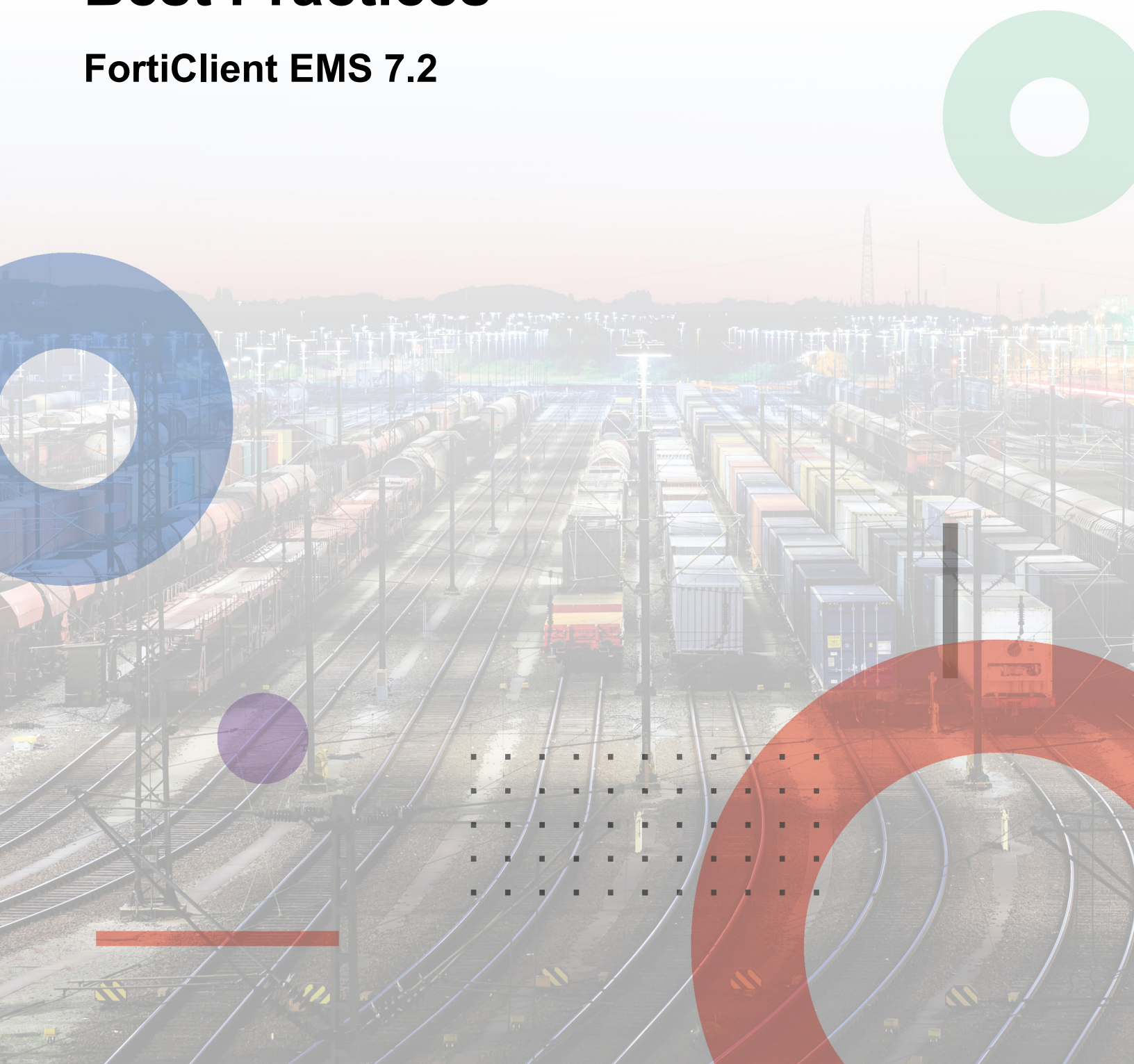
FORTINET

# Best Practices

## FortiClient EMS 7.2



**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO LIBRARY**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

April 29, 2025
FortiClient EMS 7.2 Best Practices
04-720-1051537-20250429

# TABLE OF CONTENTS

# Overview

This guide is a collection of best practices guidelines for using FortiClient EMS. Use these best practices to help you get the most out of your FortiClient EMS products, maximize performance, and avoid potential problems.

