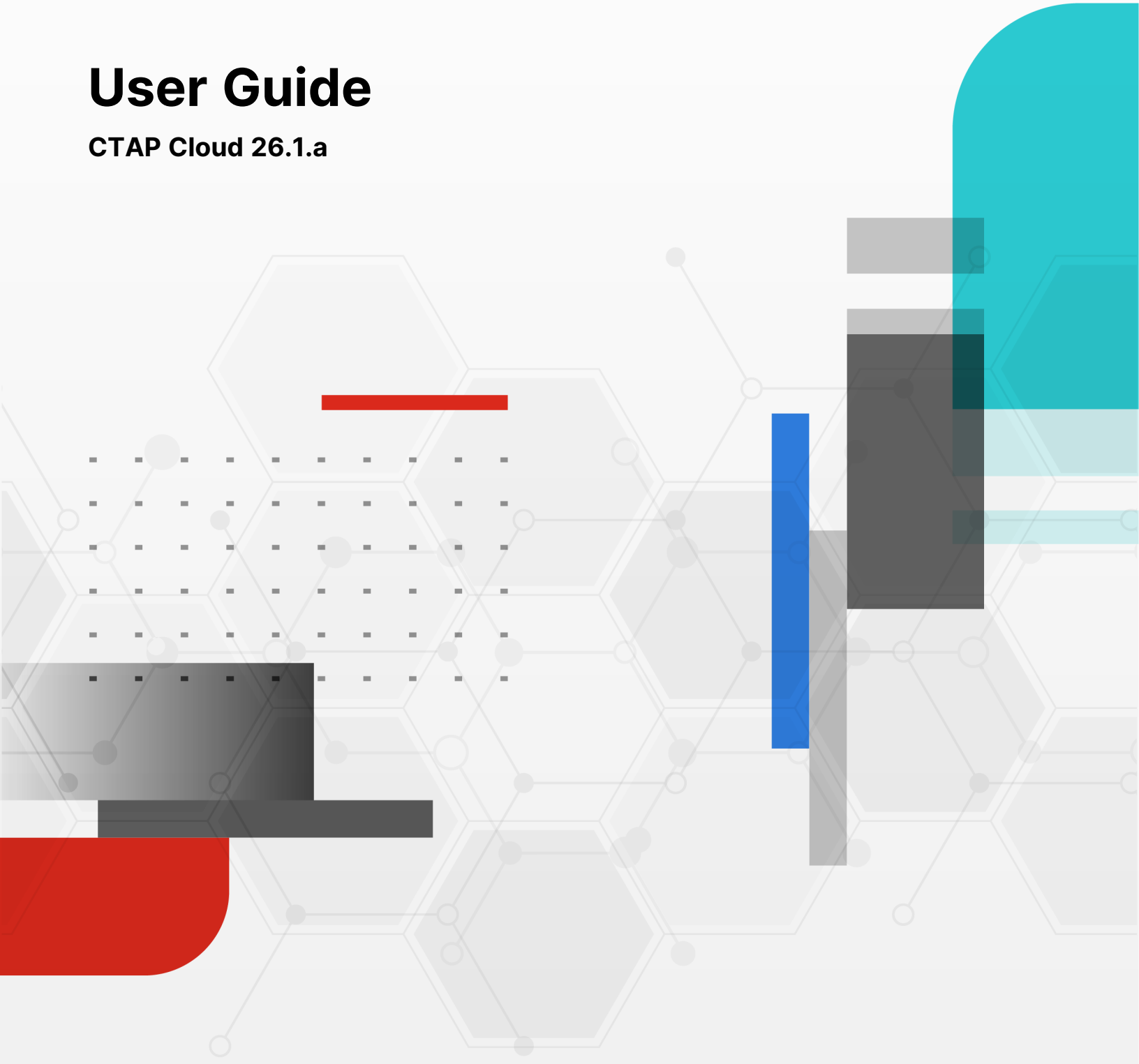
User Guide

CTAP Cloud 26.1.a



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

January 20, 2026
CTAP Cloud 26.1.a User Guide
95-261-1245009-20260120

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-01-20	Initial release.

Introduction to the CTAP Cloud portal

This document acts as an initial introduction to the new CTAP Cloud portal. Over time the new CTAP Cloud portal will replace elements of the existing https://ctap.fortinet.com portal.

The Cyber Threat Assessment Program (CTAP) is designed to help you give customers an in-depth view of the current state of their network. After deploying a Fortinet Inc. product to monitor your prospect's network for a short period of time, you can generate a report and review any findings with key decision makers.

The CTAP Cloud portal enables assessment provisioning from within the FortiCloud Services platform. After requesting CTAP Cloud service from the FortiCloud Marketplace, you can create assessments, collect logs, and generate reports to assess the current network state.

