Physical Sensor Installation Guide

FortiNDR Cloud

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

November 1, 2023
FortiNDR Cloud Physical Sensor Installation Guide
78-231-880084-20231101

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-11-15	Updated Prerequisites on page 11
2023-11-01	Initial release v1.11.0
2023-07-19	Initial release v1.10.0
2023-05-30	Initial release v1.9.0
2023-06-30	Added Sensor Troubleshooting on page 25.
2023-09-22	Updated Prerequisites on page 11 and Sensor Troubleshooting on page 25
2023-10-10	Updated Deployment process on page 6 and Accessing the sensor console on page 12

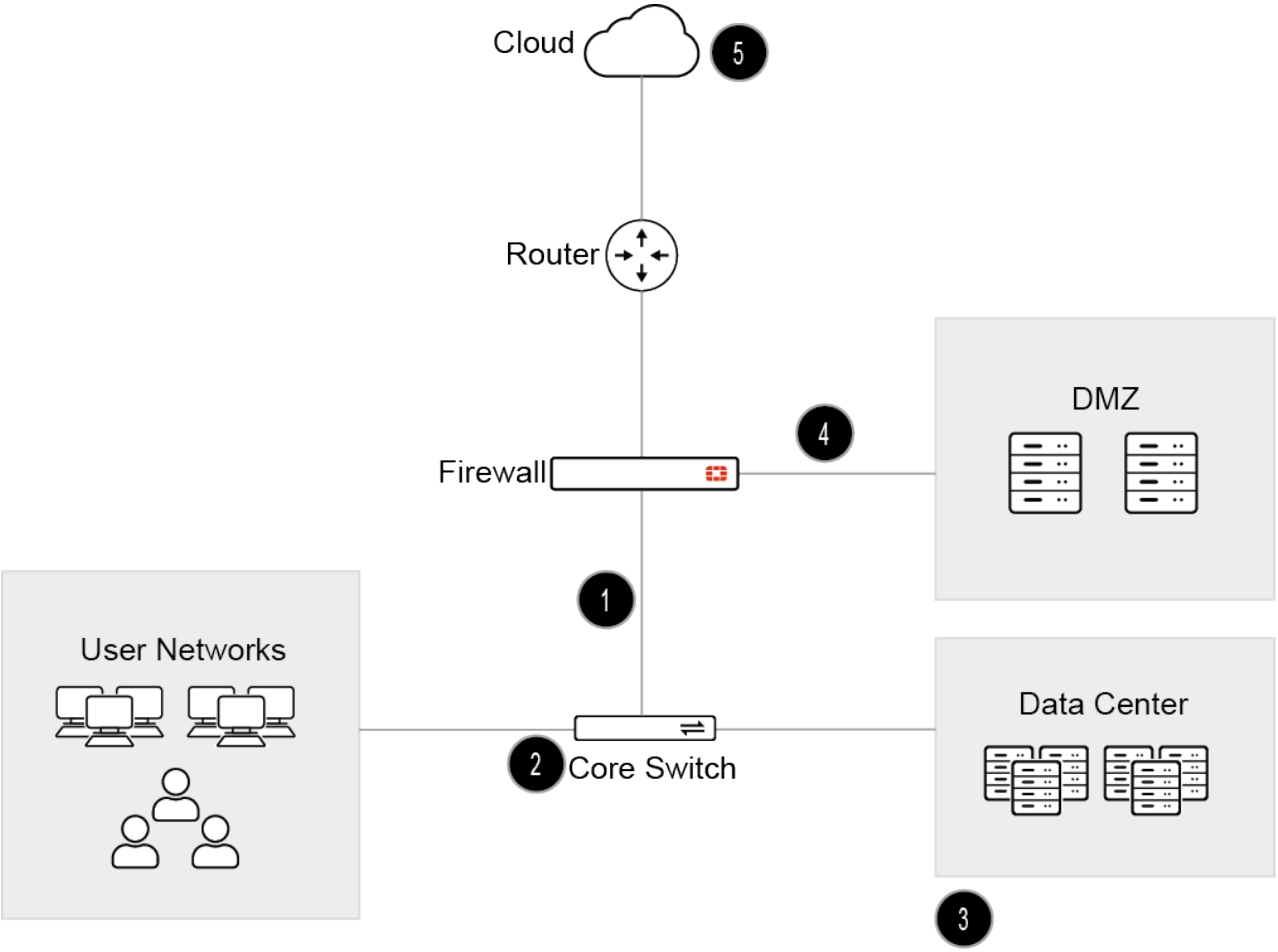
Overview

FortiNDR Cloud is a scalable network security monitoring platform designed for rapid detection and investigation of security threats within your network environment. Network sensor systems collect and process data about activity on your network and forward the data to cloud-based systems for indexing and storage. A web-based application portal and application programming interface (API) are provided for analysis of security events.

The FortiNDR Cloud platform is designed as a Software-as-a-Service (SaaS) and is fully managed by Fortinet Inc. including all network sensor systems, cloud-based systems, and the web-based portal.

Network sensors

Sensors are deployed on specific locations in your network where security events are most likely to occur. Data collected from multiple locations provides a complete and accurate picture of potential security threats. Following is a prioritized list of placement locations in a typical network environment:



Number	Location	Description
1	**Egress Points**	Monitoring activity between your network environment and the Internet provides visibility of security events related to malware beaconing, command and control, network tunneling and data exfiltration activity.
2	**Core Switch**	Activity within your network can include security events related to lateral movement and staging of attacks between workstations and important internal resources such as internal web applications, file servers or your system infrastructure.
