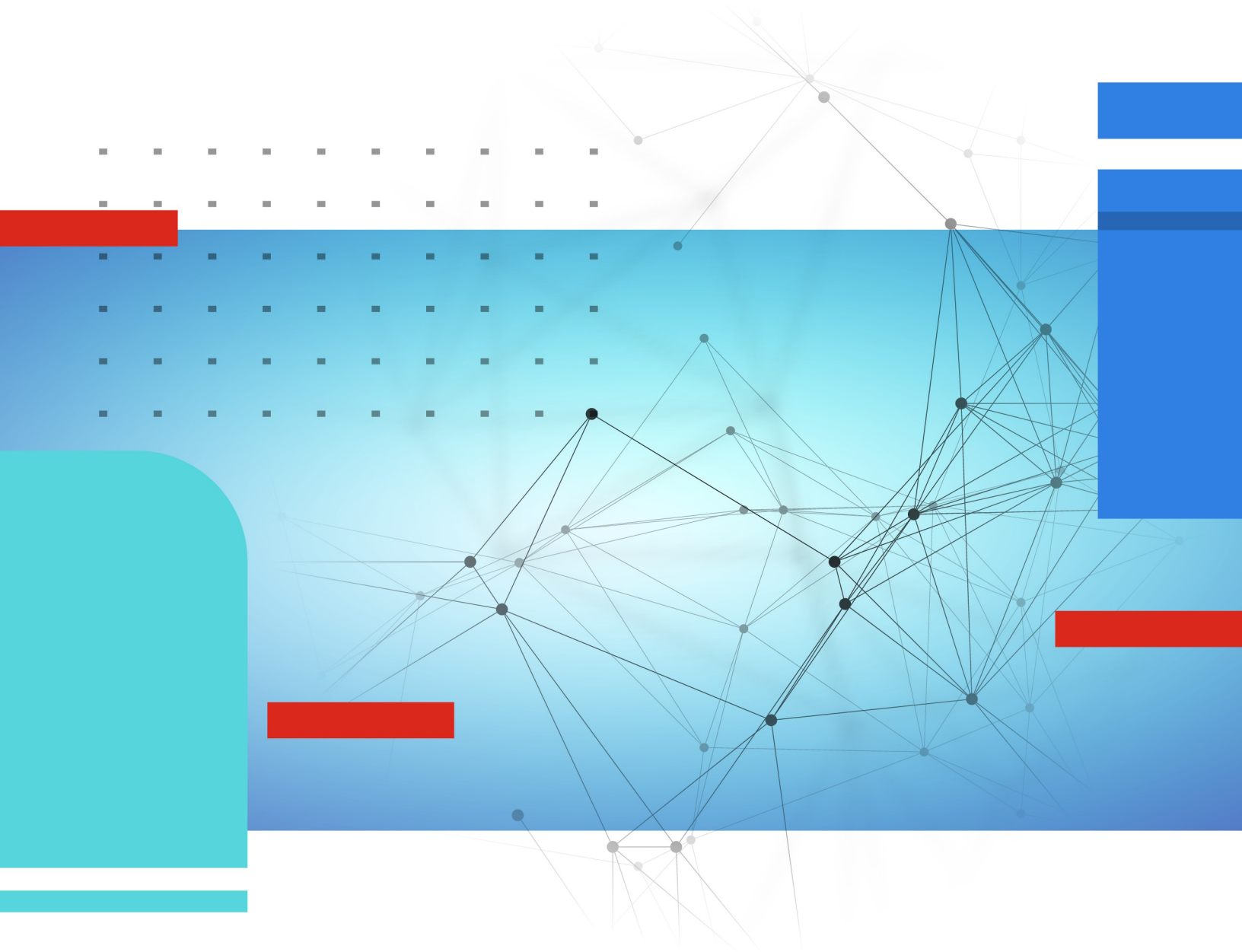
Release Notes

FortiSandbox 5.2.0



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

June 11, 2026
FortiSandbox 5.2.0 Release Notes
34-520-1112093-20260611

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-06-09	Initial release of version 5.2.0.

Introduction

This document provides the following information for FortiSandbox version 5.2.0 build 0290.

New features and enhancements

The following is summary of new features and enhancements in version 5.2.0. For details, see the *FortiSandbox 5.2.0 Administration Guide* in the Fortinet Document Library.