This section includes the following topics:

Key concepts

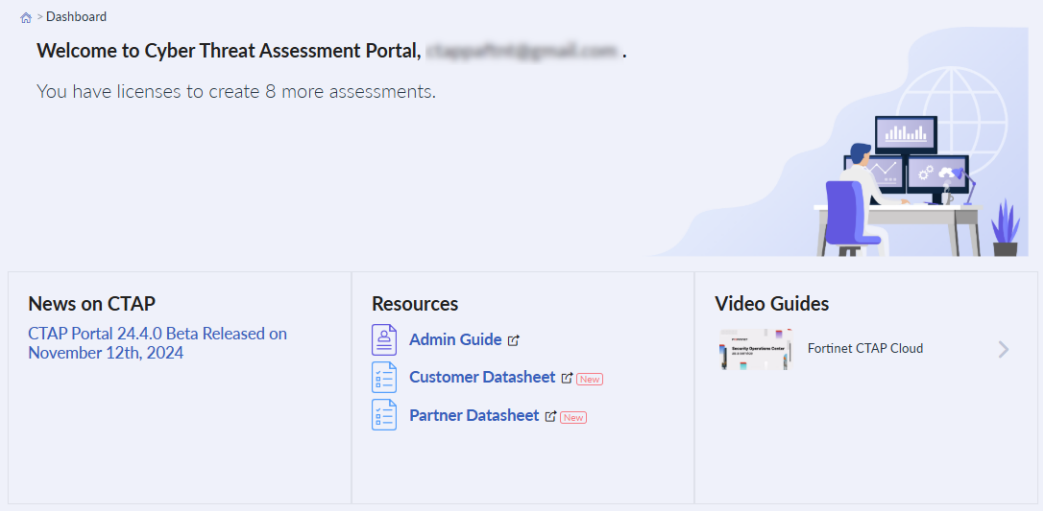
The following table describes key concepts of CTAP:

CTAP Cloud portal	The CTAP Cloud portal is used to provision network assessments and generate reports. See Introduction to the CTAP Cloud portal on page 5.
Assessments and engagements	Assessments are created in the *Assessments* page to monitor network activity. See Assessments on page 9.
Assessment stages	The assessment *Stage* can be defined as : • *Initiated*: The assessment has been provisioned and can begin logging data. • *Logs Received*: Logs have been received for this assessment. • *Report Ready*: The report has finished generating and is ready for review. • *Completed*: The assessment has been completed. • *Canceled*: The assessment was manually canceled before completion. • *Expired*: The assessment license has expired.
Configuration file	The configuration file is generated after the assessment has been created.

	It is dependent on the information selected in the assessment creation page, such as the FortiOS version and configuration details defined. See Working with configuration files on page 16.
Report	A PDF report is generated which presents a set of findings back to the customer based on logs received. Various categories of network details are included in the report, such as network utilization, suspicious behavior, threat prevention, and so on. See Generating reports on page 19.
Storage	The storage field indicates how much of the default storage amount has been used while logging data. If more storage is needed, email ctap@fortinet.com. See Viewing ongoing assessments on page 11.
Assessment types	The CTAP Cloud portal supports Next Generation Firewall (NGFW) assessments.

Getting started

You can access the CTAP Cloud portal from your FortiCloud account. After logging into the account and selecting the Partner user, go to the *Services* dropdown menu and select *CTAP*. You will be directed to the CTAP Cloud *Dashboard*.



General process

The general process of creating and provisioning an assessment is as follows:

1. Provision a CTAP Cloud assessment in the FortiCloud Marketplace portal. See CTAP in the FortiCloud Asset Management guide.

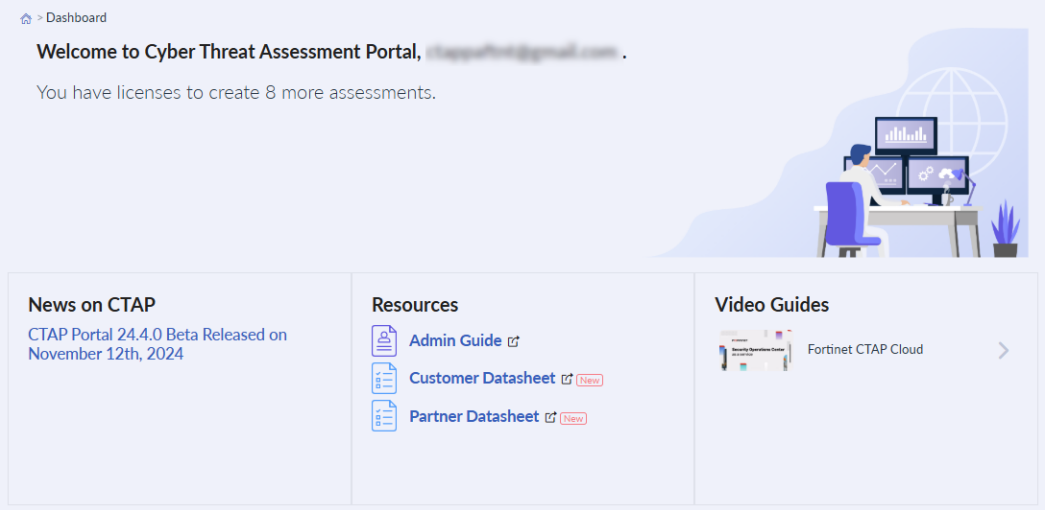
2. Create the assessment in the CTAP Cloud portal:
   a. The assessment is created by defining opportunity and device details. See Creating new assessments on page 13.
   b. The portal generates a configuration file to add to the FortiGate device. See Working with configuration files on page 16.
3. Configure the device with the provided configuration file. See Working with configuration files on page 16.
4. Provision the device and connect it to the customer's environment.
5. Collect logs from the device over a series of days.
6. Generate the report. See Generating reports on page 19.
7. Review the report with the customer.

