*allowaccess ( only for mgmt ports)</del>	Interface Table: <del>name</del> <del>type</del> <del>options:local_ip</del> <del>options:local_ipv6</del> <del>options:direction</del> <del>options:next-hop-mac</del> <del>mtu</del> <del>duplex, link_speed</del> <del>admin_state</del> <del>mac</del> <del>options:allowaccess</del>
<del>config system ovsdb-channel</del> <del>transport</del> <del>ip</del> <del>port</del> <del>passive-connection</del> <del>probe-interval</del> <del>max-backoff</del> <del>status (get only)</del>	Manager Table: <del>target (tcp:ip:port or ssl:ip:port for active</del> <del>ptcp:port, pssl:port for passive)</del> <del>target</del> <del>target</del> <del>target</del> <del>inactivity probe</del> <del>max_backoff</del> <del>is_connected</del>

OVSDDB supports only 1 row in SSL Table. The same set of certificates are used for openflow and OVSDDB channels. In CMDB, the SSL certificate configuration is in **config openflow channel**, which is applicable for both openflow and ovsdb channels.

If transport is configured as SSL, then a certificate is mandatory. Because openflow channel configuration also uses SSL transport, the openflow CLI has a provision to select a certificate. So, instead of a second certificate configuration for OVSDDB, the system uses the certificate configured under the openflow channel configuration.





# Virtualization

As OpenFlow switches are configured and managed by an OpenFlow controller, Forticore operation requires communication with an external controller.

If an external controller is unavailable, FortiCore provides the ability to run an internal OpenFlow controller. This controller runs on a virtual machine (using the KVM hypervisor), so that you can select any OpenFlow controller and the appropriate guest OS for the VM.

For example, you can launch an Ubuntu virtual machine and run the OpenDaylight controller on the Ubuntu VM.

## FortiCore Virtualization CLI Commands

FortiCore provides a set of CLI commands to configure, launch and manage the virtual machines.

### Configuring a Virtual Machine

Use the following commands to configure the parameters for the virtual machine:

```
config system virtual-machine-group
edit 1
    set name <VM name>
    set image-file <file name>
    set ram <256...2048>
    set vnc <1...4>
    set volume <volume name>
```

The following table describes the parameters:

Field	Description
virtual-machine id	Entry number in the table
name	Descriptive text name for the virtual machine
image-file	Name of the image file to use for the virtual machine
ram	Set the amount of RAM for the virtual machine. The range is 256 to 2048, and the units is Mb. The default value is 512.
vnc	VNC number to attach to the virtual machine. The default value is 1.
volume name	Name of the volume to attach to the virtual machine

## Configuring a Virtual Machine Volume

Use the following commands to configure the parameters for a disk volume:

```
config system virtual-machine-volume-group
edit 1
    set name <VM volume name>
    set size <256...2048>
```

## Configuration Notes

The FortiCore automatically assigns an IP address for each VM network interface and for the management interface. The interfaces are all connected to one internal network bridge.

The **virtual-machine-volume-group** command creates a raw disk. The VM user can create the file system and partition the volume as required.

## Starting a Virtual Machine

Use the following command to start the virtual machine that has the specified virtual machine id:

```
execute virtual-machine start <num>
```

## Stopping a Virtual Machine

Use the following command to stop the virtual machine that has the specified virtual machine id:

```
execute virtual-machine stop <num>
```

The stop command does not suspend the VM. It stops the VM process and frees up the associated memory.

## Importing a Virtual Machine Image

Use the following command to import a virtual machine image from a TFTP server:

```
get virtual-machine image tftp <name of image> <ip address of tftp server>
```

## Getting a List of Virtual Machines

```
get system virtual-machine list
```

## Getting a List of Virtual Machine Images

```
get system virtual-machine image-list
```

## Example Configuration

The following example creates a FortiPrivateCloud instance, with an associated disk volume.

```
config system virtual-machine-group
  edit 1
    set name fpc_portal
    set image-file fpcvm64image-kvm-portal.qcow2
    set ram 4096
    set volume fpc_log_disk.img
  next
end
```

```
config system virtual-machine-volume-group
  edit 1
    set name fpc_log_disk.img
    set size 60000
  next
end
```

```
FortiCore-3800E # execute virtual-machine start 1
```

```
FortiCore-3800E # get system virtual-machine list
```

Id	Name	Image-File	RAM(mb)	PID	State	VNC
1	fpc_portal	fpcvm64image-kvm-portal.qco	4096	6442	run	1
2	mysql1	mysql.qcow2	4096	0	off	2
3	testvmdk	ubuntu_64.vmdk	2048	0	off	3
4	fpc_collector	fpcvm64image-kvm-collector.	4096	0	off	4

```
FortiCore-3800E # execute virtual-machine stop 1
```

```
FortiCore-3800E # get system virtual-machine list
```

Id	Name	Image-File	RAM(mb)	PID	State	VNC
1	fpc_portal	fpcvm64image-kvm-portal.qco	4096	0	off	1
2	mysql1	mysql.qcow2	4096	0	off	2
3	testvmdk	ubuntu_64.vmdk	2048	0	off	3
4	fpc_collector	fpcvm64image-kvm-collector.	4096	0	off	4

# VXLAN and MPLS Tunnels

## VXLAN Operation

The FortiCore terminates all of the VxLAN tunnels, and maps the VXLANs to VLANs for processing by the network security devices.