GUI

- Introduced a new dashboard page to showcase FortiSandbox's malware scanning and detection capabilities.
- Introduced a new *Threat Intelligence* menu.
- Enhanced Job Details reports for detected suspicious files with enriched FortiGuard Threat Intelligence.
- Enhanced Cloud VM naming to reflect support for Windows, Linux, Android, and macOS.
- Added Lite-Mode-specific *Top 5 File Types* and *Top 5 0-Day Malware Categories/Top 5 Suspicious URL Categories* widgets to the dashboard.
- Added a warning banner when global conserve mode is active.
- Added trap port number configuration for SNMP v3.
- Added support for adjusting image category ratings.
- Added a consolidated MITRE ATT&CK matrix view for all threats within a selected time period.
- Added best practice compliance checklists to the System menu.
- Improved archive file ratings to indicate *Clean* (contains malicious/suspicious files) when risky child files are present.
- Improved *Job Detail* visibility and *Tree View* readability
- Updated the Modify URL package to the same style as the Malware Package.
- Migrated the GUI to the Neutrino framework to improve modularity, maintainability, and consistency with other Fortinet products.

Security Fabric & Deployment

- Introduced Sentinel Mode support for AWS S3 buckets using event-driven notifications to enable faster detection of new files.
- Added webhook-based callback support to push FortiSandbox detection results and job completion notifications to FortiSOAR for streamlined integration and automation.
- Added support for processing up to 10,000 FortiClients in FortiSandbox.
- Added support for Hyper-V on Windows Server 2025.
- Added support for .hta files in Inline Block Profile file types.
- Added support for Android, Linux, and macOS files for ILB by allowing inline devices to submit jobs with the APT_ILB service flag while skipping prefiltering.

- Improved ICAP resiliency and request handling when the system enters conserve mode.

Scan & Engine

- Introduced Lightning mode to reduce storage by not saving clean job details.
- Introduced image categorization using the new AI-based FIRE engine, with support for OCR and QR code extraction.
- Introduced a new AV scan daemon to improve ICAP quick scan performance.
- Enhanced dynamic scan performance to complete in as fast as 15 seconds.
- Enhanced Inline Block to return results faster when a suspicious file condition is detected during compressed file handling.
- Enhanced NetShare scanning with event-driven support and reduced minimum interval to one minute.
- Enhanced the ICAP adapter to return results faster when a suspicious file condition is detected during compressed file handling.
- Enhanced the scan flow for URL detonation jobs to better handle multi-stage evasion techniques involving layered payload delivery.
- Enhanced NetShare to resume scanning after reboot in standalone and cluster modes.
- Enhanced URL processing.
- Added support for embedded URL extraction in executable script files.
- Added support for extracting URLs from SVG files.
- Added support for extraction and analysis of URLs embedded in all file types.
- Added support for unpacking Microsoft Outlook PST files.
- Added global conserve mode.
- Added support for unpacking LZIP archives.
- Added support for rescanning previously dynamically scanned jobs.
- Added support for a new Android Docker environment.
- Added support for AndroidVM6 on FortiSandbox 5.2, with outdated AndroidVM or AndroidVM5 automatically disabled during initialization.
- Increased the maximum timeout for full scan operations via the ICAP adapter to 30 minutes.

Threat Intelligence

- Introduced a new malware clustering model based on dynamic sandbox behavior, using machine learning–based scoring.
- Enhanced embedded URL visibility with QR code or direct URL display on the Job Details report page.
- Enhanced the Incident Assist page to list manual file uploads and URL detonation analysis jobs.
- Enhanced Threat Intelligence with automated IOC validation against FortiGuard for every suspicious file, replacing on-demand queries.
- Added detailed information for installer file types to PDF reports (e.g., Nullsoft Installer, MSI, EXE).

System & Security

- Introduced Data-at-Rest Encryption (DARE) support for system storage.
- Enhanced Certificate Authority (CA) management by centralizing usage across multiple locations.
- Added an option on the *diagnose debug* CLI command to debug report generation.
- Added email alerts when the system enters and exits conserve mode.
- Enhanced system security and stability.
- Improved data preparation for the Scan Performance widget to enhance accuracy and responsiveness.