3	**Data Center**	Your data center infrastructure is where your important information is stored, making it a target for theft and unauthorized access. Sensors placed between these servers and virtual hosts provide visibility of security events related to this activity.
4	**DMZ**	Public facing applications such as mail services, web sites and business-to-business applications are constantly attacked. Monitoring network zones that host these applications provides visibility of security events related to unauthorized access and data exfiltration.

Deployment process

The FortiNDR Cloud sensor deployment process includes the following steps:

1. Receive, install, and configure a sensor for FortiNDR Cloud.
   After receiving your physical sensor for FortiNDR Cloud, you must install and configure the sensor, and then ensure the sensor can communicate with FortiNDR Cloud through the Internet. This guide includes steps for installation, configuration, and connectivity verification.
2. Register the sensor using a Provisioning Token from FortiNDR Cloud.
   After the sensor is installed and connectivity is verified, you must register the sensor using a Provisioning Token obtained from FortiNDR Cloud. Once the sensor is registered, the provisioning process begins. The provisioning process can take up to two hours to complete.
3. After the provisioning process completes, FortiNDR Cloud analysts start receiving data from your network, and use the data to generate an analysis report for you.
   Once the provisioning process is complete, the sensor will begin forwarding data to the FortiNDR Cloud platform.

Sensor installation

Sensor installation requires the following steps:

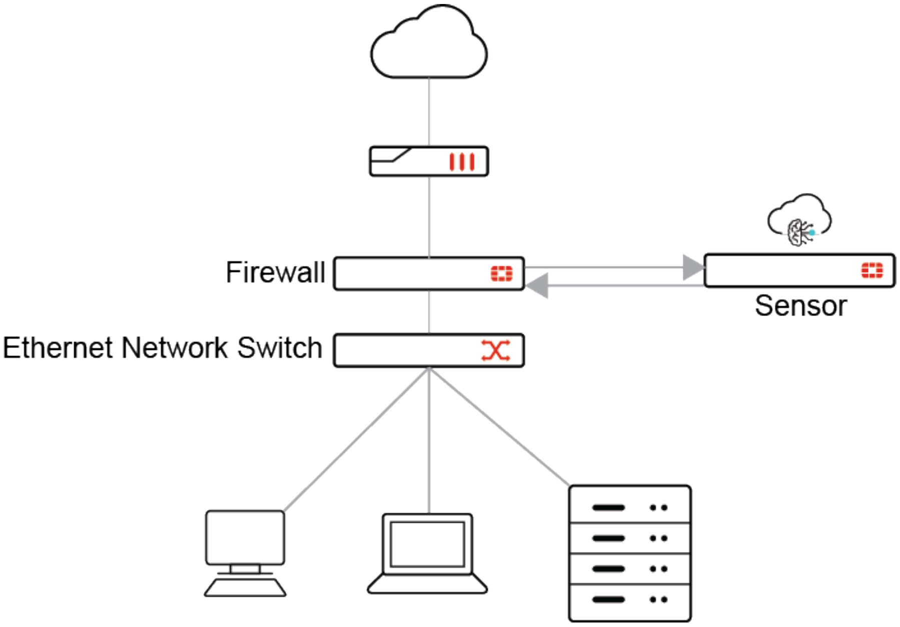
1. Configure a data source for the sensor. See Configuring a network data source on page 7.
2. Install the physical sensor. See Installing a physical sensor on page 8.