The FortiCore creates a logical port to represent the VxLAN tunnel, and sends a PORT-UP message to the OpenFlow controller to inform the controller of the port.

## Traffic flow

### North and South

Ingress on a NB or SB port: FortiCore uses the VNI to match a flow entry. The flow entry provides the VLAN value to use and the egress port number.

### East and West

Ingress on an EB or WB port: FortiCore uses the VLAN to match a flow entry. The flow entry provides the VNI value to use and the egress port number.

## Configuring VXLAN

Use the following CLI commands to configure a VxLAN tunnel:

```
config system interface
  edit <port number>
    set ip <IPv4 address>
    set ip6 <IPv6 address>
    set direction {northbound | southbound | eastbound | westbound }
    set mac-addr <MAC address>
    set next-hop-mac-addr <MAC address>
  end
```

```
config system tunnel
  edit <name>
    set remote-ip4 <IPv4 address>
    set remote-ip6 <IPv6 address>
    set port <vxlan port>
    set vni <integer>
    set interface <port>
  end
```

Field	Description
name	Name for this entry
interface	Egress port for the packets
port	Ingress VXLAN port
remote-ip4	remote IPv4 address
remote-ip6	remote IPv6 address
vni	Set the VXLAN network indicator

## Example Configuration

```
config system interface
  edit port3
    set ip 10.1.1.1/24
    set direction northbound
    set mac-addr 33:44:55:66:77:00:11:22
    set next-hop-mac-addr aa:bb:cc:dd:ee:ff:00:11
  end

config system tunnel
  edit vxlan1
    set remote-ip4 10.1.1.2
    set port 47
    set vni 200
    set interface 3
  end
```

## VXLAN Flows

To provide the associated VNI and VLAN values, you need to program the following flows for each tunnel:

### NorthBound Flow:

- Match: VNI;
- Action: Decapsulate VxLAN, Push VLAN,
- OutBound Port EastBound

### SouthBound Flow:

- Match: IP;
- Action: Push VLAN,
- OutBound Port WestBound

**EastBound Flow:**

- Match: VLAN;
- Action: Pop VLAN, Encapsulate VxLAN,
- OutBound Port SouthBound

**WestBound Flow:**

- Match: VLAN;
- Action: Pop VLAN, Encapsulate VxLAN,
- OutBound Port NorthBound

## MPLS Operation

For MPLS, FortiCore maps the MPLS labels to specific VLANs for processing by the network security devices.

When the FortiCore receives an MPLS packet, it decapsulates the MPLS label and encapsulates the associated VLAN value for that MPLS label. When the FortiCore receives a VLAN-encapsulated packet, the FortiCore decapsulates the VLAN and encapsulates an MPLS label associated with the value of the VLAN ID (assuming that the VLAN ID matches a value associated with an MPLS label).

### Traffic flow

**North and South**

Ingress on a NB or SB port: FortiCore uses the MPLS label value to match a flow entry. The flow entry provides the VLAN value to use and the egress port number.

**East and West**

Ingress on an EB or WB port: FortiCore uses the VLAN to match a flow entry. The flow entry provides the MPLS label value to use and the egress port number.

## Configuring MPLS

Use the following FortiCore CLI commands to configure MPLS:

### MPLS Flows

To provide the associated VLAN value, you need to program the following flows for each MPLS label:

**NorthBound Flows**

Match: MPLS;

Action: Pop MPLS, Push VLAN,  
OutBound Port EastBound

### **SouthBound Flows**

Match: MPLS;  
Action: Pop MPLS, Push VLAN,  
OutBound Port WestBound

### **EastBound Flows**

Match: VLAN;  
Action: Pop VLAN, Push MPLS,  
OutBound Port SouthBound

### **WestBound Flows**

Match: VLAN;  
Action: Pop VLAN, Push MPLS,  
OutBound Port NorthBound

## **Logical Port Types**

The FortiCore generates a PORT-UP/PORT-DOWN message to the OpenFlow controller when a new logical port is created. Because FortiCore supports multiple tunnel-encapsulation methodologies, the logical-port-value must include the type of logical-port that is being provided.

In prior releases, **port speed** is encoded in the third octet of the logical port-number.