# Installing and licensing EMS

Before installing EMS, reviewing the server, hardware, software, and port requirements in the *FortiClient EMS Administration Guide* is recommended. Also, follow these guidelines:

- Ensure that EMS is installed on a dedicated server.
- Check that port 443 is not in use.
- Ensure access to EMS is available. Open any firewall ports as needed.
- By default, FortiClient EMS is installed with SQL Server Express. If you have an existing SQL Server instance (Express, Enterprise, or Standard) installed on the EMS server, you can customize the SQL Server instance by installing EMS using the CLI. When managing more than 5000 endpoints, using FortiClient EMS with SQL Server Enterprise or Standard is recommended. See Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise.

It is recommended to provide remote users direct access to the EMS server. In this case, you must configure EMS FQDN-accessible from the inside and outside. You must also open the following ports to allow client access:

- 8013: receive profile updates
- 10443: allow downloading software updates

# SQL database management

The following lists best practices when using SQL Server with FortiClient EMS:

- By default, EMS is installed with SQL Server Express. However, SQL Server Express has a 10 GB limit. If managing more than 5000 users, using EMS with a licensed SQL Server version, such as Enterprise or Standard, which support redundancy, backup, and more database entries and storage, is recommended.
- Perform SQL database backups regularly.
- Practice data redundancy to ensure an instance of the database is available at all times.

# EMS configuration

## Server settings

The following lists tasks that require direct access to the EMS console. You can do other tasks via remote HTTPS access.

- Decide whether to assign a fully qualified domain name or static IP address to FortiClient EMS. Do not assign a dynamic IP address to EMS.
- Enable remote HTTPS access for administrators.
- Set the hostname and FortiClient download URL. Ensure endpoints can access the download URL by going to it from a browser on an endpoint.

## Logs settings

Configure the log level and number of days to keep logs. These settings affect database size. If managing a large number of endpoints, reducing the number of days that EMS stores logs and alerts is recommended.

## FortiGuard settings

You can use FortiManager to download signature updates from FortiGuard. When managing more than 5000 endpoints, using FortiManager for local updates and category lookup is recommended.

See the FortiManager Administration Guide.

## Endpoints settings

| Setting | Description |
|---|---|
| *Keep alive interval* | Interval between endpoint connections to EMS to check for profile updates. If managing a large number of endpoints, a large number of endpoints frequently connecting to EMS can affect server and network performance. In this case, increasing the keepalive interval is recommended. |
| *EMS license timeout* | Useful for EMS administrators who manage reusing licenses. The minimum license timeout interval is one day. Modify this setting based on the number of licenses and of managed endpoints. |

# Administrator

- Change the password for the default administrator after logging in. Use a strong password that combines uppercase and lowercase letters, numbers, and symbols.
- Add a remote administrator.
- Add local Windows users.
- Super administrator permissions allow the administrator to access and modify all EMS settings. Restrict these permissions to as small a group as possible to ensure security for both the server and endpoints.
- You cannot configure an administrator to have access to only certain groups or organizational units within a domain. You can only configure an administrator to have full access to a domain or no access at all.

# Alerts settings

You can configure an email server and EMS to email alerts to you. Receiving alerts about non-compliant and unregistered endpoints is recommended.

| Alerts settings | Description |
|---|---|
| *EMS Alerts* | Enable receiving information in case of issues with EMS. |
| *Endpoint Alerts* | Enable receiving information about security events on endpoints. |
| *SMTP Server* | Configure to receive email alerts. |

# Endpoint provisioning

FortiClient EMS provides scalable and centralized management of multiple endpoints. One of the following endpoint management structures is recommended depending on the use case.