Configuring a network data source

A network data source must be configured for the sensor. Sensors collect and process network data using standard network packet capture sources such as a network switch Switched Port Analyzer (SPAN) port or Test Access Port (TAP) device connected to a monitoring interface on the sensor. For more details about the configuration of data sources, please refer to documentation provided by your network hardware vendor.

SPAN Port:

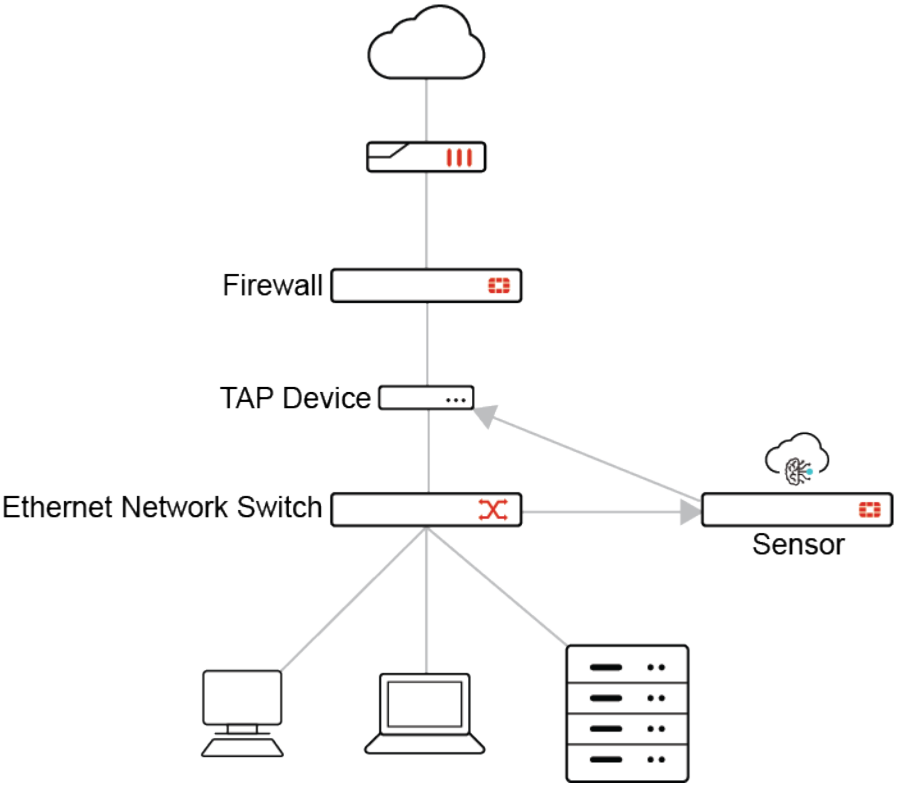
An ethernet network switch port configured to receive copies of all network frames sent or received by other ports on the switch



SPAN ports are sometimes referred to as mirror ports.

