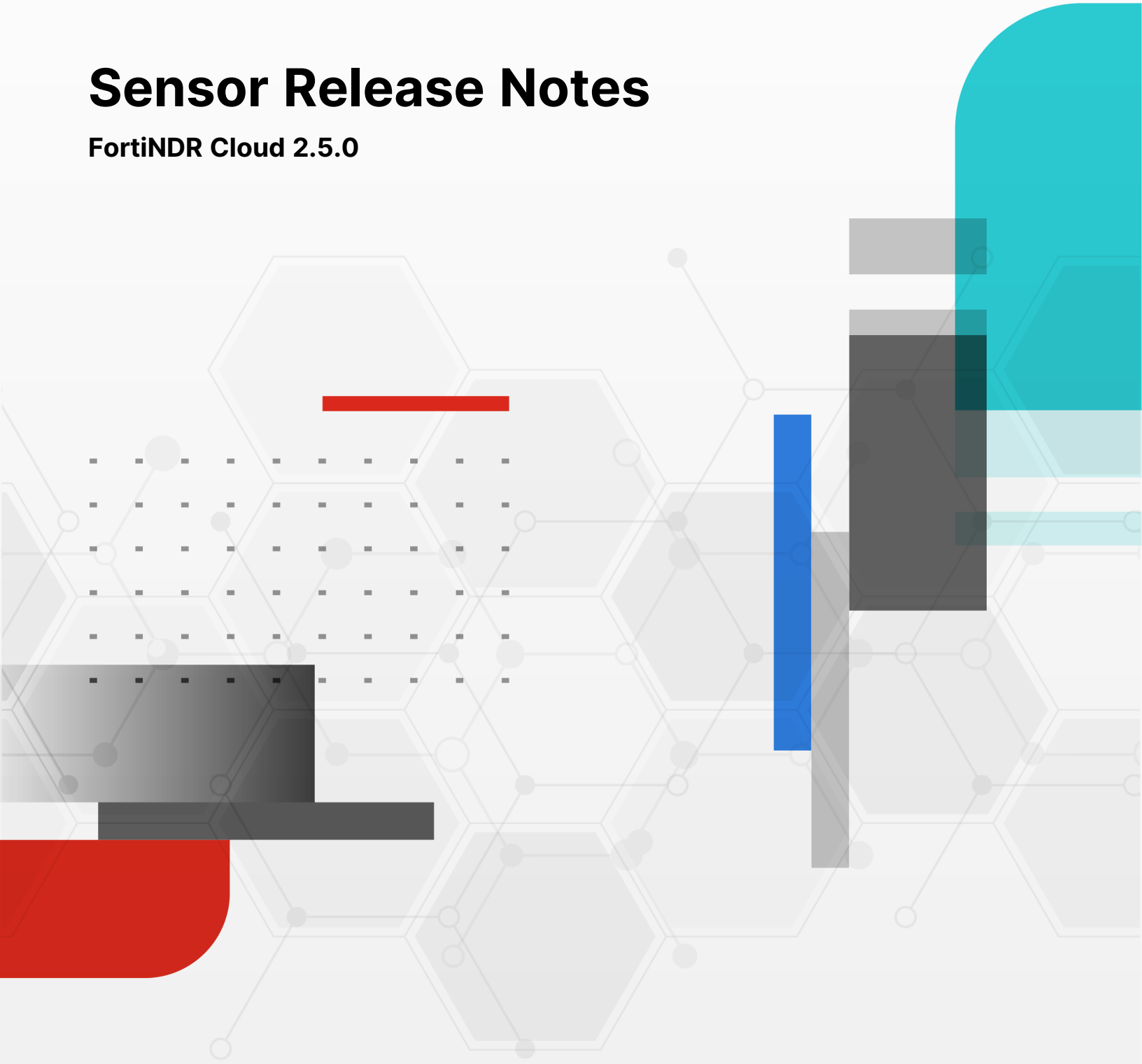
Sensor Release Notes

FortiNDR Cloud 2.5.0



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

April 1, 2026
FortiNDR Cloud 2.5.0 Sensor Release Notes
78-250-1199847-20251224

TABLE OF CONTENTS

FortiNDR Cloud sensor release notes

This document provides information about FortiNDR Cloud (formerly known as ThreatINSIGHT) sensor releases.

FortiNDR Cloud is a SaaS network security monitoring platform designed to facilitate rapid detection, investigations, and threat hunting within your environment. FortiNDR Cloud is designed to be scalable and to remove the responsibilities of maintaining tooling from security analysts. For more information, see the FortiNDR Cloud User Guide.

