



FortiPortal MEA - Administration Guide

Version 6.0.1 Beta

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



February 11, 2021

FortiPortal MEA 6.0.1 Beta Administration Guide

02-601-668064-20210211

TABLE OF CONTENTS

Change Log	4
Introduction	5
Key concepts	5
Customer sites	5
Storage limits	6
Remote authentication	6
Trusted hosts	6
How FortiPortal MEA works with FortiManager	7
Quick start	8
Enabling FortiPortal MEA	8
Adding customers	9
Adding customer sites	9
Adding customer users	10
Connecting to the portal	10
Viewing Reports	11
Adding FortiAnalyzer devices	11
Dashboard	11
Log View and Monitors	13
More information	16

Change Log

Date	Change Description
2020-12-23	Initial release.
2021-02-11	Added Connecting to the portal on page 10 .

Introduction

FortiPortal Management Extension Application (MEA) enables customers to operate a cloud-based hosted security management and log retention service. It provides end customers with centralized reporting, traffic analysis, configuration management, and log retention without the need for the end customer to invest in additional hardware and software.



You must enable the ADOM mode for FortiManager to work with FortiPortal MEA.
FortiPortal MEA 6.0.1 Beta requires FortiManager 6.4.4 or later, and you must be in a 6.4 ADOM to access FortiPortal MEA.

FortiPortal MEA is well-suited to multi-tenancy customers. For example, a managed security service provider (MSSP) can provide a self-service portal for FortiManager for a customer's managed security devices such as FortiGate devices, VDOMs, and FortiWiFi. Having both FortiManager and FortiPortal MEA provides new service revenue opportunities for MSSPs.

This section contains the following topics:

- [Key concepts on page 5](#)
- [How FortiPortal MEA works with FortiManager on page 7](#)

For information on FortiPortal MEA as a standalone product, see the [Fortinet Docs Library](#).

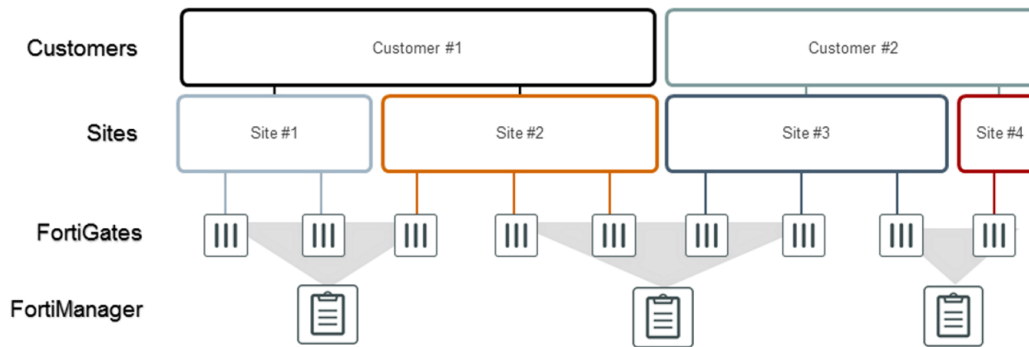
Key concepts

This section contains information about the following key concepts and features of FortiPortal MEA:

- [Customer sites on page 5](#)
- [Storage limits on page 6](#)
- [Remote authentication on page 6](#)
- [Trusted hosts on page 6](#)

Customer sites

- An end-customer can have multiple sites.
- A site is a logical grouping of devices (independent of which FortiManager manages the device).
- Devices are FortiGate devices or AP wireless devices.



Storage limits

Each end-customer has a storage capacity maximum amount, which is expressed as a number of GB of database storage.



By default, the storage size set for each customer is 100 MB.

The system requires other overheads as well, which may take 15 GB of storage. As a minimum, 40 GB of storage is required.

If a customer exceeds their storage limit, one of the following strategies is applied (this is configurable for each customer):

- Overwrite the oldest logs
- Stop logging

Remote authentication

You have the choice of local or remote user authentication of the Admin and Customer portal users. Local authentication works by defining the users in the local user databases. Remote authentication provides a choice of Radius authentication or FortiAuthenticator. The choice of authentication method is global to the whole FortiPortal.