TAP Device

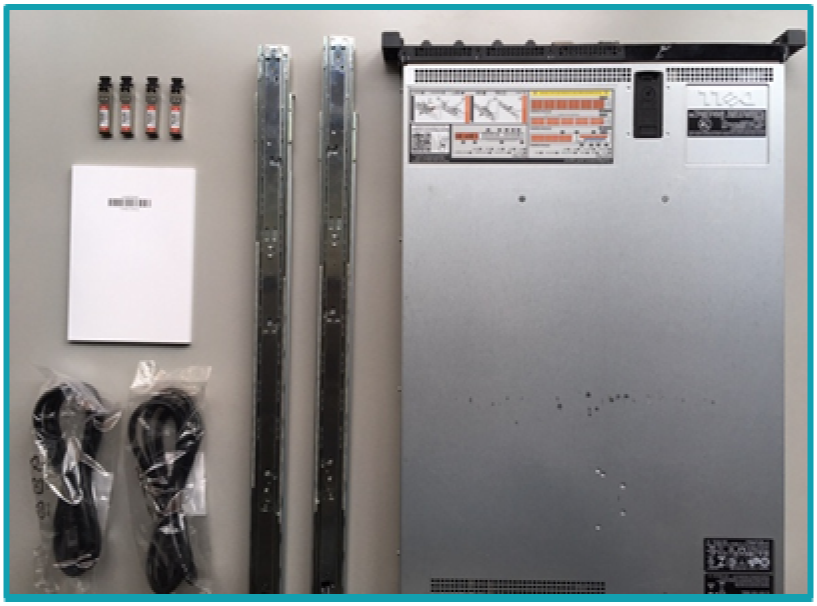
A specialized network device designed to passively intercept and copy network frames as they are transmitted between two network devices such as a switch and firewall



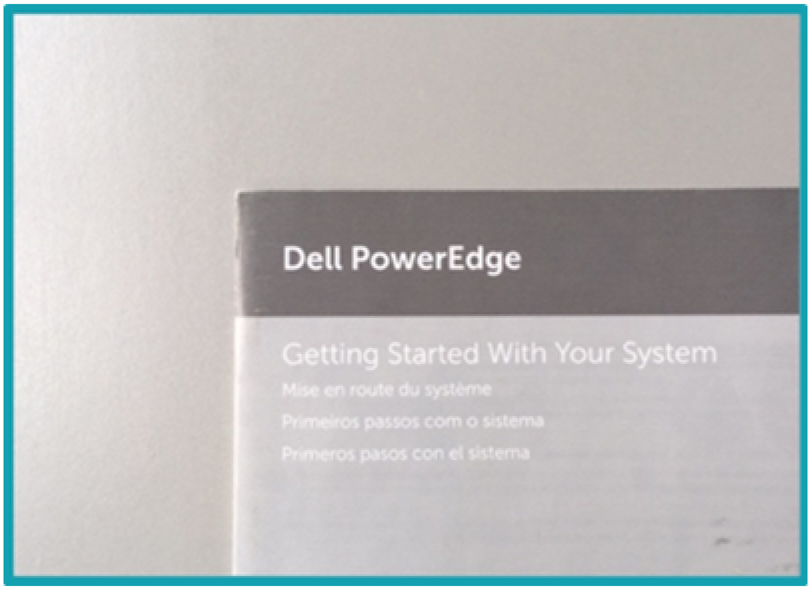
Installing a physical sensor

To install a physical sensor:

1. Confirm that the following items are included in the box:
   - 1U Sensor Chassis
   - 2 Power Cables
   - Server Rack Rails
   - Dell Installation Guide
   - Intel Fiber SFP Modules (optional)



2. Mount the sensor chassis on a server rack within your data center using the included server rack rails. Connect both power cables to available rack power.