Licensing

Licensing for CTAP services can be provisioned from the FortiCloud Asset Management portal. An onboarding license is provided for lab use. Once all of the onboarding assessment licenses have been used, new licenses can be provisioned from the FortiMarketplace. Multiple licenses can be purchased in the FortiMarketplace at one time to be used over the span of a year. See CTAP in the FortiCloud Asset Management guide for information on configuring.

Dashboard

The CTAP Cloud portal *Dashboard* displays high level information on the status of your assessment licenses, news, and resources.



Assessments

Assessments can be created and managed in the CTAP Cloud *Assessments* page. Once an assessment has been created and logs collected from the network, the assessment can then create a report to detail the current state of the network.

This section includes the following:

Understanding deployment topologies

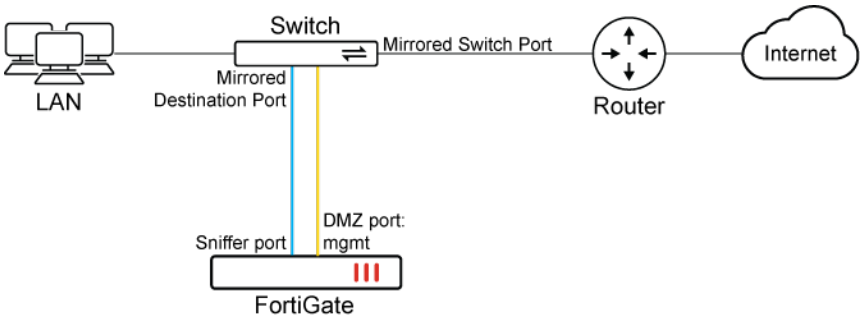
When deploying a FortiGate-based assessment, there are two primary deployment topologies you can use: One-Arm Sniffer and Transparent Mode.

Configuration files generated by the CTAP Cloud portal support both One-Arm Sniffer and Transparent Mode at the same time. The interfaces used by each mode are pre-defined in the configuration file. Smaller models will typically only include a single 1 GE port, but devices with 10 GE capabilities will also be configured with a 10 GE interface. Similarly, transparent mode ports (LAN and WAN destined) are pre-defined and map to their respective 1 GE interfaces (or 10 GE interfaces in higher end models).

One-Arm Sniffer

One-Arm Sniffer mode is the least invasive deployment method that can be used during an assessment and is the most common way to deploy FortiGate-based assessments. This deployment configuration is also sometimes referred to as promiscuous mode or mirrored mode.

FortiGates deployed in sniffer mode are simply analyzing a copy of inbound and outbound network traffic sent from an upstream switch. A copy of the network traffic is sent from a mirrored port on the switch. In other words, the switch facilitates both LAN destined and WAN destined traffic, and a third mirrored port is configured to siphon traffic to the deployed FortiGate for additional inspection.

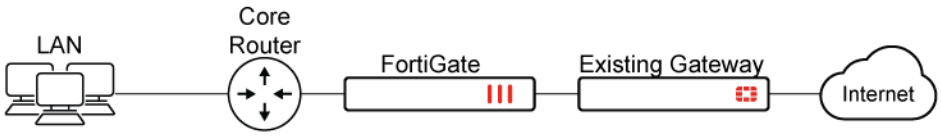


Advantages	Disadvantages
• Passively scans traffic out-of-band (not inline) • Unobtrusive to install; no network downtime required while cabling • Does not present a new potential point of failure for the network backbone	• Requires a more expensive managed switch with port mirroring capabilities • Configuration varies between switch vendors • Sniffer traffic is processed by the CPU; be extra aware of bandwidth requirements

The CTAP team recommends using One-Arm Sniffer mode when possible as it is the least intrusive option for running assessments.

Transparent Mode

When deployed in Transparent Mode, the FortiGate sits directly on the network backbone and inspects traffic as it flows through the system (LAN <> WAN). Since it can affect the flow of network traffic, it is less commonly used during assessments. Transparent mode is also sometimes called an inline, virtual wire, or port pair configuration.