If you set the authentication mode to remote, all user management functions reside with the remote system. FortiPortal user management capabilities (add/modify/delete users, reset password, change password) are blocked, as these apply only to local users.

For additional information regarding FortiAuthenticator, refer to the [FortiAuthenticator product documentation](#).

Trusted hosts

If you are using local user authentication, you can add the Trusted Hosts capability as an added level of security. You can apply the Trusted Hosts capability as a global feature. Optionally, you can add per-customer allowlists.

If you enable Trusted Hosts as a global setting, the system enforces a configurable blocklist and configurable allowlist for all admin and customer users.

You can also enable Trusted Hosts as a customer setting. The system creates an allowlist of trusted hosts for the customer users. The default entry in the allowlist is to allow all users, so you need to delete this entry to create a real allowlist.

For a customer with Trusted Hosts enabled, the system also enforces the global blocklist and allowlist for the customer users.

How FortiPortal MEA works with FortiManager

FortiPortal MEA requires that the customer FortiGate devices must be managed by FortiManager. FortiManagers may reside in the customer network or in the cloud.

FortiPortal MEA makes configuration changes to the assigned policy package, ADOM objects, and device manager settings using the FortiManager JSON API. The FGFM protocol is used for any changes between FortiManager and FortiGate devices.

When you add FortiManager to FortiPortal MEA, FortiPortal MEA polls FortiManager immediately to obtain information about managed devices. FortiPortal MEA subsequently polls FortiManager based on the configured polling frequency.

Quick start

This section provides a summary of how to get started with FortiPortal MEA:

1. Enable FortiPortal MEA. See [Enabling FortiPortal MEA on page 8](#).
2. Add customers. See [Adding customers on page 9](#).
3. Add customer sites. See [Adding customer sites on page 9](#).
4. Add customer users. See [Adding customer users on page 10](#).
5. Connect to the portal. See [Connecting to the portal on page 10](#).
6. View reports. See [Viewing Reports on page 11](#).
7. Add FortiAnalyzer devices. See [Adding FortiAnalyzer devices on page 11](#).
8. Monitor using the dashboard. See [Dashboard on page 11](#).
9. View security event logs and monitor information for a customer. See [Log View and Monitors on page 13](#).

For information on the limitations of FortiPortal MEA, see the *FortiPortal MEA Release Notes* on the [FortiManager page](#) of the [Document Library](#).

Enabling FortiPortal MEA

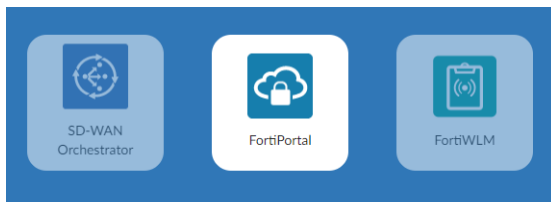
FortiManager provides access to the FortiPortal MEA application that is released and signed by Fortinet.



Only administrators with a *Super_User* profile can enable management extensions.
A CA certificate is required to install management extensions on FortiManager. See CA certificates in the *FortiManager Administration Guide*.

To enable FortiPortal MEA:

1. Ensure you are using ADOM version 6.4 or later.
2. Go to *Management Extensions*.
3. Click the grayed out tile for FortiPortal MEA to enable the application.
Grayed out tiles represent management extensions. In the following example, *FortiPortal* is enabled, and other management extensions are disabled.



4. Click *OK* in the dialog that appears. It may take some time to install the application.

To enable FortiPortal MEA in the CLI:

```
config system docker
```



```

set status enable
set fortiportal enable
end

```

Adding customers

The *Customers* tab shows summary information for each customer. The content pane lists the customer name and the number of devices per customer.

You can use the *Customers* tab to add or edit customers by entering customer details, information, and selecting other available options in the *Add/Edit Customer* dialog.

To add a customer, select *Add Customer* on the top-left of the *Customers* tab.