Before deploying to the production server, test deployment with a test endpoint group and test profiles. If the test deployment succeeds, attempt deployment on the production server.

| Use case | Endpoint management structure |
|---|---|
| Active Directory (AD) is set up and the same structure is desired for endpoint management. | AD integration:<br>• Put endpoints in organizational units (OU)<br>• Keep OU structure<br>• Group changes made in EMS do not sync back to AD (one-way sync only)<br>• EMS does not import endpoints in security groups |
| Large deployment that needs custom grouping or does not have AD setup | Automated group assignment. See Group assignment rules for details. |
| Small deployment | Custom groups:<br>• Manually create groups in EMS, then move endpoints into groups<br>• By default, endpoints are placed in the *Other Endpoints* group |

Endpoint provisioning consists of the following steps. For details on each step, see the *FortiClient EMS Administration Guide*.

1. In 7.2, you cannot deploy initial FortiClient installations to AD domain-joined devices. See Initially deploying FortiClient software to endpoints. You must use one of the following methods to deploy FortiClient:
   - Microsoft System Center Configuration Manager or group policy object
   - Mobile device management
   - Send installer link to end users
2. Create a deployment package. Select the desired FortiClient features to deploy to endpoint. See FortiClient feature recommendations on page 10 for details.
3. Assign the deployment package to desired endpoint groups using *Manage Deployment*.
4. Create endpoint policies to assign endpoint profiles and on-fabric detection rules to groups of Windows, macOS, and Linux endpoints. The *Endpoint Policy & Components* > *Manage Policies* page provides a comprehensive summary of which endpoint policies are applied to which endpoint groups.

FortiClient endpoints lock configuration changes in the FortiClient console. The end user cannot change the configuration.

Create a profile for the *Other Endpoints* group, and assign the profile to the group. This allows you to assign preferred settings to any FortiClient endpoints assigned to the *Other Endpoints* group.

# FortiClient feature recommendations

When creating deployment packages in FortiClient EMS to deploy FortiClient to endpoints, including different sets of FortiClient features to install depending on the endpoint is recommended. Do not install components that are not required. For example, if you have no users who need to access the network remotely, do not install Remote Access.

| Endpoint description | Recommended features |
|---|---|
| No third-party antivirus (AV) product installed | • Fortinet Security Fabric Agent (Vulnerability Scan)<br>• Advanced Persistent Threat (APT) Components (FortiSandbox)<br>• AntiVirus, Anti-Exploit<br>• Web Filter |
| Only VPN needed (endpoint already has a third-party AV product installed) | • Security Fabric Agent (Vulnerability Scan)<br>• Secure Access Architecture Components (SSL and IPsec VPN)<br>• Zero trust network access (ZTNA)<br>• Web Filter |

The following lists the recommended options to enable for each feature:

| Feature | Recommended options |
|---|---|
| AntiVirus | • *Block Access to Malicious Websites*<br>• *Block Known Communication Channels Used by Attackers*: uses Application Firewall. If Application Firewall is disabled, it is still active if you enable *Block Known Communication Channels Used by Attackers*.<br>• *Automatically Submit Suspicious Files to FortiGuard for Analysis*: unless the organizational security policy restricts it, enabling this option is recommended. It allows faster malicious file detection.<br>• *Exclusions*: follow the OS and other software vendors' recommendations to configure AV scan exclusions. Configuring recommended exclusions on servers is recommended.<br>• If you deploy FortiClient on a Windows Server with Web Filter and Application Firewall components, disable *Block Access to Malicious Websites* and *Block Known Communication Channels Used by Attackers*. Also disable *Scan Email* for Windows Servers.<br>• Enable *Identify Malware and Exploits Using Signatures Received From FortiSandbox*.<br>• Set *Action on Virus Discovery* to *Quarantine infected files*.<br>• Enable *Scan Network Files* only if you will not install FortiClient on file servers. If you will install FortiClient on a file server, enabling Malware Protection on the server and disabling *Scan Network Files* on workstation profiles is advised to avoid scanning the same files several times.<br>• *Machine Learning Analysis*<br>• *Scheduled Scan*<br>• *Cloud-Based Malware Protection*<br>• *Anti-Ransomware* |