Dell PowerEdge

Getting Started With Your System

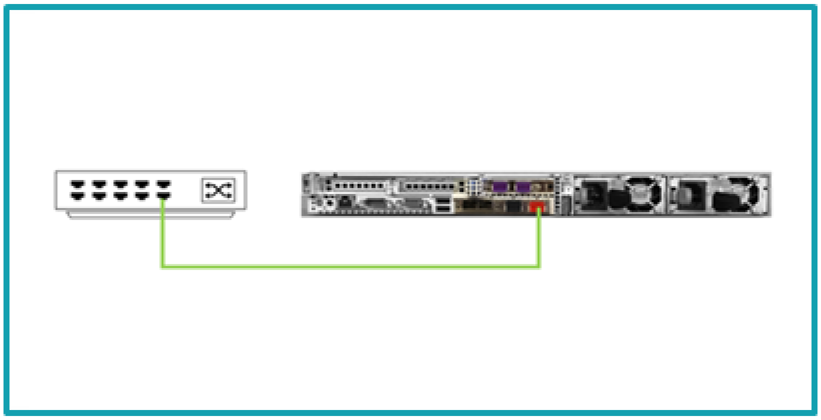
Mise en route du système

Primeiros passos com o sistema

Primeros pasos con el sistema

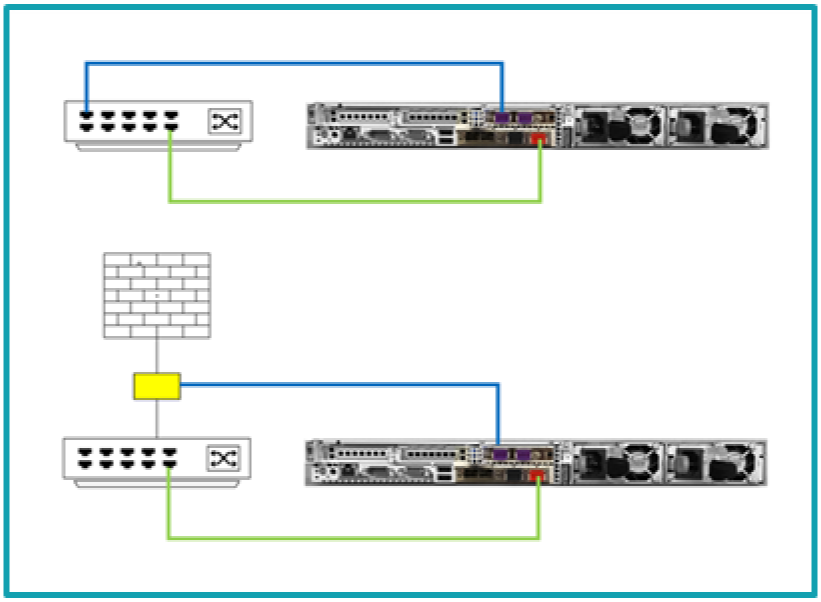
The Dell Installation Guide includes detailed instructions.

3. Connect the *management interface* to an available *switch port* with Internet access.
   The management interface is on the lower-right side of the rear panel marked with a RED port blocker.



4. Connect the *monitoring interfaces(s)* to SPAN port or TAP device *data sources*.
   The monitoring interfaces are marked with BLUE port blockers. The fiber interfaces can be interfaced with SFP modules optionally included with the sensor.

On physical sensors, any number of monitor interfaces can be chosen.



Sensor configuration

Sensor configuration requires the following steps:

1. Understand the prerequisites. See Prerequisites on page 11.
2. Access the sensor console. See Accessing the sensor console on page 12.
3. (Optional) Change the IP assignment for the sensor from DHCP to static if desired. See Changing from DHCP to static IP on page 12.
4. Verify the sensor is connected to the network. See Verifying network connectivity on page 14.
5. Verify the sensor can collect data. See Verifying network data collection on page 16.

Prerequisites

- **Whitelist Addresses**: Sensors must have access to the FortiNDR Cloud infrastructure in order to collect and process data from your network. The following FortiNDR Cloud platform addresses may need to be added to network firewall whitelists to enable this access.

  For sensor versions 1.11.0 and above:

  - 52.36.236.168:443
  - 44.239.228.141:443
  - 138.43.114.141:443
  - 138.43.114.16:443

  The last two IP address/port combinations correspond to *bucket.vpce-0e8d47840a7ffbf5f-hedlogmh.s3.us-west-2.vpce.amazonaws.com:443*. Please ensure this address is not blocked in your web gateway or advanced firewall.

  For sensor versions prior to 1.11.0:

  - 52.36.236.168:443
  - 44.239.228.141:443
  - icebrg-preprod-sensor-ingest.s3.us-west-2.amazonaws.com 443

  If your firewall is not capable of allowing DNS names, you would need to whitelist all the outbound traffic over port 443 with the sensor's management IP address as source.