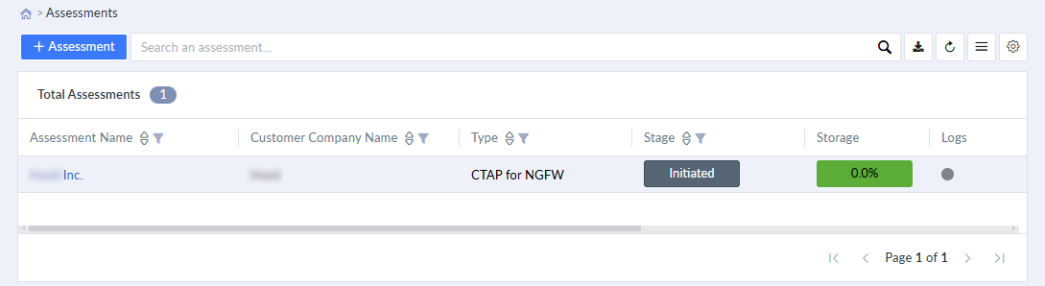


Advantages	Disadvantages
• Easy to install by connecting connect between the core router and firewall • Illustrates performance capabilities of FortiGate within customer's actual network	• Undersized systems can result in dropped packets, negatively impacting network • Requires some (minimal) network downtime during installation and cabling • Introduces new potential points of failure within network backbone: the system and the new cable

The CTAP team only recommends using transparent mode when the end customer explicitly requests it. It applies primarily in cases where the a demonstration of the FortiGate's performance relative to the model used is requested or there is no managed switch available.

Viewing ongoing assessments

Assessments are listed in the *Assessments* page.



The assessment list can be managed by selecting the icons available or by entering assessment information in the search bar.

+ Assessment	New assessments can be created by selecting *+ Assessment*. See Creating new assessments on page 13.
Download	Download a list of the existing assessments as an Excel (.xlsx) file.
Refresh	Refresh the list of assessments to review *Stage*, *Storage*, and *Log* updates, if needed.
Columns	Select the assessment detail columns visible in the table. Click *Apply* to display changes.
Custom View	After setting up the *Assessments* table and applying column visibility changes, save the view in the *Custom View* option.

Assessment statuses

This section primarily applies to assessments using remote logging.

The *Logs* status and *Storage* indicators in the CTAP Cloud *Dashboard* can provide visibility into the connectivity status of a CTAP device. Using these indicators, you can quickly confirm that traffic is being received by the device, and that the device is able to connect back to the hosted FortiAnalyzer for log storage and report generation.

Logs

The *Logs* status indicator displays if the hosted FortiAnalyzer is actively receiving logs from the CTAP device. Hovering over the status indicator will display a time stamp for when the last log was received.

Status color	Definition
Green	A green status indicator mean that the CTAP Cloud portal is actively receiving logs from the CTAP device.
Yellow	A yellow status indicator means that a potential issue has been detected and may require further action. Click on the status indicator to view more information about the reported status and potential causes or solutions.
Red	A red status indicator means that the CTAP Cloud portal is not currently receiving logs from the CTAP device. This may mean that the portal has never received logs, or that the portal has not received any logs within the last 15 minutes.
Gray	A gray status indicator means that the log status is unavailable. This is shown for assessments that have been completed or when an assessment is newly created and has not yet retrieved status from the hosted FortiAnalyzer.

Storage

The *Storage* indicator shows how much disk space is currently being used on the hosted FortiAnalyzer represented as a percentage. By referencing the storage indicator, you can make an estimation as to how long you can run an assessment without overwriting existing logs. Hovering over the storage indicator will show you the exact amount of storage that is currently being used versus the storage that is available.

Status color	Definition
Green	When the storage indicator is green, storage utilization is within the expected limit.
Yellow	When the storage indicator is yellow, the assessment has reached 80% of its available storage. The system will soon begin purging old data to free up space for new logs.
Red	When the storage indicator is red, the assessment has reached its maximum log capacity and will now begin to purge old logs to free up space for new logs coming in. Logs will be purged in a FIFO fashion (first in/first out). Once logs have been removed from the system, they cannot be recovered.

Log storage can be increased to accommodate larger customers. To increase the available log storage for an assessment, contact the CTAP team at ctap@fortinet.com.

Creating new assessments

New assessments can be created in the CTAP Cloud portal.

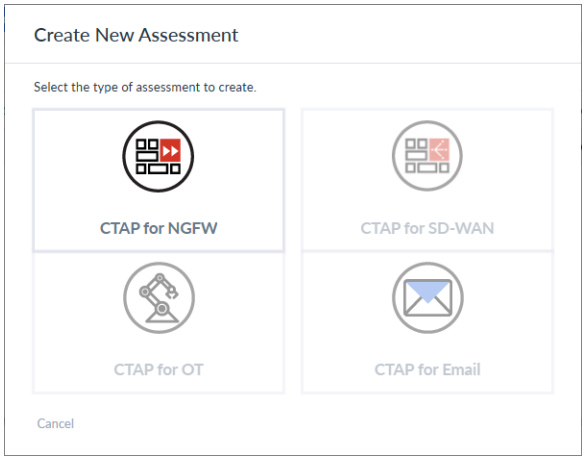
An assessment license must be available in the account to create a new assessment. If there is no available license, new licenses can be purchased in the FortiMarketplace. See CTAP in the FortiCloud Asset Management guide for information on requesting licenses.

Fields marked with an asterisk (*) are mandatory information. The assessment request will not process without these fields.