Customer Name ↑	# FGT VDOM / FSA Devices	Action
Customer-136	4/0	[Add] [Edit] [Delete] [Details]
Customer-230	7/0	[Add] [Edit] [Delete] [Details]

10 entries

Selecting a customer name in the *Customer* tab opens the customer portal for this customer in a new tab.

For details on filling in the *Add Customer* dialog, see the *FortiPortal Administration Guide* on the [Fortinet Docs Library](#).

Adding customer sites

Selecting the *Sites* (🏠) icon from the *Action* column on the *Customers* tab opens the *Sites* window.

To add a customer site, select *Add Site* on the *Sites* window, and fill in the dialog that appears.

Name ↑↓	Email ↑↓	Devices	Action
Site1		⚠️ ADOM60:FGVM0\$TM20003891/root ⚠️ ADOM62:FGVM0\$TM20003892/root ⚠️ root:FGVM0\$TM20003890/root ⚠️ root:FGVM0\$TM20003890\%dom1	[Wireless] [Edit] [Delete]

10 entries

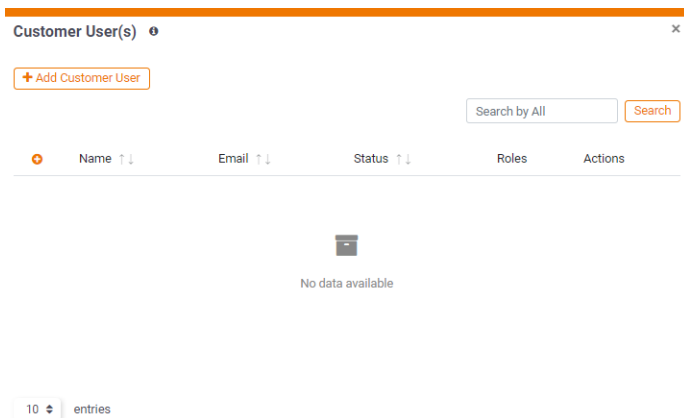
For information on customer sites, filling in the *Add/Edit Site* dialog, and wireless network, see the *FortiPortal Administration Guide* on the [Fortinet Docs Library](#).

Adding customer users

Selecting the *User(s)* (👤) icon from the *Action* column on the *Customers tab* opens the *Customer User(s)* window.

The *Customer User(s)* window displays information about the local administrative users for a customer.

To add a customer user, select *Add Customer User* on the *Customer User(s)* window, and fill in the dialog that appears.



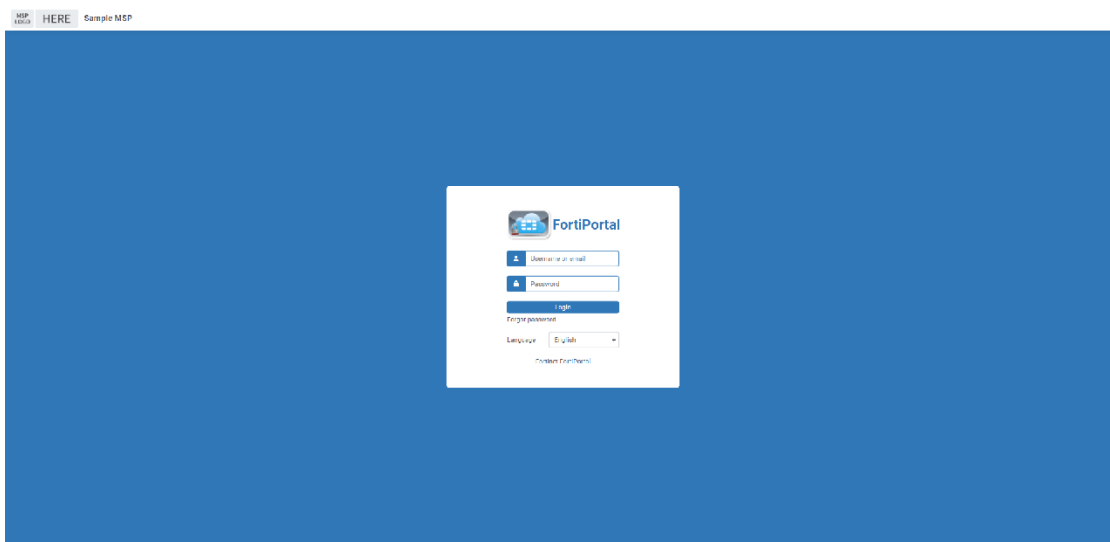
For information on customer users, filling in the *Add/Edit Customer User* dialog and roles, see the *FortiPortal Administration Guide* on the [Fortinet Docs Library](#).