Version history

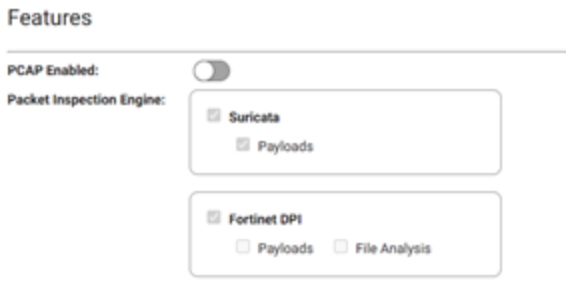
Date	Version	Identifier
27 March 2026	2.5.0	Build 0213
29 December 2025	2.4.0	Build 0111
05 September 2025	2.3.0	Build 0013
21 May 2025	2.2.0	1c661fe1ffb02c9c-2.2.0
31 January 2025	2.1.0	1d2cc12353cc5f86-2.1.0
29 July 2024	2.0.0	334f59baf1da1902-2.0.0
04 March 2024	1.12.0	6cffc926ae6ab7eb-1.12.0
01 November 2023	1.11.0	0df18d46a4609673-1.11.0
17 July 2023	1.10.0	718f6712d637065c-1.10.0
30 May 2023	1.9.0	de170f2d5a4409d7-1.9.0
16 March 2023	1.8.1	aa6ded41b2746ae7-1.8.1
16 December 2022	1.8.0	48cbd83715e73129-1.8.0

New Features and improvements

This section details what's new in each maintenance release.

2.5.0

- **APAC region support**: Sensors can now be deployed in the APAC region.
- **File Analysis**: Sensors now have the ability to extract and scan files for malware.
- **DPI payload support**: Sensors now have the ability to enable packet payload in the DPI logs.
- **Enabling features through the Portal**: You can now enable sensor features from the FortiNDR Cloud portal.



- **DPI Engine Upgrade**: Upgraded DPI engine to version 7.6.1179
- **Suricata memory cap**: Increased the memory cap for Suricata for better performance.
- **Security updates**: Several security vulnerabilities have been addressed.
- **Network drivers**: Network interface drivers on several sensors were upgraded.
- **Zeek logging**: Enabled SSL extension log and improved VLAN tagging.
- **Link scan**: Added *linkscan* feature to monitor management port's link status regularly, this is to ensure sensor operation after a power outage

2.4.0

- **ERSPAN Support**: Sensors can now ingest traffic via ERSPAN for remote monitoring.
- **Device Enrichment**: Added device enrichment using LDAP and DNS servers to enhance asset context and visibility
- **DPI Engine Upgrade**: Upgraded DPI engine to version 7.6.1136
- **NetFlow Enhancements**: Improved NetFlow performance, configuration workflow, and scalability for all sensors, including support for running NetFlow with a single dedicated collector interface to optimize performance

- **Sensor Upgrade Support**: Added support for upgrading sensors deployed in AWS and Oracle Cloud Infrastructure (OCI)
- **Resiliency Improvements**: Sensors now support automatic reboot on kernel panic
- **Platform Enhancements**: Improved KVM/Proxmox DHCP support
- **Security Updates**: Updated multiple packages to address known vulnerabilities

2.3.0

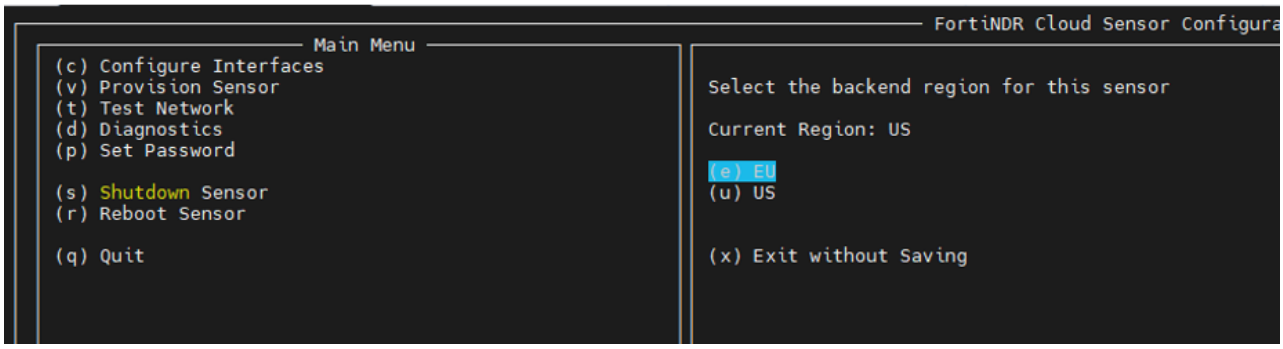
- **Netflow Suppor**t: Sensors can now be configured to receive NetFlow traffic, enabling improved network visibility and detection.
- **OCI Cloud Support**: Sensor is now available on Oracle Cloud Infrastructure (OCI).
- **Azure Platform Support**: Sensor is now available on Microsoft Azure.
- **Suricata Upgrade**: Upgraded to Suricata v7.0.11
- Expanded Protocol and Logging Support for Zeek and Suricata