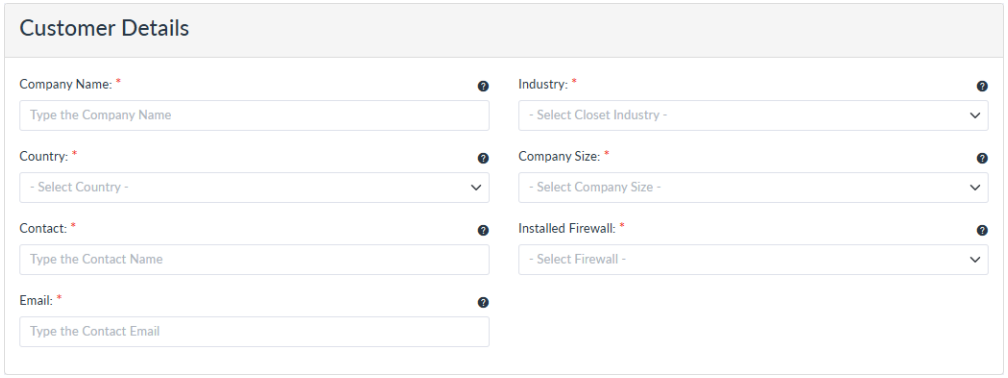
Hover over a *?* for more information on a field's required information.

To create a new assessment:

1. Go to *Assessments*.
2. Click *+ Assessment*.
3. Select *CTAP or NGFW*.

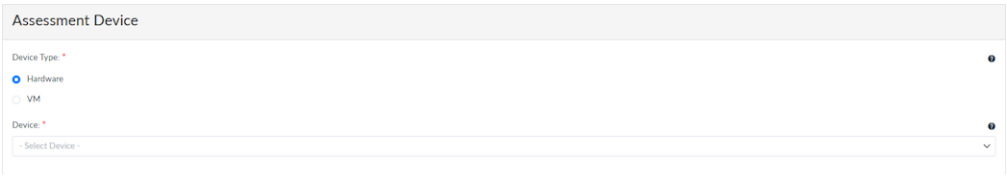


4. Configure the assessment details:
   a. Enter the *Customer Details*.



b. Select the FortiGate *Device Type* and enter the device details in the *Assessment Device* fields:

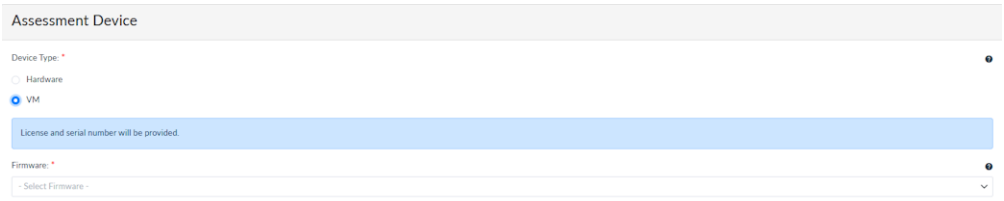
i. If you select *Hardware*, select the *Device* serial number from the dropdown list.



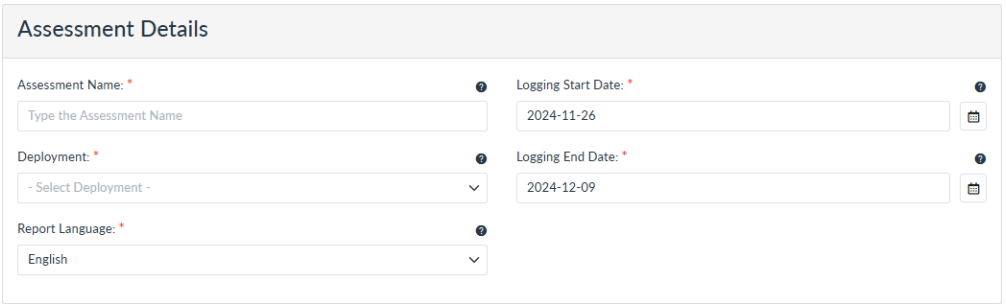
ii. If you select *VM*, select the *Firmware* version from the dropdown list.

There may be instances where running hardware-based assessments with CTAP Cloud does not make sense. Perhaps physical access to the data center is not possible, or there are logistical issues moving hardware to where it needs to be. In these cases, using a FortiGate VM may be the best option for all parties concerned.

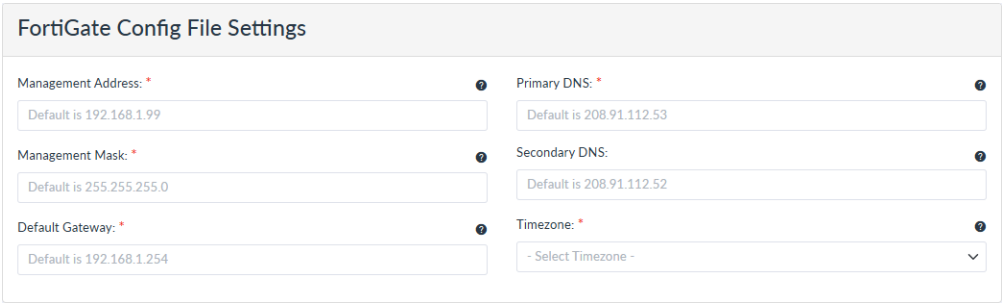
You can run a FortiGate-based assessment using a virtual machine. Currently, only ESXi VMs are available in the CTAP Cloud portal.



c. Enter the *Assessment Details*.



d. Enter the FortiGate configuration details in the *FortiGate Config File Settings* fields.



e. Enter the account information in the *Opportunity* fields, if available.