| Feature | Recommended options |
|---|---|
| | • *Anti-Exploit*<br>• *Scan Removable Media on Insertion* |
| Web Filter | • Block the *Security Risk* site category.<br>• Enable *Client Web Filtering When On-Net*.<br>• *Client Web Filtering When On-Fabric*: enable if using Off-Fabric profiles to ensure Web Filter is enabled even when the endpoint is On-Fabric.<br>• *Log All URLs* and *Log User Initiated Traffic*: logged to FortiAnalyzer only and not to EMS.<br>• *Exclusion List*. See Web Filter.<br>• Set *Block* for *Allow websites when rating error occurs*.<br>• *Web Browser Plugin for Web Filtering*<br>• Enable *Log All URLs* for FortiClient to send logs to FortiAnalyzer.<br>• Set *FortiGuard Server Type* as *FortiGuard Anycast*. |
| VPN | Using IPsec VPN or ZTNA is recommended over using SSL VPN.<br>The following options are available when configuring a VPN tunnel:<br>• *Secure Remote Access*<br>• *Keep Running* for *Always up*<br>• `<use_gui_saml_auth>0</use_gui_saml_auth>`<br>• Configure Azure auto login.<br>• *Allow Non-Administrators to Use Machine Certificates*: you must configure `<run_fcauth_system>`. See IKE settings.<br>• *Save Password*<br>• *Auto Connect*<br>• *Enable Local LAN*<br>• *Dead Peer Detection*: disabling this option is recommended when on a poor connection, as this option can cause dropped connections.<br>• *Enable Implied SPDO*<br>• *Auto Keep Alive*<br>• *On Connect/On Disconnect Scripts* |
| Vulnerability Scan | • Configure *Scheduled Scan*.<br>• Enable *Automatic Patching* for vulnerabilities that are rated *High* and above.<br>• FortiClient cannot patch some programs, such as Adobe software and Java, automatically. For these programs, manual patch is required. See Manually fixing detected vulnerabilities.<br>• *Scan on Vulnerability Signature Update* |
| System Settings | • *UI > Require Password to Disconnect from EMS*: you can use a password lock to allow end users to disconnect FortiClient from EMS using a configured password. Instead of disabling the option for users to disconnect, enabling it and configuring the password lock is recommended. This allows administrators to disconnect FortiClient using the configured password when needed and is useful for troubleshooting scenarios.<br>• *Log > Level*: setting the log level to *Debug* is not recommended, except for troubleshooting purposes. |

| Feature | Recommended options |
|---|---|
| | • *Update* > *Use FortiManager for Client Signature Update*: FortiClient downloads updates directly from FortiGuard servers. Ensure all endpoints can access the update servers. If FortiManager is present, you can use it to receive signature updates.<br>• *Update* > *FortiGuard Server Type: FortiGuard Anycast*<br>• *Endpoint Control* > *Disable Unregister*: when enabled, FortiClient cannot disconnect from EMS. Using *Require Password to Disconnect from EMS* instead is recommended.<br>• *Endpoint Control* > *On-Net Subnets* and *Endpoint Control* > *Gateway MAC Addresses*: See On-fabric Detection Rules for how FortiClient determines on-net/off-net status. The MAC address list is optional and can only be used with on-net subnet configuration.<br>• *Endpoint Control* > *Send Software Inventory*: get application inventory.<br>• *Invalid Certificate Action*: *Deny* or *Warn* |

Since Windows Server supports a limited feature set, creating separate installers for Windows Server where only AV is enabled is recommended. Windows Server does not support Application Firewall, so you must disable this feature on the installer. To view the features that Windows Server supports, see Product integration and support.

When creating a deployment package, if you enable *Keep updated to the latest patch*, the deployment package is automatically updated when a new FortiClient version is available on FortiGuard distribution servers, then deployed to endpoints. To control software updates manually, disable this option. Disabling this feature on installers used to deploy FortiClient to servers is recommended to prevent uncontrolled service disruption during a FortiClient upgrade.

If a FortiGate is present, set up a Fabric connection to between EMS and FortiGate for better visibility and control over endpoints.

# FortiClient hardening

FortiClient hardening reduces security risk by eliminating potential attack vectors and shrinking FortiClient's attack surface. Some of the best practices described previously in this document contribute to the hardening of FortiClient with additional hardening steps listed here.