- **SSL Decryption and Inspection**: Sensors depend on trusted communication and all communications with the FortiNDR Cloud platform are encrypted in transit. SSL decryption and inspection devices may prevent communication between the sensor and the FortiNDR Cloud platform.
- **Public DNS**: Sensor relies on the below public DNS servers to resolve the end points to the sensor infrastructure in FortiNDR Cloud, at least one of these servers should be accessible for sensor registration:
  - 1.1.1.1
  - 8.8.8.8
  - 9.9.9.9

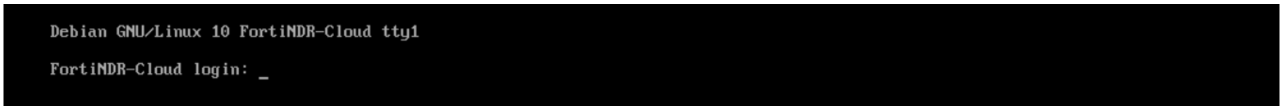
Accessing the sensor console

To access the sensor console:

1. Power on the system.
2. Connect a monitor using the VGA
3. Connect a keyboard using USB2.

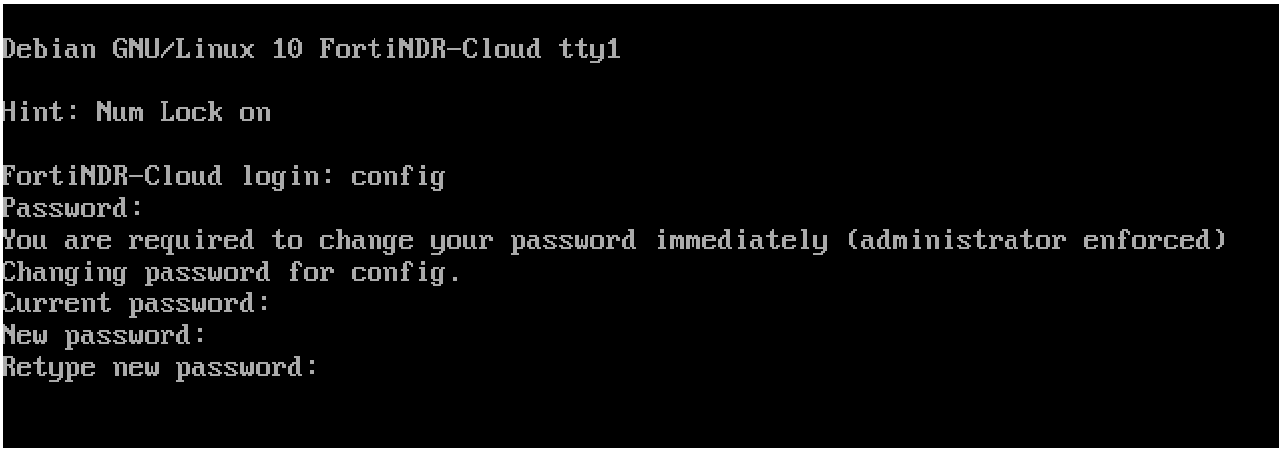
iDRAC and SSH are disabled on all FortiNDR Cloud sensors. Sensors are managed remotely once they are registered and provisioned.

4. When login prompt appears, wait for about 90 seconds for all sensor services to start.



```
Debian GNU/Linux 10 FortiNDR-Cloud tty1

FortiNDR-Cloud login: _
```

5. Log in to the sensor with the following username and password:
   - *Username*: config
   - *Password*: configure
6. Change the password when prompted.



```
Debian GNU/Linux 10 FortiNDR-Cloud tty1

Hint: Num Lock on

FortiNDR-Cloud login: config
Password:
You are required to change your password immediately (administrator enforced)
Changing password for config.
Current password:
New password:
Retype new password:
```