5. Enter any *Notes* about the assessment.
6. Click *Submit*. The assessment has been created.

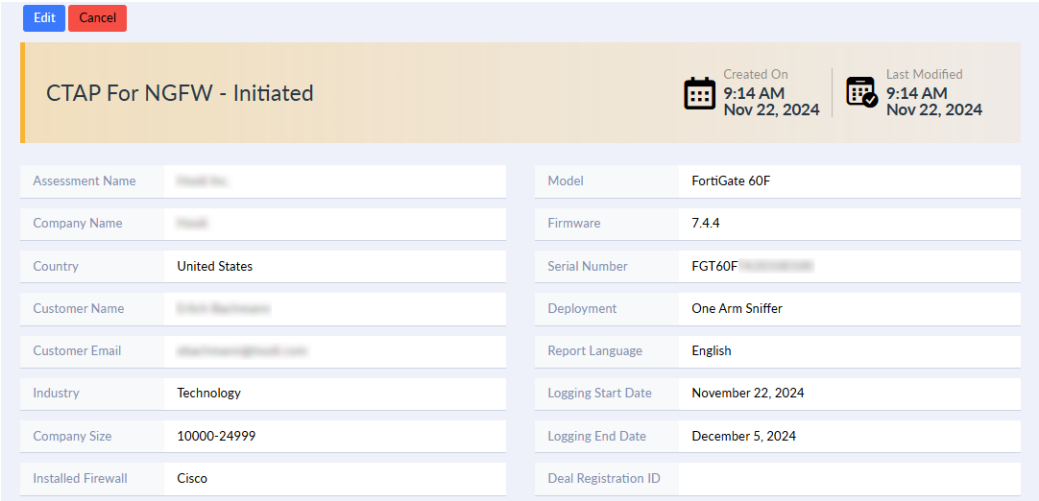
Once the assessment has been created, you can configure the hardware device or VM. See Configuring the device on page 16.

Editing existing assessments

Existing assessments can be edited to update the information as needed.

To edit an assessment:

1. Go to *Assessments*.
2. For the assessment you want to edit, click the *Assessment Name*.



3. Click *Edit*.
4. Edit the assessment details, as needed.
5. Click *Update*.

Working with configuration files

The configuration file is generated after the assessment has been successfully created. It is dependent on the information selected in the assessment creation page, such as the FortiOS version and configuration details defined.

The configuration file is used to configure the FortiGate being used for network monitoring. For example, the `config system interface` section of the configuration determines the port mapping of the FortiGate, and the root and CTAP VDOM configuration.

To implement the configuration file on the FortiGate:

1. Go to *Assessments*.
2. For the assessment you want to configure a device for, click the *Assessment Name*.
3. In the *FortiGate Configuration* section, click *Download* to save the files needed to configure the FortiGate.
4. Upload the configuration file to the FortiGate. See Configuring the FortiGate hardware device on page 16.

The hardware device configuration file can be restored in the FortiOS GUI or in the CLI using `execute restore config`. See Configuration backups and reset in the FortiOS Administration Guide for more information.

Once the FortiGate is configured, the assessment stage is displayed as *Initiated* in the *Assessments* page and the *Logs* indicator will appear as green when logging has begun.

Configuring the device

Once the configuration file is available, the FortiGate hardware or VM can be configured and connected to the network.

- Configuring the FortiGate hardware device on page 16
- Configuring a FortiGate virtual machine (VM) on page 19

Configuring the FortiGate hardware device

Once the configuration file is available, the FortiGate can be configured and connected to the network.

To prepare and configure the FortiGate:

1. Power the unit on and connect to the web GUI:
   - Using an Ethernet cable, connect your PC to the management port on the FortiGate. Open a web browser and navigate to: https://192.168.1.99 or the provided IP address of the loaner device.

- Advanced users can opt to use a Serial-to-Ethernet cable to perform this initial configuration from the CLI. Refer to the FortiGate product documentation for CLI commands and instructions.

2. Log in to the system as an administrator. The default credentials are *admin* / *fortinet*.
3. Confirm the system firmware version matches the firmware selected in the assessment.
4. Verify that the required FortiGuard licenses are active:
   a. Go to *System* > *FortiGuard*.
   b. Confirm that *Intrusion Prevention*, *AntiVirus*, and *Web Filtering* licenses are active.
5. Import the CTAP configuration file:
   a. Using the admin drop-down menu, navigate to *Configuration* > *Restore*.
   b. Upload the configuration file downloaded from the CTAP Cloud portal.
   c. Click *OK*. The system will reboot.
   d. Move the Ethernet cable to the management port if it is not already the factory management port.
   e. Following the reboot, re-login to the FortiGate.
6. Change the default password to something more secure:
   a. In the admin drop-down menu, click *Change Password*.
   b. With all of the settings in place, connect the management port to the local network and confirm that you can access the web GUI using the supplied IP address and password.

Connecting to the network

The device can be connected to the network in sniffer or transparent mode.

See Understanding deployment topologies on page 9.