2.2.0

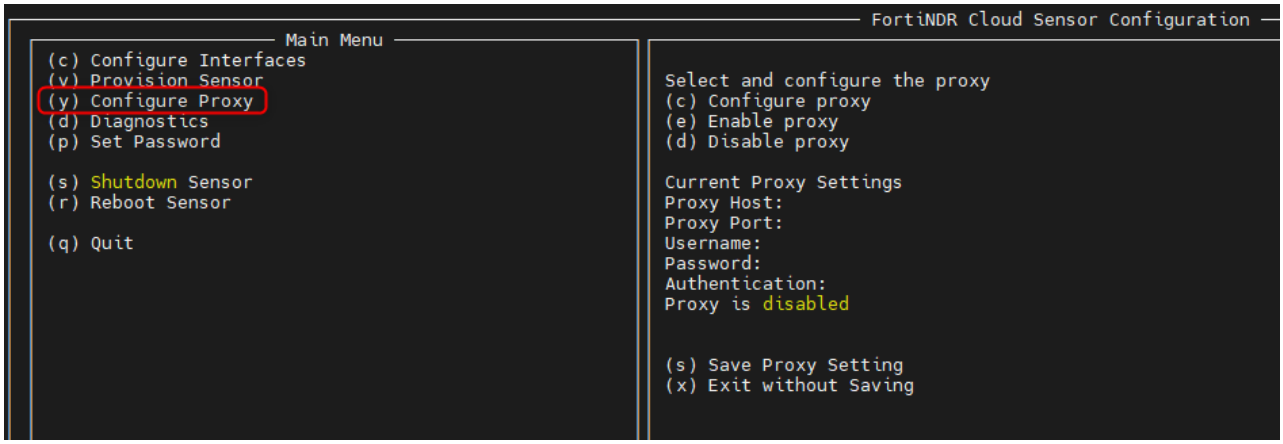
- Zeek upgraded to version 7.0.5.1
- Suricata upgraded to version 7.0.10
- GCP sensor is now available in the Google Cloud Marketplace
- PF_RING upgraded to version 8.8
- Sensor can now be provisioned without the requirement for the monitoring port/s to have a link.
- Sensor can be reset to factory defaults using the serial console
- New physical platforms 500G and 900G introduced

2.1.0

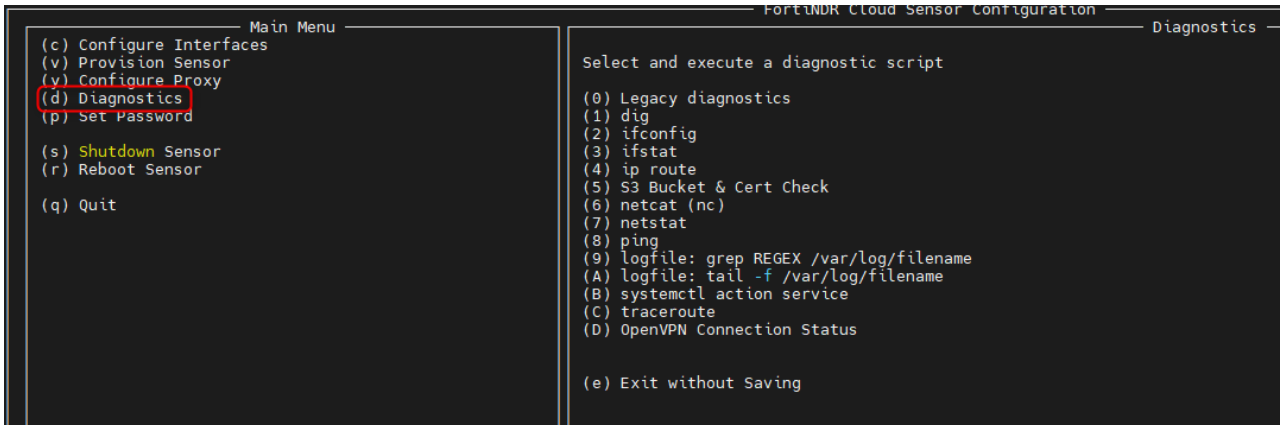
- Support for sensor provisioning in the EU region.



- Suricata upgraded to version 7.0.7.
- Proxy support.



- Improved diagnostics for more advanced troubleshooting.



- New 2540 physical sensor with support for 40 Gbps.
- New Hyper-V sensor.
- Updated AWS sensor.

- KVM sensor officially supported
- Various security improvements.