Logging & Reporting

- Enhanced CSV report functionality with predefined columns.
- Enhanced TAC reports to display conserve mode value and status.

CLI & API

- Introduced a new URL deep scan feature with recursive analysis, redirect handling, and chained URL detonation to detect multi-stage malware across multiple link combinations and levels.
- Enhanced the API to support image category scoring.
- Added a *Submit multiple files* option to the administrator creation API.
- Added the `paix-ioc` CLI to enable or disable enriched PAIX IOCs.
- Added a dedicated mode for cluster nodes that operate as primary or secondary members without performing any scanning functions.
- Added power status(`ps-status`) monitoring for 1500G models.
- Added support for the `ps-status` command on models beyond 3000E and 3000F.
- Added the `scan-perf` CLI command to capture scan performance statistics for tracking and troubleshooting.
- Added an option in the `embeddedurl` CLI to configure the number of embedded URLs extracted per scan job for dynamic scan.
- Renamed the CLI command `sandboxing-embedded-url` to `sandboxing-embeddedobj` to reflect support for multi-stage URL scanning and embedded object analysis.

Upgrade Information

Before upgrade

Before any firmware upgrade, save a copy of your FortiSandbox configuration by going to *System > System Recovery*.

If you intend to use the new VMs after upgrade:

Ensure you have the appropriate VM licenses. Activating a VM requires the license specific to the version you are using with the equal number of clones. For example, if you have Win11 and Office 2021 activation keys you can use those keys to run the *Win11O21 VM*. If you want to configure 10 clones, then you will need 10 licenses.

Keep the following considerations in mind:

- We recommend purchasing a new license, downloading the VMs, and then reassigning the clones.
- If you download the new VMs (without updating your license) and then remove existing clones to make room for new ones, the old license will not work.

For more information about license keys, see *VM Settings > Optional VMs* in the *FortiSandbox Administration Guide*.

For a list of supported hardware and VM models, see Supported models on page 12.

Downgrading to previous firmware versions

Downgrading to previous firmware versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Fortinet Customer Service & Support portal located at https://support.fortinet.com. After logging in, select *Support > Downloads > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Upgrade procedure

Upgrading FortiSandbox firmware consists of the following steps:

1. Download the firmware image from the Fortinet Customer Service & Support portal.
2. When upgrading via the CLI, put the firmware image on a host that supports file copy with the SCP or FTP command. The FortiSandbox must be able to access the SCP or FTP server.
   In a console window, enter the following command string to download and install the firmware image:
   `fw-upgrade -b -s<SCP/FTP server IP address> -u<user name> -t<ftp|scp> -f<file path>`
3. When upgrading using the GUI, go to *Dashboard* > *Insights*. In the *System Information* widget, click anywhere inside the card and select *Update Firmware*. The *Firmware Upgrade* window opens. Follow the prompts to either select the recommended release for an automatic upgrade or browse to a firmware image on your management computer and click *Submit* to perform a manual upgrade.
4. Microsoft Windows Sandbox VMs must be activated against the Microsoft activation server if they have not been already. This is done automatically after a system reboot. To ensure the activation is successful, port3 of the system must be able to access the Internet and the DNS servers should be able to resolve the Microsoft activation servers.

Upgrade path

FortiSandbox 5.2.0 officially supports the following upgrade path.

Upgrade from	Upgrade to
5.0.6	5.2.0
5.0.0 - 5.0.5	5.0.6
4.4.0-4.4.9	5.0.0

To download the latest engine:

1. Log in to FortiCloud.
2. In the banner, click *Support* > *Service Updates*.
3. On the *FortiGuard Updates* page, click *FortiSandbox* and select the OS version.

Upgrade Notice

FortiSandbox Hyper-V model

1. Delete all checkpoints of the Virtual Machine instance that will be upgraded.
2. Power off the instance.
3. In Hyper-V Manager, go to the instance *Settings* > *IDE Controller* > *Hard Drive* > *Edit*. Increase the *fsa.vhdx* value to be larger than 1GB .

Cluster environments

Before upgrading, it is highly recommended that you set up a cluster IP so the failover between primary and secondary can occur smoothly.