Refer to the model matrix to identify the specific ports you will be cabling.

To connect the system in Sniffer Mode:

1. Identify an open port on the core switch (where all traffic aggregates just before reaching the gateway).
2. Connect the first sniffer port (1GE) or second sniffer port (10GE) to the open port on the switch.
3. Create a port mirroring rule on the switch to send internal traffic to the FortiGate.

The port mirroring configuration on the switch varies between switch vendors. You will need to refer to the switch vendor's administrative guide for steps to enable mirroring.

4. Review traffic logs on the FortiGate to confirm installation.

To connect the system in Transparent Mode:

1. Identify the cable connecting the core router or switch to the network gateway. This is where you will be inserting the CTAP FortiGate.
2. Get a new Ethernet cable and have it ready for a quick installation.
3. Install the system:
   a. Connect the first WAN port (1GE) or the second WAN port (10GE) to the ingress (LAN) interface on the network gateway.

   b. Connect the first LAN port (1GE) or the second LAN port (10GE) to the egress (WAN) interface on the core router or switch.
4. Confirm that connectivity to the Internet has been reestablished and is working.
5. Review traffic logs on the FortiGate to confirm installation.

Confirming installation

Traffic logs should be reviewed on the FortiGate to confirm that the system is receiving traffic. You should also confirm that the FortiGate can connect to the hosted FortiAnalyzer.

Review traffic logs

When correctly installed, the FortiGate will begin processing network traffic and recording traffic logs. You can review traffic logs directly on the FortiGate to confirm that it is receiving traffic.

To review traffic logs:

1. Log in to the FortiGate's web GUI.
2. View the traffic logs:
   - If you are in sniffer mode, go to *Log & Report > Sniffer Logs*.
   - If you are in transparent mode, go to *Log & Report > Forward Logs*.
3. In the upper-right corner of the page, adjust the *Log Location* dropdown to read from the local system.
4. Confirm that you can see user traffic in the logs (such as HTTPS and internal IP addresses).

Common misconfigurations to look for include logs that only show broadcast / multicast traffic, or traffic that shows public IP addresses on both sides of the connection. If this is the case, you may need to review your installation.

Verify connectivity to FortiAnalyzer

Confirm that the FortiGate can connect to the hosted FortiAnalyzer that was automatically provisioned by the CTAP portal.

To verify connectivity to FortiAnalyzer:

1. Log in to the FortiGate's web GUI.
2. Go to *Security Fabric > Fabric Connectors*.
3. Click the *Logging & Analytics* card and select *Edit*.
4. Click the *Refresh* button. The test result will indicate the current status:
   - *Connected*:The connection was successful.
   - *No connection* : The connection failed. Confirm that TCP/514 is allowed outbound.
   - *Unauthorized*: The connection was successful, but the FortiAnalyzer has not authorized this FortiGate to send logs. This may occur if the FortiGate is deployed before the assessment is created, if there is a serial mismatch, or if the FortiGate is configured to connect to the wrong FortiAnalyzer IP address.

Configuring a FortiGate virtual machine (VM)

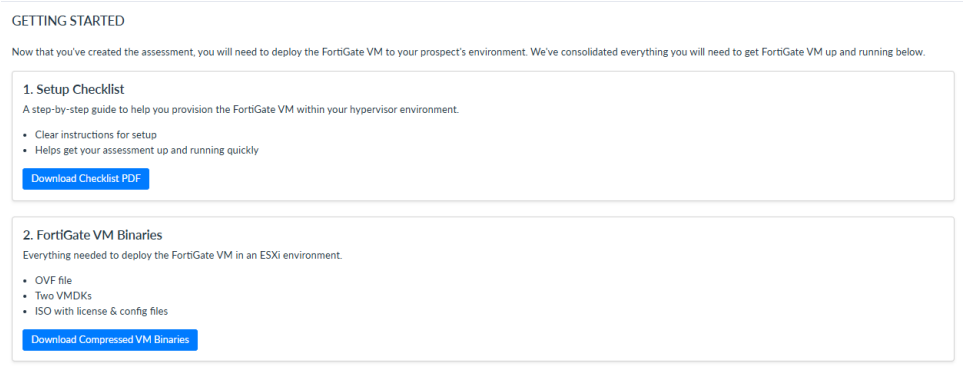
After creating an FortiGate VM assessment, the *Setup Checklist* and *FortiGate VM Binaries* files will become available:

- The *Setup Checklist* outlines the procedure needed to prepare and set up your FortiGate VM.
- The *FortiGate VM Binaries* compressed file includes the OVF file, two VMDKs, and the ISO with the license and configuration files. These files are necessary to preparing and running the VM ahead of the assessment.

Currently, only ESXi-based FortiGate VMs are supported by CTAP Cloud. After creating the FortiGate VM in the ESXi environment, upload and install the OVF file. Once the OVF file is deployed, the binaries, license, and configuration files should be installed automatically.

To access the files needed to configure the VM:

1. Go to *Assessments*.
2. Select the VM assessment you created.
3. In the *Getting Started* section, select *Download Checklist PDF* and *Download Compressed VM Binaries*.