2.0.0

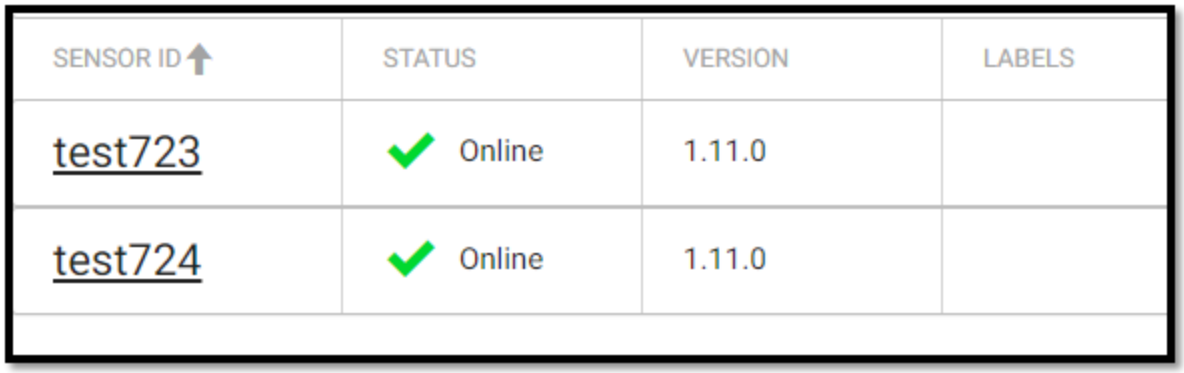
- Upgraded Sensor Operating System.
- Support for sensor Pause/Resume.
- Upgraded Zeek version.
- Upgraded OpenSSL.
- Upgraded OpenSSH.
- Upgraded JA3 plugin in Zeek.
- Enabled SSL/TLS certificate validation in Zeek.
- Various security improvements.

1.12.0

- Support for sensor decommissioning.
- Upgraded Zeek and Suricata version for additional functionality and performance.
- Enabled new protocols such as DNP3 and MODBUS for meta extraction.
- Upgraded OpenSSH version.

1.11.0

- Suricata was updated to version 6.0.12 release.
- Sensor version is now reported on the Portal.



1.10.0

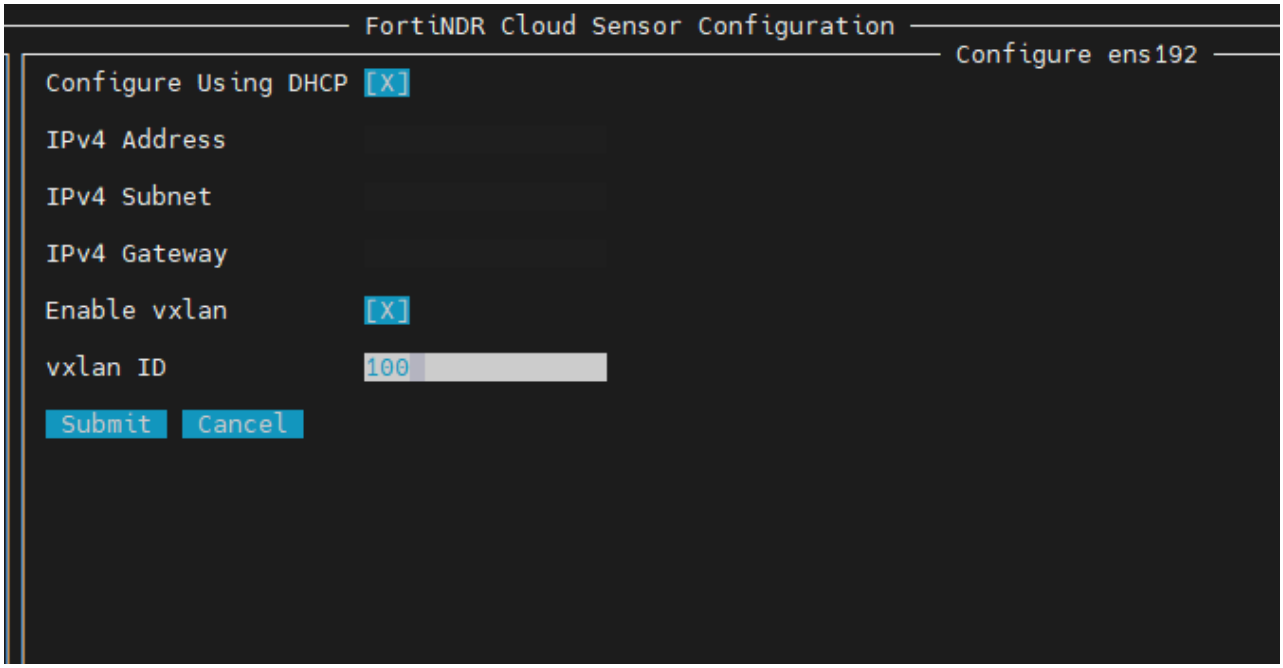
- User is now asked to change the console password immediately after the first login.

```
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for config.
Current password:
New password:
Retype new password:
```

- VXLAN support: This feature allows the user to forward traffic to the FortiNDR sensors' interface using a vxlan tunnel. Currently VXLAN is supported on the sensor's management port.