## Disabling or enabling locked settings

You can lock settings in EMS to prevent users from disabling or modifying key security features like real-time protection, firewall rules, or VPN.

In EMS, go to *Endpoint Profiles*, select or create a profile, and lock the desired settings. See Endpoint Profiles.

## Password protection to prevent unauthorized FortiClient uninstall

You can configure *Require Password to Disconnect from EMS* to ensure that users enter an admin password before disconnecting from EMS, adding security against unauthorized disconnection. See System Settings.

## Network lockdown

Network lockdown blocks all network traffic if the VPN connection is inactive, ensuring data security. Configure this locally when configuring a VPN connection in FortiClient or via EMS profiles to enforce lockdown when the VPN tunnel is not established. See Remote Access.

## Antiransomware

Antiransomware can protect specific data from unauthorized changes or encryption. In EMS, go to the desired *Malware Protection* profile and enable antiransomware and define what resources to protect. See Malware Protection.

## Encrypting backup configuration file

FortiClient supports encrypted backup configuration files. When backing up configurations, users can opt to encrypt the backup with a password, though this is more about securing the backup than the configuration in use. See Backing up the full configuration file.

## Allow User to Shutdown When Registered to EMS

Allow admin and non-admin users to shut down FortiClient from FortiTray even when FortiClient is still registered to EMS.

## FortiClient Service monitoring

The Scheduler.exe daemon provides service monitoring. It starts required FortiClient processes when FortiClient is started. It also monitors FortiClient running processes and automatically restarts the processes if they should be running but were stopped or terminated for any reason.

# EMS maintenance

The following lists best practices for EMS maintenance:

- Ensure to regularly upgrade FortiClient EMS whenever a new version is available. For details on each release, check the *FortiClient EMS Release Notes*.
- Back up the EMS database weekly by going to *Administration* > *Back up Database*.
- Review alerts regularly.
- For details on migrating EMS to a new server, see Use Case: Migrating EMS to a New Server.

To ensure server security, follow these best practices for server hardening:

- User account best practices:
  - Configure user accounts with strong, complex passwords. Change passwords regularly. Do not reuse passwords.
  - Lock accounts after a number of login failures. Login failures may be illegitimate attempts to gain access to your system.
  - Do not permit users to configure accounts with empty passwords.
  - Limit user accounts to access only what they need. Increased access should only be granted on an as-needed basis.
- Firewall best practices:
  - Configure the system firewall. Proper setup of a firewall can prevent many attacks.
  - Consider using a hardware firewall.
- Avoid using insecure protocols that send your information or passwords in plain text format.
- Minimize unnecessary software on your servers.
- Keep your operating system up-to-date. Ensure to install any security patches.
- Minimize open network ports to only what is needed for your specific circumstance.
- Maintain proper database backups.
- Ensure physical server security.

# Troubleshooting

## Seeing the file path for a vulnerable application

You can see the file path for a vulnerable application in FortiClient.

**To see the file path for a vulnerable application:**

1. In FortiClient on the endpoint, go to *Vulnerability Scan*, then click the number of total vulnerabilities.
2. Expand the desired vulnerability. FortiClient displays the file path for the vulnerable application.

## Gathering debug logs

**To gather debug logs:**

1. Create an endpoint profile intended for troubleshooting.
2. Set the log level to *Debug*.
3. Create a new endpoint group, then move the desired endpoint to the group.
4. Assign the new profile to an endpoint policy, then assign the endpoint policy to the group. This turns on debugging for the endpoint.
5. Repeat the desired action on the endpoint.
6. Run the Diagnostic Tool in FortiClient and send the output to Fortinet support.
7. Set the log level in the profile back to *Info*.

If experiencing slow performance or abnormally high CPU usage with FortiClient, enabling then disable Application Firewall, then AntiVirus, is recommended. This may solve the issue without need for further troubleshooting.

# Change log

| Date | Change description |
|---|---|
| 2024-07-10 | Initial release. |
| 2024-08-13 | Updated FortiClient feature recommendations on page 10. |
| 2024-12-31 | Added FortiClient hardening on page 13. |
| 2025-04-29 | Updated Installing and licensing EMS on page 5. |

www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.