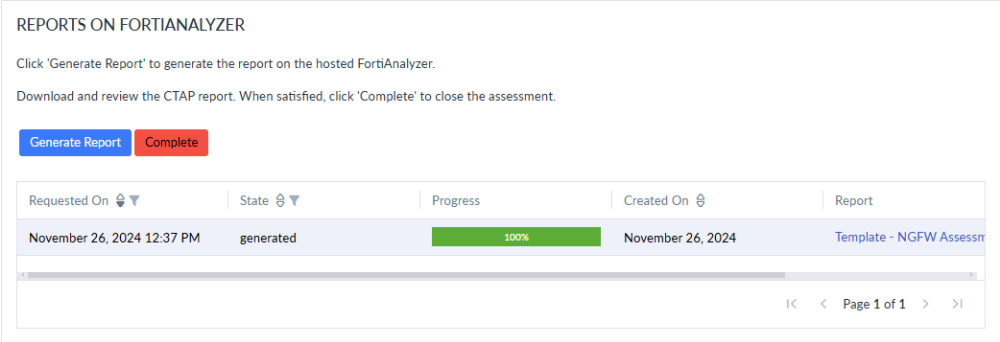
4. Follow the instructions in the *Setup Checklist* to prepare your VM.

Generating reports

When you are finished collecting log data from the customer's network, a report can be generated to outline the current status of the network, such as network utilization, suspicious behavior, threat prevention, and so on.

To generate a report:

1. Go to *Assessments*.
2. For the assessment you want to generate a report for, click the *Assessment Name*.
3. In the *Reports on FortiAnalyzer* section, click *Generate Report*. The report will be generated.

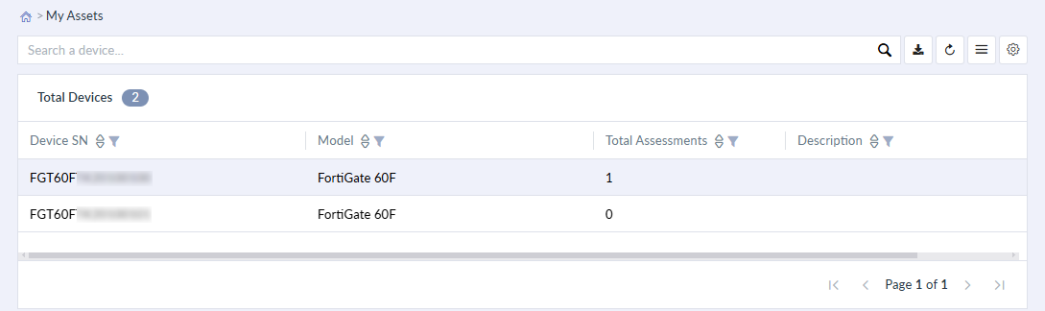


The assessment *Stage* will display *Report Ready* when the report generation has completed.

4. Download the report.
5. Click *Complete* when the assessment is done.

My Assets

The *My Assets* page lists devices currently registered to your account and the number of assessments conducted by the device.



Download	Download a list of the existing devices as an Excel (.xlsx) file.
Refresh	Refresh the list of devices, if needed.
Columns	Select the device detail columns visible in the table. Click *Apply* to display changes.
Custom View	After setting up the *My Assets* table and applying column visibility changes, save the view in the *Custom View* option.

Appendix A - Model and firmware support

The following table lists the supported models and versions, along with their associated ports:

			10/100 Interfaces				10GbE Interfaces		
	Models	Firmware	Management	WAN	LAN	Sniffer	WAN	LAN	Sniffer
G Series	90G / 91G	7.4.5 / 7.4.7 / 7.6.4	WAN1	Port1	Port2	Port4	-	-	-
F Series	40F	7.4.5 / 7.4.7 / 7.6.4	WAN	Port1	Port2	Port3	-	-	-
	60F / 61F	7.4.5 / 7.4.7 / 7.6.4	DMZ	Port1	Port2	Port4	-	-	-
	70F / 71F	7.4.5 / 7.4.7 / 7.6.4	DMZ	Port1	Port2	Port4	-	-	-
	80F / 81F	7.4.5 / 7.4.7 / 7.6.4	WAN1	Port1	Port2	Port4	-	-	-
	100F / 101F	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port1	Port2	Port4	-	-	-
	200F / 201F	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port1	Port2	Port4	X1	X2	X4
	400F / 401F	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port1	Port2	Port4	X1	X2	X4
	600F / 601F	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port1	Port2	Port4	X1	X2	X4
	1800F / 1801F	7.4.5 / 7.4.7 / 7.6.4	MGMT1	Port1	Port2	Port4	Port25	Port26	Port28
E Series	60E / 61E	7.4.5 / 7.4.7	DMZ	Port1	Port2	Port4	-	-	-
	300E / 301E	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port1	Port2	Port4	-	-	-
	400E / 401E	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port1	Port2	Port4	-	-	-
	600E / 601E	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port1	Port2	Port4	-	-	-
	1100E / 1101E	7.4.5 / 7.4.7 / 7.6.4	MGMT	Port13	Port14	Port16	Port25	Port26	Port28

www.fortinet.com