To configure VXLAN:

1. In the configuration UI, press *c* or select *Configure Interfaces*.
2. Select the current management port.
3. Enable VXLAN.
4. Type VXLAN ID of choice and select *submit*.
5. Save the configuration
6. Reboot the sensor by pressing *r* or selecting *Reboot*..



Important:

After enabling the VXLAN feature, sensor will only process packets on the VXLAN interface (attached to the management port). Packets received on any other interfaces on the sensor will not be processed.

- **AWS sensor**: As of version 1.10 the new Zeek based AWS sensor ami is available on the AWS marketplace.
- **Configure UI**: In this version you are asked to change the password to access the configuration UI from the default (configure) password when you access the configuration UI for the first time

1.9.0

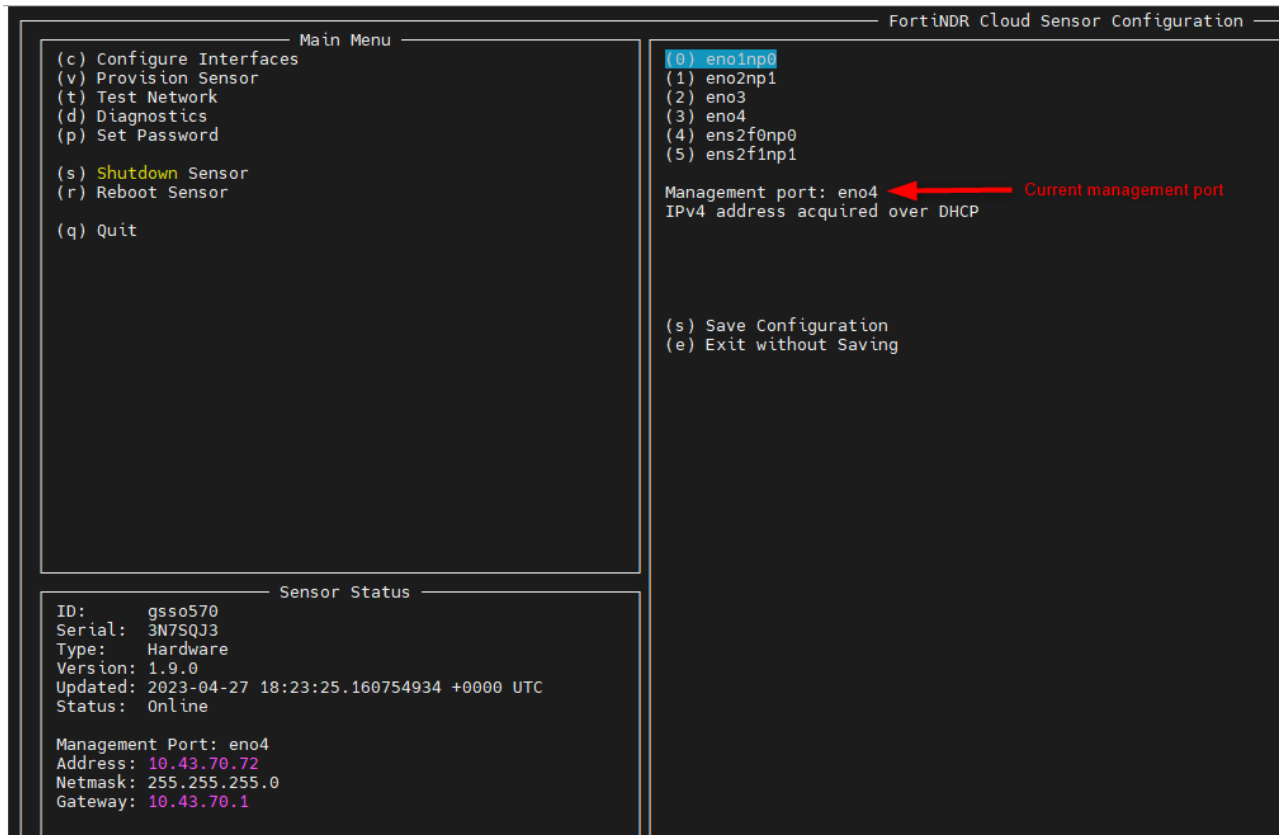
Interface selection utility

The new interface selection utility in the configuration menu allows you to select a port of choice as management port if you do not wish to use the management port identified by the sensor automatically.