As port speed has already been reported to the OpenFlow Controller as part of the PORT-UP/PORT-DOWN message, it is not required in the logical port value. Instead, the logical-port value will be encoded as 0xFCxyzz where the third octet is now the logical port type:

xx = Port Direction

01 = NorthBound  
11 = SouthBound  
21 = EastBound  
31 = WestBound

yy: set to 0x10 for a VxLAN port.

zz = VxLAN port number

# Packet-In and Packet-Out Support

FortiCore supports Packet-In and Packet-Out functionality, as described in the OpenFlow 1.3 specification.

FortiCore uses the Packet-In message to send a captured packet to the controller.

An OpenFlow controller can use the Packet-Out message to inject packets into the data plane of the FortiCore. The Packet-Out message can carry a raw packet to inject into the switch, or can reference a local buffer on the switch that contains the raw packet.

FortiCore provides rate limiting on the open-flow channel to the CPU, so that the CPU is not overloaded by the messages on this channel. The rate limits are currently not configurable. The default values are as follows (units are packets per second):

- rate limit: 256
- burst limit: 1024

For additional information about OpenFlow, including the specifications, follow this link:

<https://www.opennetworking.org/sdn-resources/technical-library>

## Packet-In Messages

OpenFlow 1.3.4 specifies the following reason codes for sending a packet to the controller:

- **NO MATCH**: No matching flow (table-miss flow entry).
- **ACTION**: Action explicitly output to controller.
- **INVALID TTL**: Packet has an invalid TTL value.

FortiCore supports only the ACTION reason code - the FortiCore sends a Packet-In message only if an explicit Packet-In flow is defined. A Packet-In flow specifies the controller as the out-port in the flow action. The controller port is openflow reserve port OFFP\_CONTROLLER (0xffffffd).

For a Packet-In flow, the controller out-port action cannot be combined with other flow actions.

## Packet-Out Messages

The Packet-Out capability is enabled by default. You can use the following CLI command to disable Packet-Out messages:

```
config system open-flow-channel
    set packet-out-status disable
end
```



## Displaying Counters

The Packet-In and Packet-Out counters are added to the OpenFlow protocol counters.

Use the following CLI command to display the counters:

```
get open-flow protocol counters
hello-rx                : 13
hello-tx                : 34
...
port-status-tx          : 0
packen-in-tx            : 0
packen-out-rx           : 0
total-rx                : 4427671
total-tx                : 705083993
error-rx                : 0
error-tx                : 435988
```

Packet-In and Packet-Out error counters are added to the OpenFlow protocol error counters.

Use the following CLI command to display the error counters:

```
get open-flow protocol error-counters
hello-failed-incompatible-tx      : 0
...
unsupported-field-in-match-rx      : 0
bad-request-bad-table-id-rx      : 0
pkt-in-no-matching-flow-drops-tx : 0
pkt-in-connection-queue-overflow-drops-tx : 0
pkt-in-rate-queue-overflow-drops-tx : 0
pkt-out-unknown-pkt-buffer-rx     : 0
pkt-out-pkt-buffer-reuse-error-rx : 0
pkt-out-invalid-action-rx         : 0
pkt-out-invalid-in-port-rx        : 0
pkt-out-invalid-action-argument-rx : 0
no-connection-to-controller-drops-tx : 435988
```

# Logs and Reporting

Use the logs and reporting page to configure log settings and email alert settings.

## Log Browsing

**To browse the logs:**

1. Go to **Log & Report>Log Browsing**.
2. Select the sub-type of logs to browse: Configuration, System or Admin
3. (Optional) Click **Filter Setting** to filter by various attributes.

## Log Download

**To download a set of logs:**

1. Go to **Log & Report>Log Download**.
2. Select the sub-type of logs to download : Configuration, System or Admin.
3. Choose the start time and end time for the set of logs to be downloaded.
4. Click the **Download** button.

## Configuring Local Log Settings

The local log is a datastore hosted on the FortiCore system.

Typically, you use the local log to capture information about system health and system administration activities. We recommend that you use local logging during evaluation and verification of your initial deployment, and then configure remote logging to send logs to a log management repository where they can be stored long term and analyzed using preferred analytic tools.

Local log disk settings are configurable. You can select a subset of system events, traffic, and security logs.

**To configure local log settings:**

1. Go to **Log & Report>Log Setting**.  
**The configuration page displays the Local Log tab.**
2. Complete the configuration as described in the table below.
3. Save the configuration.