Connecting to the portal

Once the customer site and the users are created, you can then connect to user side of the portal using the link:

`https://<fmqip>:4443/fpc/login`

The following figure shows the default landing page:



For information about the landing page, see the *FortiPortal User Guide* on the [Fortinet Docs Library](#).

Viewing Reports

Selecting the *Reports* (📊) icon from the *Action* column on the *Customers* tab opens the *Reports* window.

The *Reports* window displays information about the available reports to this customer.

The *Reports* tab on the customer portal displays a list of available FortiAnalyzer reports to this customer.



Whether a customer can create or run reports depends on the roles assigned to that customer user.

For information on reports and customer user roles, see the *FortiPortal Administration Guide* and the *FortiPortal User Guide* on the [Fortinet Docs Library](#).

Adding FortiAnalyzer devices

The *FortiAnalyzer* tab shows a list of all the FortiAnalyzer devices.

Go to *Devices > FortiAnalyzer*, and select *Add FortiAnalyzer* to add a new FortiAnalyzer device.

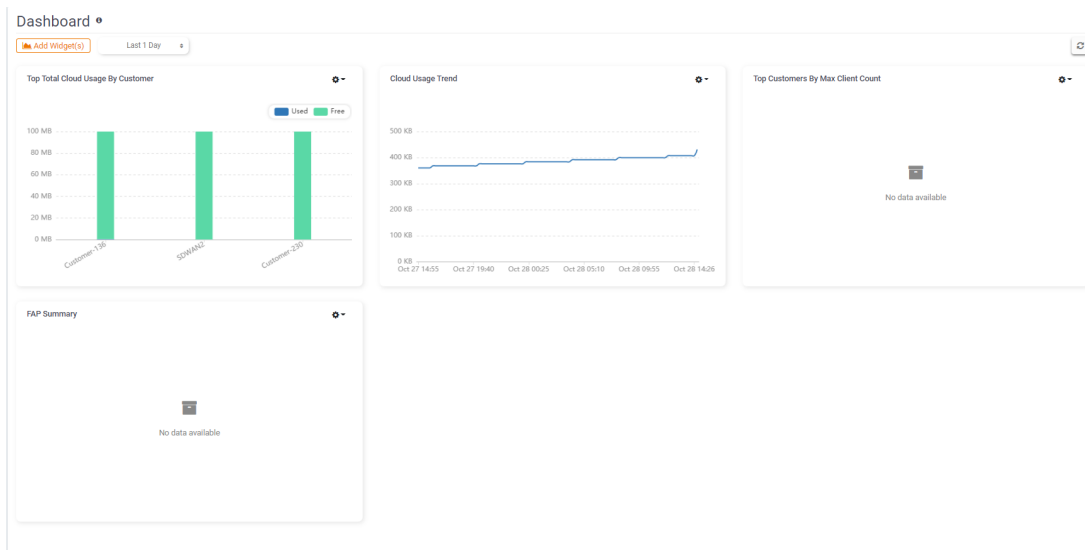
Name	IP Address/Domain Name	Status	Action
FAZ-89	192.168.1.1	Active	[Icons]
FAZ-107	192.168.1.2	Active	[Icons]

For information on prerequisites for setting up FortiAnalyzer devices, filling in the *Add/Edit FortiAnalyzer* dialog, and viewing FortiAnalyzer reports, see the *FortiPortal Administration Guide* on the [Fortinet Docs Library](#).

Dashboard

You can use the dashboard to see monitoring information.