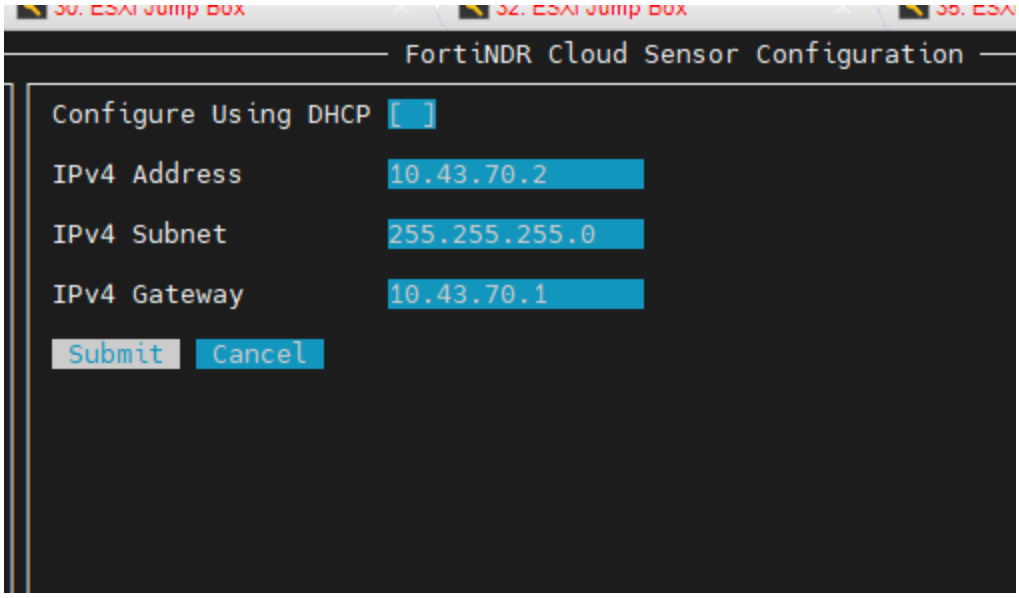
When selecting a different management port than the one detected by the sensor, all other ports will be considered as monitoring ports.

To configure interfaces:

1. In the config UI, press `c` or go to `Configure Interfaces`.
2. Select the interface that you want to designate as management interface (if it is different than the port already identified as management by the sensor).



3. Select `DHCP` or disable DHCP by pressing the space bar to enable static IP
4. Click `Submit`.



Supported models

The following table lists the sensors that are currently supported. Sensor installation guides are available on the FortiNDR CloudSensors page.

Network Sensor	Description
Physical sensors	Version 2.4.0
Public Cloud sensors	AWS, Azure, GCP, OCI
Private Cloud sensors	ESXi, Hyper-V, KVM, Nutanix (version AOS 7.3.1)

Resolved issues

The following issues have been fixed. To inquire about a particular bug, please contact Customer Service & Support.

2.5.0

Missing partition	Addressed an issue where after upgrading a cloud sensor, a non-essential partition was missing.
Sensor pause	Resolved an issue where in some condition, sensor would not go to the pause state
Security	Addressed multiple vulnerabilities to improve system security.

2.4.0

Upgrade Stability	Fixed upgrade-related issues affecting DPI rules, Suricata configuration, ensuring proper retention and reload behavior.
Service Reliability	Ensured engine services shut down cleanly when sensord exits and resolved connectivity loss after Zeek service restarts.
NetFlow Stability & Performance	Resolved NetFlow configuration inconsistencies, missing logs in shared subnets, low-disk handling, and improved performance on all sensors.
Provisioning	Fixed provisioning and status reporting issues when monitoring interfaces are not connected.
Diagnostics	Fixed diagnostics failures when a proxy is enabled.
Cloud platforms	Resolved GCP-specific logging and syslogd restart issues.
Security	Addressed multiple vulnerabilities to improve system security.

2.3.0

GCP TAP Interfaces	Fixed an issue where IPs were not flushed from additional TAP interfaces.

Proxy Connectivity	Corrected sensor scans so they now route through the configured proxy.
Decommissioning Swap	Resolved an issue where swap was lost after decommission and reboot.
DHCP Configuration	Fixed an issue where DHCP changes were not applied automatically on some platforms.
Interface Configuration	Changes to network interfaces now take effect automatically without requiring manual reboot.
KVM TAP Interface	Corrected TAP interface MTU to remain at 9000 instead of 1500.
500G/900G Platforms	Fixed excessive *ACPI Error* and *Failed* log messages.
Security	Addressed multiple vulnerabilities to improve system security.

2.2.0

Fixed an issue where sensor upgrades under certain conditions could cause the sensor service to reboot unexpectedly.
Resolved an issue where disabling the proxy would delete the existing proxy configuration.
Addressed multiple Suricata security vulnerabilities.

2.1.0

Addressed an interface packet drop issue on some platforms.
Resolved a problem with Zeek falsely showing excessively increasing drops at boot.
Resolved an issue where after container upgrade, the version was not reflected in the Portal.
Addressed an issue with sensor state transitioning into incorrect state when no TAP interface is present.
Resolved an issue where during reboot after an upgrade, the boot menu would show 2 previous versions instead of one.
A number of Suricata security vulnerabilities were addressed.