Settings	Guidelines
Status	Select to enable local logging.
File Size	Maximum disk space for a local log file. The default is 200 MB. When the current log file reaches this size, a new file is created.
Log Level	<p>Select the lowest severity to log from the following choices:</p> <ul style="list-style-type: none"> <li>• Emergency—The system has become unstable.</li> <li>• Alert—Immediate action is required.</li> <li>• Critical—Functionality is affected.</li> <li>• Error—An error condition exists and functionality could be affected.</li> <li>• Warning—Functionality might be affected.</li> <li>• Notification—Information about normal events.</li> <li>• Information—General information about system operations.</li> <li>• Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior.</li> </ul> <p>For example, if you select <b>Error</b>, the system collects logs with level Error, Critical, Alert, and Emergency. If you select <b>Alert</b>, the system collects logs with level Alert and Emergency.</p>
Disk Full	<p>Select log behavior when the maximum disk space for local logs (30% of total disk space) is reached:</p> <ul style="list-style-type: none"> <li>• Overwrite—Continue logging. Overwrite the earliest logs.</li> <li>• No Log—Stop logging.</li> </ul>
Event	Select to enable logging for events.

## Configuring Syslog Settings

A remote syslog server is a system provisioned specifically to collect logs for long term storage and analysis with preferred analytic tools.

### To configure syslog settings:

1. Go to **Log & Report>Log Setting**.
2. Click the **Syslog Server** tab.
3. Click **Add** to display the configuration editor.
4. Complete the configuration as described in the table below.
5. Save the configuration.

Settings	Guidelines
Status	Select to enable the configuration.
Address	IP address of the syslog server.
Port	Listening port number of the syslog server. Usually this is UDP port 514.
Log Level	<p>Select the lowest severity to log from the following choices:</p> <ul style="list-style-type: none"> <li>Emergency—The system has become unstable.</li> <li>Alert—Immediate action is required.</li> <li>Critical—Functionality is affected.</li> <li>Error—An error condition exists and functionality could be affected.</li> <li>Warning—Functionality might be affected.</li> <li>Notification—Information about normal events.</li> <li>Information—General information about system operations.</li> <li>Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior.</li> </ul> <p>For example, if you select <b>Error</b>, the system sends the syslog server logs with level Error, Critical, Alert, and Emergency. If you select <b>Alert</b>, the system collects logs with level Alert and Emergency.</p>
CSV	Send logs in CSV format. Do not enable CSV if you are using FortiAnalyzer.
Facility	Identifier that is not used by any other device on your network when sending logs to FortiAnalyzer/syslog.
Event	Select to enable logging for events.
Event Category	<p>Select the types of events to send to the syslog server:</p> <ul style="list-style-type: none"> <li>Configuration—Configuration changes.</li> <li>Admin—Administrator actions.</li> <li>Application—Health check results.</li> <li>System—System operations, warnings, and errors.</li> </ul>

## Configuring High Speed Logging

This feature is intended for deployments that require a high volume of logging activity. The logs are sent in binary format so they can be sent at a high speed. If you want to use high speed logging, contact Fortinet to obtain a utility for handling the binary format.

The high speed log feature supports traffic logs; event logs and security logs are not supported.

**To configure high speed log settings:**

1. Go to **Log & Report>Log Setting**.
2. Click the **High Speed Server** tab.
3. Click **Add** to display the configuration editor.
4. Complete the configuration as described in the table below.
5. Save the configuration.

Settings	Guidelines
Status	Select to enable the configuration.
Address	IP address of the syslog server.
UDP Port	Listening port number of the syslog server. Usually this is UDP port 514.

## Configuring Alert Email Settings

You can configure alerts to be sent based on either event categories or event severities. See [SNMP Settings](#) for information on how to set up the connection to the mail server.

**To configure alert email settings:**

1. Go to **Log & Report>Log Setting>Alert Mail**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

Settings	Guidelines
<b>By Category</b>	
By Category	Select this option to send alerts that match the specified categories. If you do not select this option, alerts are sent based on event severity.
Category	Select the events for which alerts are sent: <ul style="list-style-type: none"><li>• Admin</li><li>• Configuration</li><li>• Disk</li></ul>
<b>By Log Level</b>	

Settings	Guidelines
Log Level	<p>Select the lowest severity for which alerts are sent:</p> <ul style="list-style-type: none"> <li>• Emergency—The system has become unstable.</li> <li>• Alert—Immediate action is required.</li> <li>• Critical—Functionality is affected.</li> <li>• Error—An error condition exists and functionality could be affected.</li> <li>• Warning—Functionality might be affected.</li> <li>• Notification—Information about normal events.</li> <li>• Information—General information about system operations.</li> <li>• Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior.</li> </ul> <p>For example, if you select <b>Error</b>, the system sends alerts with level Error, Critical, Alert, and Emergency. If you select <b>Alert</b>, the system sends alerts with level Alert and Emergency.</p>
<b>General Settings</b>	
Interval	If identical alerts are occurring continuously, select the interval between each email that will be sent while the event continues.
From	Sender email address used in the alert email.
<b>Recipient</b>	
Recipient	Select <b>Recipient&gt;Add</b> to display the configuration editor.
Name	Recipient name to appear in the alert email.
Mail To	Recipient email address.



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.