In a cluster environment, use this upgrade order:

1. Upgrade the workers and install the new rating and tracer engine. Then wait until the devices fully boot up.
2. Upgrade the secondary and install the new rating and tracer engine. Then wait until the device fully boots up.
3. Upgrade the primary. This causes HA failover.
4. Install the new rating and tracer engine on the old primary node. This node might take over as primary node.

After upgrade

After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox so that web UI screens display properly.

Tracer and Rating Engines

The tracer and rating engines are automatically downloaded by the FortiSandbox from FortiGuard. For air-gapped mode, the engines are available for download from our Support site.

Rating engine

Every time FortiSandbox boots up, it checks FDN for the latest rating engine.

If the rating engine is not available, you get these notifications:

- A warning message informs you that you must have an updated rating engine.
- The *Dashboard System Information* widget displays a red blinking *No Rating Engine* message besides *Unit Type*.

If necessary, you can manually download an engine package from Fortinet Customer Service & Support.

If the rating engine is not available, FortiSandbox functions in the following ways:

- FortiSandbox still accepts on-demand, network share, and RPC submissions, but all jobs are pending.
- FortiSandbox does not accept new devices or FortiClients.
- FortiSandbox does not accept new submissions from Sniffer, Device, FortiClient, or Adapter.

> ⚠ After upgrading, FortiSandbox may stop processing files until the latest tracer, rating, and AV engines are installed through a FDN update or manual upload. Because the tracer and rating engines are large, allow sufficient time for the download.

AV Engine Upgrade Notification

Upgrading to FortiSandbox 5.2.0 installs AV engine version 8 and removes the existing AV scanner and signatures. System notifications are displayed until the new AV signatures are installed. No action is required.

Supported models

FortiSandbox	FSA-500F, FSA-500G, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000E, FSA-3000F and FSA-3000G.
FortiSandbox-VM	ALI, AWS, Azure, GCP, OCI, Hyper-V, KVM, Nutanix and VMware ESXi.

For more information on VM, see the VM Installation Guide in the Fortinet Document Library.

Product Integration and Support

The following table lists FortiSandbox 5.2.0 product integration and support information. FortiSandbox integration and support is tested based on the firmware image of the product's latest available GA build during the release testing process. FortiSandbox also supports backwards compatibility to the product's earlier GA builds.

FortiSandbox integration and support is tested on the firmware image of the product's major release (*7.0.0, 7.2.0, 7.4.0* etc). Minor releases (*7.0.1, 7.0.2, 7.0.3* etc) are not individually tested because they are based on the same firmware image.

Where indicated, version *x.x.x and later* means integration and support is based on the major version, including minor versions unless otherwise indicated in the *Administration Guide* or *Release Notes*.

Web browsers	• Google Chrome version 147 • Microsoft Edge version 147 • Mozilla Firefox version 147 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 8.0.0 • 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiAnalyzer	• 8.0.0 • 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiManager	• 8.0.0 • 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiMail	• 8.0.0 • 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiClient	• 7.4.0 and later • 7.2.0 and later
FortiEMS	• 7.4.0 and later • 7.2.0 and later
FortiADC	• 8.0.0 and later • 7.6.0 and later

	• 7.4.0 and later
FortiProxy	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiWeb	• 8.0.0 and later • 7.6.0 and later • 7.4.0 and 7.4.1
FortiEDR	• 6.2.0 and later • 5.2.0 and later
FortiSOAR	• 7.6.5 and later
AV engine	• 00008.00014
FortiSandbox System tool	• 5002.00112
Traffic Sniffer Engine	• 00007.01184
Virtualization environment	• VMware ESXi: 5.1, 5.5, 6.0, 6.5, 6.7, 7.0.1, 8.0, and 9.0 • KVM: CentOS 8, 9 and Ubuntu 22 • Microsoft Hyper-V: Windows server 2016, 2019, 2022, and 2025 Hyper-V • Nutanix: AHV

Special Notices

Deprecation of NFSv2 and SMB1.0

NFSv2 and SMB1.0 are deprecated as of release 5.2.0 and will be removed in a future major release.

These protocols are considered obsolete and are no longer maintained or recommended by most vendors. Most environments have transitioned to newer protocol versions that provide improved performance, reliability, and security.