2.0.0

Addressed a rare crash condition in the metric exporter.
Resolved an issue with log redirects following the upgrade.
Resolved a partitioning problem that occurred after the Debian upgrade.
Addressed an issue with Suricata fast logs consuming excessive disk space.
Resolved a problem where Suricata logs grew beyond the upload limit under certain conditions.
Resolved an issue where certain DHCP packets caused the DHCP to exceed the allowed size.
Resolved a problem where Zeek logs would not upload under certain conditions.

1.12.0

Resolved an issue where sensor would send NTP requests through the management port.
Resolved an issue related to Suricata rules not being applied at runtime.
Resolved an issue related to DHCP lease not being renewed .
Resolved an issue related to Suricata path not getting updated after upgrade
Resolved an issue related to Suricata log rotation after upgrade.
Resolved an issue related to Suricata version 6.0.13 on external source of rules.
Addressed an intermittent issue where an invalid memory address was observed at sensor daemon initialization.

1.11.0

Resolved issues related to VPN connection errors to the VPN end point .
Resolved an issue related to syslog traffic causing high disk usage
Various fixes related to the PCAP feature
OpenSSH and curl vulnerability patches.
Several bugs addressed in the sensor upgrade area.
Addressed a problem with metadata logs not getting uploaded through the s3 proxy.
Resolved an issue related to the sensor in a specific scenario reporting incorrect status to the portal .

1.10.0

Resolved an issue related to MIME types not correctly being identified
Various optimizations

1.9.0

Updated device drivers.
Kernel optimizations.
Resolved issues with port media type display in the portal.
Resolved the issue related to incorrect disk size being displayed.

1.8.1

An issue in the Suricata EXTERNAL_NET field cause some Suricata rules to not be processed.
A bug in the PCAP feature caused packet capture to produce empty PCAP files in some scenarios.
PCAP log files improved.
An issue setting the ring buffers and MTU on the monitoring interfaces is corrected.
An issue with VPN fallback when the primary gateway is unavailable is corrected.
Various optimizations are applied to the network interfaces .

Known issues and limitations

The following issues have been identified. To inquire about a particular bug, please contact Customer Service & Support.

2.5.0

PCAP Limitation	PCAP capture is not supported on Azure and OCI sensors.
Collector port	Default gateway is not displayed in the config console (cosmetic).
Proxy	When a proxy is enabled on the Azure sensor, the sensor type may appear as Hyper-V after provisioning. This is a known issue and has no functional impact on the sensor

2.4.0

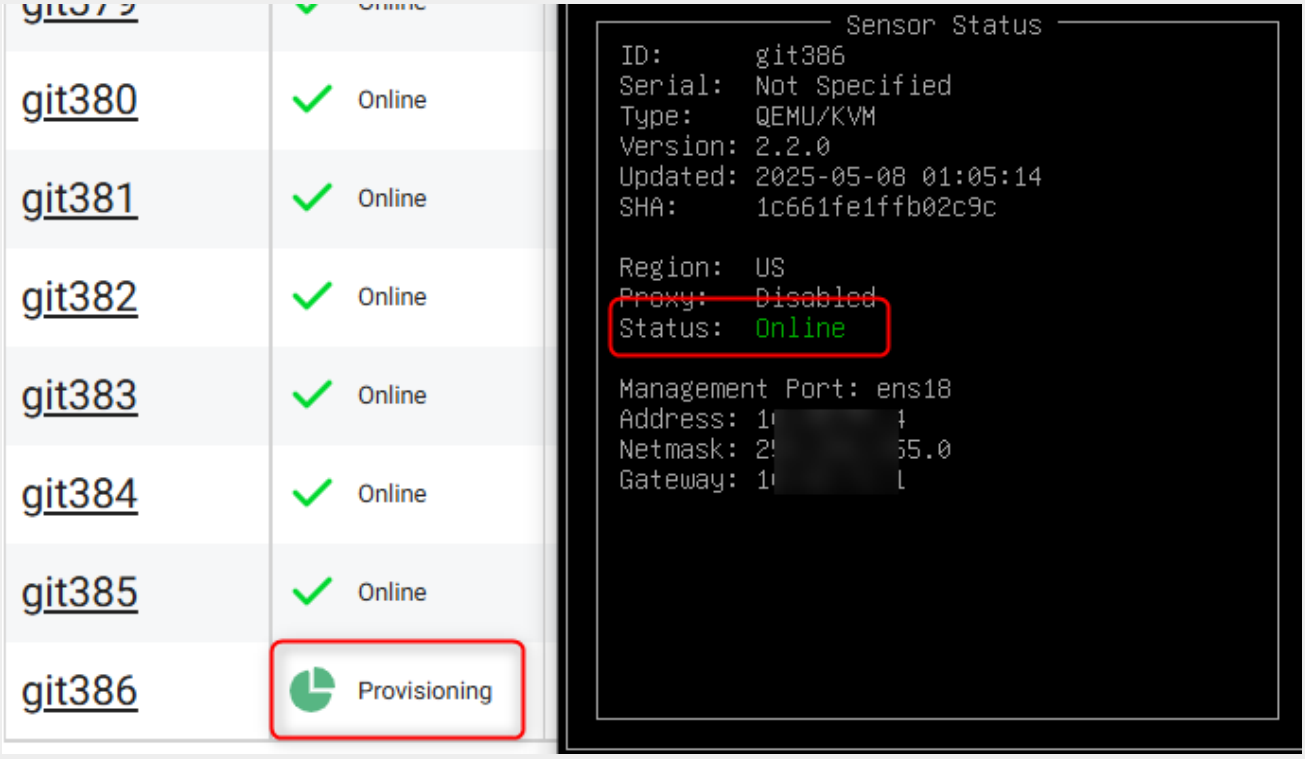
PCAP Limitation	PCAP capture is not supported on Azure and OCI sensors
Diagnostics Limitation	Under rare conditions, sensor connectivity diagnostics may falsely indicate an invalid certificate. Use Legacy Diagnostics as a workaround for connectivity testing.