On the service provider side, the dashboard displays information about the customers using a set of widgets.



On the customer side, the dashboard displays security event logs and other information for this customer using a set of widgets.



For information on dashboard widgets, see the *FortiPortal Administration Guide* and the *FortiPortal User Guide* on the [Fortinet Docs Library](#).

Log View and Monitors

You can use the *Log View* and the *Monitors* tab in *View* on the customer portal to display event logs and monitoring information for a customer.

The *Log View* tab displays information about the security event logs.

The following figure shows an example of the *Traffic* tab:

View / Log View

Traffic All Last 5 Minutes

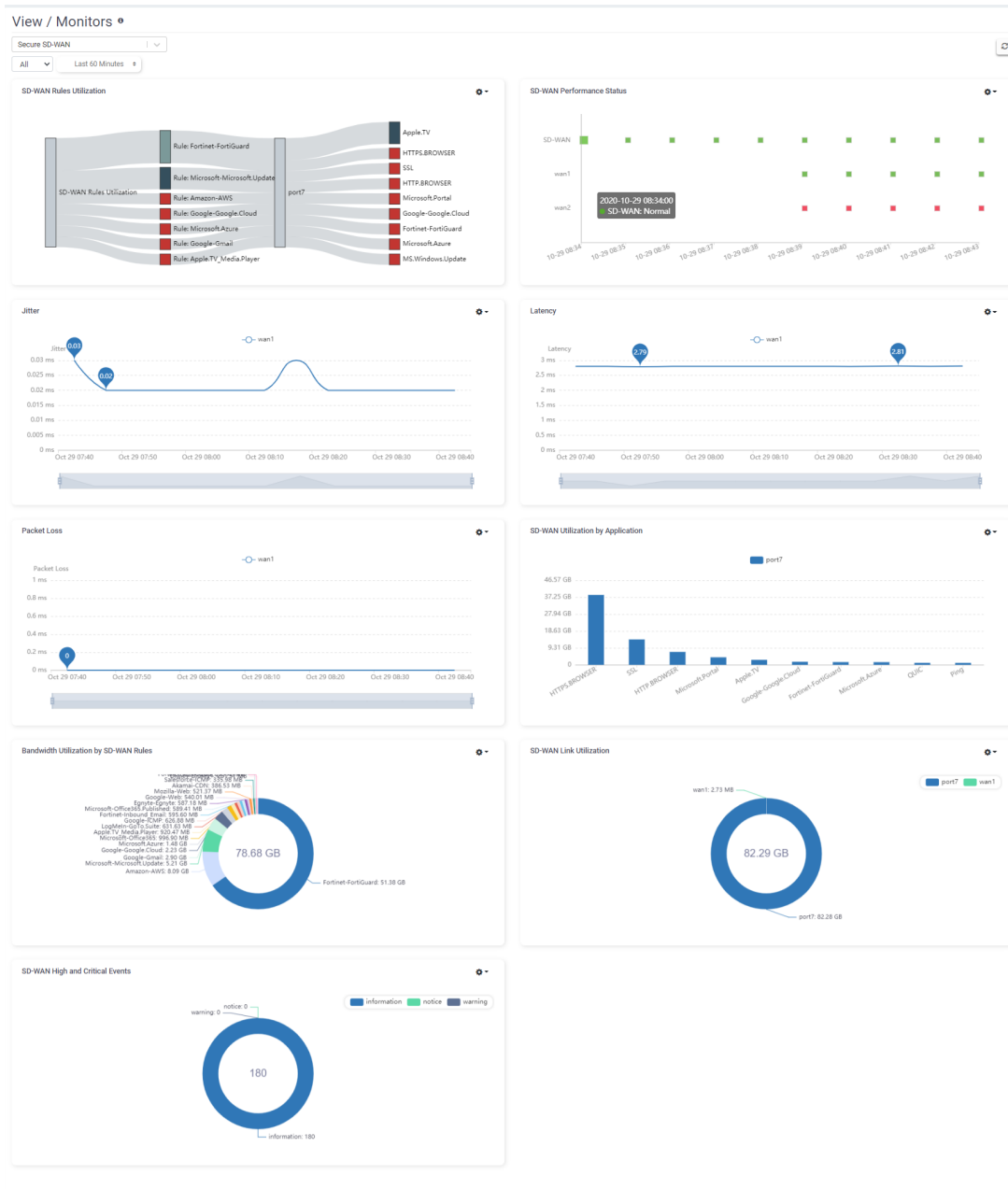
Date/Time	Device ID	Action	Source IP	Users	Destination IP	Service	Application	Category	Sent Bytes	Received Bytes
2020-10-29 08:39:59	FG3K5ETB19900075	deny	192.168.1.100		192.168.1.100	tcp/13033	tcp/13033 (Canada)	unscanned	0	0
2020-10-29 08:39:59	FG3K5ETB19900075	ip-conn	192.168.1.100		192.168.1.100	icmp/0/0	icmp/0/0 (Canada)	unscanned		
2020-10-29 08:39:59	FG3K5ETB19900075	client-rst	192.168.1.100		192.168.1.100	Fortinet-FortiGuard	SSL_TLSv1.3 (United States)	Network.Service	897	6.05 KB
2020-10-29 08:39:59	FG3K5ETB19900075	accept	192.168.1.100		192.168.1.100	PING	PING (Canada)	unscanned	300	88
2020-10-29 08:39:59	FG3K5ETB19900075	client-rst	192.168.1.100		192.168.1.100	Fortinet-FortiGuard	HTTPS.BROWSER (United States)	Web.Client	5.50 KB	5.38 KB
2020-10-29 08:39:59	FG3K5ETB19900075	client-rst	192.168.1.100		192.168.1.100	Fortinet-FortiGuard	SSL_TLSv1.3 (United States)	Network.Service	897	6.05 KB
2020-10-29 08:39:59	FG3K5ETB19900075	client-rst	192.168.1.100		192.168.1.100	Fortinet-FortiGuard	SSL_TLSv1.3 (United States)	Network.Service	897	6.05 KB