Support for NFSv2 and SMB1.0 currently applies to:

- NetShare
- Quarantine
- Job Archive

Customers should migrate to supported protocol versions to avoid disruption:

- NFSv3 and NFSv4 are supported alternatives to NFSv2
- SMB2 and SMB3 are supported alternatives to SMB1.0

Deprecated CLIs

Deprecated and removed the following CLI commands: anti-phishing, iptables, oftp-con-mode, ocr-scan, and sandboxing-embeddedurl (replaced by sandboxing-embeddedobj) from 5.2.0.

Deprecated VMs

Windows VMs

Windows 7x VMs are no longer supported as of version 5.2.0; to maintain system stability, set the WIN7X clone value to 0 in the VM settings.

Android VMs

FortiSandbox now automatically detects outdated Android virtual machines during VMINIT. When an older Android VM (such as AndroidVMV5) is present, the system disables it and generates a critical warning log to

ensure correct Android file scanning. Only AndroidVMV6 or newer is supported for Android analysis.

Resolved Issues

The following issues have been fixed in FortiSandbox 5.2.0. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
0627506	Fixed an issue where the authentication method was not displayed after creating a user with two-factor authentication enabled.
1144262	Fixed an issue where on-demand direct URL submissions did not support port numbers.
1210323	Fixed an issue with improper session handling.
1215283	Fixed an issue where CSRF verification failed when creating a local or LDAP administrator account.
1234396	Fixed an issue where FortiSandbox in air-gap mode showed the FortiGuard update status as Unknown after a reboot.
1239465	Fixed an issue where FQDNs containing dashes could not be added as NTP servers.
1289866	Fixed a FortiGuard update issue by adding support for both current and upcoming FDN server certificates.

Fabric integration and Deployment

Bug ID	Description
1180040	Fixed an issue where FortiSandbox attempted to resolve mac, mac2, fsavm, and fqdl when deployed in air-gap mode.
1236888	Fixed an issue where FortiGuard AV updates caused timeouts for the ICAP client.
1281865	Fixed an issue where PNG, JPG, or TXT files were not submitted to FortiSandbox from FortiGate when the FSA primary was in management mode.
1283995	Fixed an issue where *srcip/dev* fields from ICAP traffic were sometimes incorrect in a cluster environment.

Bug ID	Description
1284615	Fixed an issue where users could not save the configuration when the Share Path included a “$” character.

Scan and Engine

Bug ID	Description
1191884	Dynamic scan performance on FSA KVM VMs running FC4 with 128 CPUs is lower than on FC3 with 64 CPUs.
1201522	Fixed issue of malware package if upgraded to 5.0.4 from prior 5.0.2.
1218631	Fixed an issue where the system was still querying the APT server when the remote Windows cloud VM was disabled.
1221200	Fixed an issue where the Sandbox quarantine placeholder file did not replace the original file.
1223830	Fixed an issue where malicious files were not detected when FortiSandbox Community Cloud was disabled.
1223830	Fixed an issue where malicious files were not detected when FortiSandbox Community Cloud was disabled.
1247162	Fixed invalid utf8 due to truncated string.
1251514	Fixed the Job Archive feature failed to archive files.
1253309	Fixed an issue where an EXE file renamed as a ZIP was not correctly identified.

System & Security

Bug ID	Description
1196029	Resolved an issue where FSA-1000F units lost embedded Windows/Office licenses after upgrading to version 5.0.4.
1228856	Hardened TLS configuration by removing insecure cipher suites from management interfaces to address vulnerability scan findings.
1258885	Enhanced cluster communication port tolerance to avoid failover caused by short network jitter.

Logging & Reporting

Bug ID	Description
1171394	Fixed an issue with corrupted archive file logging and customized ratings.
1260137	Fixed an SNMPv3 polling failure on FortiSandbox 500F.

CLI and API

Bug ID	Description
1196097	Fixed an issue where script-type executable files did not require the correct file extension; this option is now enabled by default.
1226626	Fixed the show command displaying member ports even after they were assigned to a bonded interface.
1230769	Fixed an issue where read-only LDAP accounts created through the CLI were unable to authenticate.

Common vulnerabilities and exposures

Bug ID	Description
1245752	FortiSandbox 5.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2026-25089

Known Issues

No new issues have been identified in version 5.2.0.

www.fortinet.com