2.3.0

NetFlow	NetFlow may require a sensord restart or sensor reboot the first time it is enabled in order to receive Netflow traffic.
Collector interface	• Gateway is not visible from the TUI. • Port link and speed not shown in portal (only IP address is displayed).
OCI Sensor:	• NetFlow has limited functionality and may disrupt TAP traffic. The workaround is to use dedicated sensors for each purpose: one for NetFlow and another for TAP traffic rather than running both on the same sensor. • Collector interface cannot obtain DHCP IP (current limitation). The

	workaround is to assign the designated DHCP address as a static IP to the collector interface. • Collector port IP is not removed when unconfigured. The workaround is to reboot the sensor after resetting the collector interface.

2.2.0

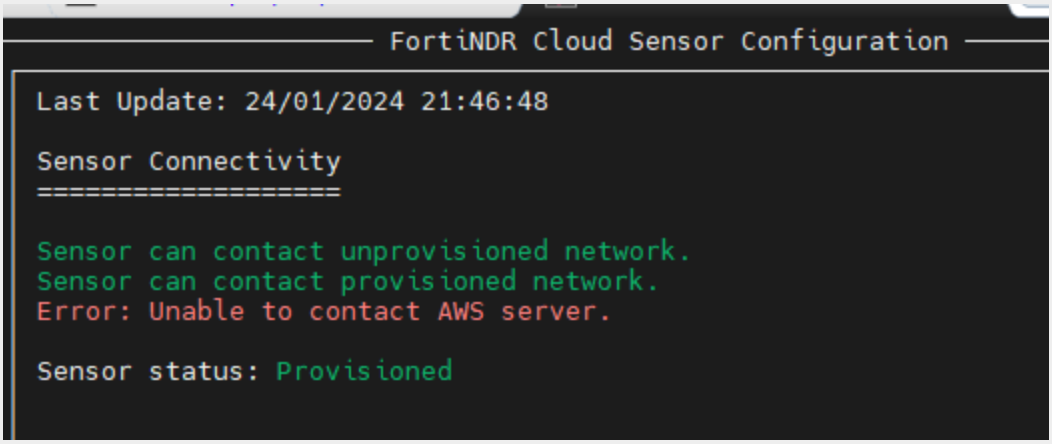
Sensor initial connectivity scans do not go through proxy if proxy is enabled.
AWS sensor upgrade is not supported. To upgrade to this version, a new sensor must be provisioned.
When the sensor is provisioned without a link on any of the monitoring ports, the portal will show the sensor status as *provisioning* even though sensor is online.  For the sensor status to appear as *online* in the FortiNDR Cloud portal, you must establish a link on at least one monitoring port and reboot the sensor.

2.1.0

When disabling proxy, the previous proxy configuration will be deleted and when enabling the proxy again, need to provide the required configuration again and save the configuration

1.11.0

Sensor diagnostics falsely states *Unable to contact AWS server*. This is a cosmetic defect and has no effect on the sensor functionality. This defect also exists in the prior versions and is a result of replacing some backend services.



1.9.0

After upgrading from version 1.6.x (legacy) to version 1.9.0, portal displays the ports both from the 1.6 version and 1.9.0 version. It should only show the ports in 1.9.0 version.

1.8.1

The sensor port media in the portal shows all ports as optical, regardless of the actual port media.

The portal shows the incorrect disk size.

When a PCAP task is in progress, rebooting the sensor or restarting the daemon does not terminate the task. Instead, it causes two PCAP files to be uploaded instead of one.

Change Log

Date	Change Description
2026-04-02	Initial release of 2.5.0.

www.fortinet.com