2020-10-29 08:39:59	FG3K5ETB19900075	client-rst	192.168.1.100		192.168.1.100	Fortinet-FortiGuard	HTTPS.BROWSER (United States)	Web.Client	7.96 KB	9.96 KB
2020-10-29 08:39:59	FG3K5ETB19900075	accept	192.168.1.100		192.168.1.100	Fortinet-FortiGuard	FortiGuard Search (Canada)	Cloud.IT	7.02 KB	3.27 KB
2020-10-29 08:39:59	FG3K5ETB19900075	accept	192.168.1.100		192.168.1.100	Fortinet-FortiGuard	FortiGuard Search (United States)	Cloud.IT	2.34 KB	1.63 KB

10 entries

1 2 3 4 5 6 ... 63 64

The *Monitors* tab shows information about SD-WAN, threats, and VPN.

The following figure shows an example of the *Secure SD-WAN* tab:



For more information, see the *Log View* and the *Monitors* section in the *FortiPortal User Guide* on the [Fortinet Docs Library](#).

More information

FortiPortal is available as follows:

- As a management extension application with FortiManager called FortiPortal MEA
For information about FortiPortal MEA, see the [FortiManager page](#) on the [Document Library](#).
- As a stand-alone product called FortiPortal
For information about stand-alone FortiPortal, see the [FortiPortal page](#) on the [Document Library](#).

This guide includes information about enabling and configuring FortiPortal MEA in FortiManager. It also provides information about how FortiPortal MEA works with FortiManager.

How administrators configure FortiPortal MEA differs slightly from configuring stand-alone FortiPortal. For information on configuring FortiPortal MEA, see this guide.

However end-customers use FortiPortal MEA the same way as stand-alone FortiPortal. As a result, end-customers can use the *FortiPortal User Guide* for information about using either stand-alone FortiPortal or FortiPortal MEA. For more information, see the *FortiPortal User Guide* on the [Fortinet Document Library](#).



FORTINET®



Copyright© 2021 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.