Changing from DHCP to static IP

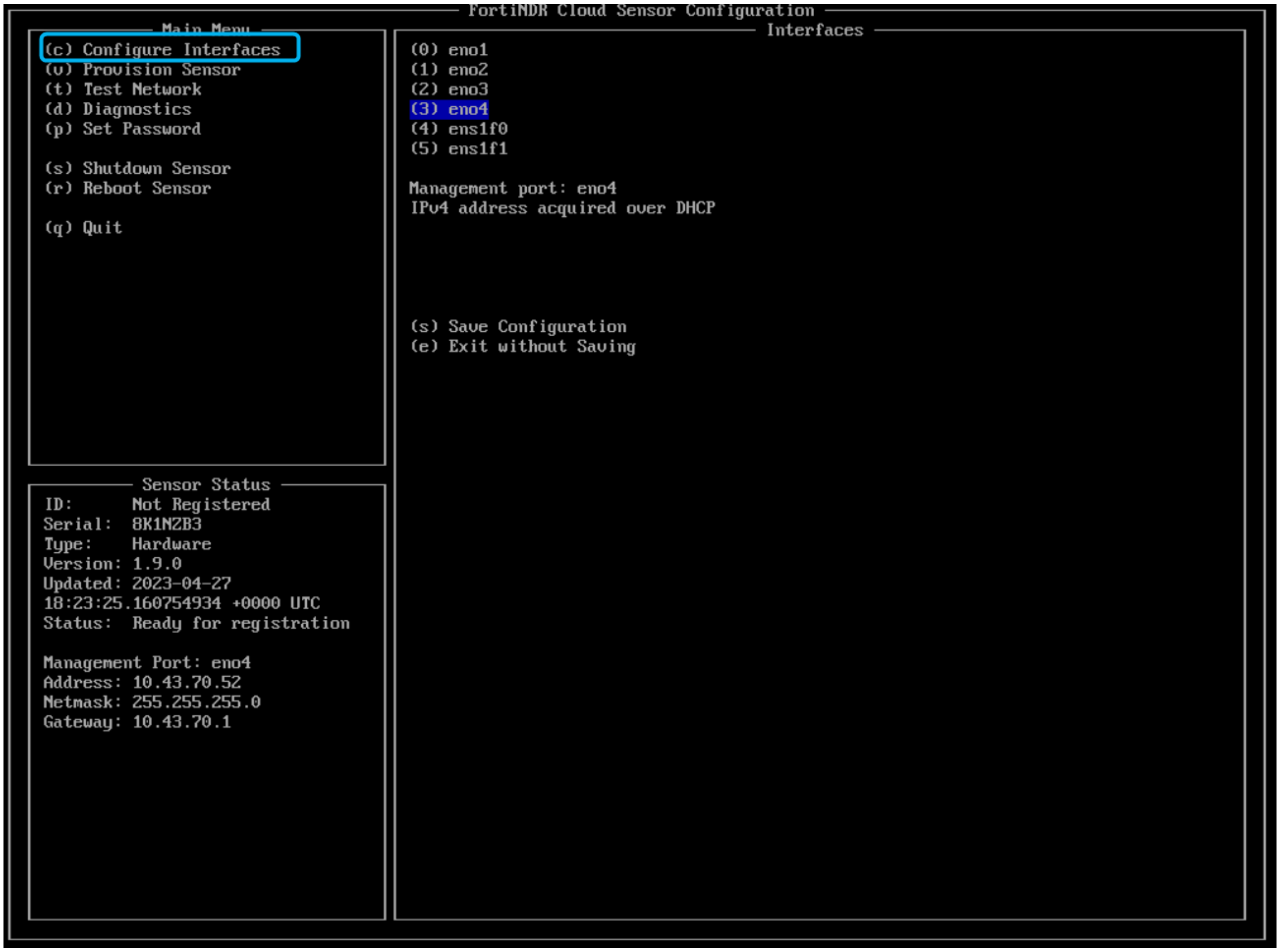
The sensor is configured for DHCP IP address assignment by default. You can change the network configuration to static IP address or select an interface other than the port automatically selected by the sensor to be the management port, as long as the IP stack is available on the network connected to the port you choose.

If you select a different port to be the management port, all other ports will be considered as monitoring ports.

From version 1.10.0, you can enable vxlan on the sensor’s management port. Though this feature is available on the physical sensors, it is recommended for virtual sensors due to the physical sensor’s bandwidth limitation on the management port.

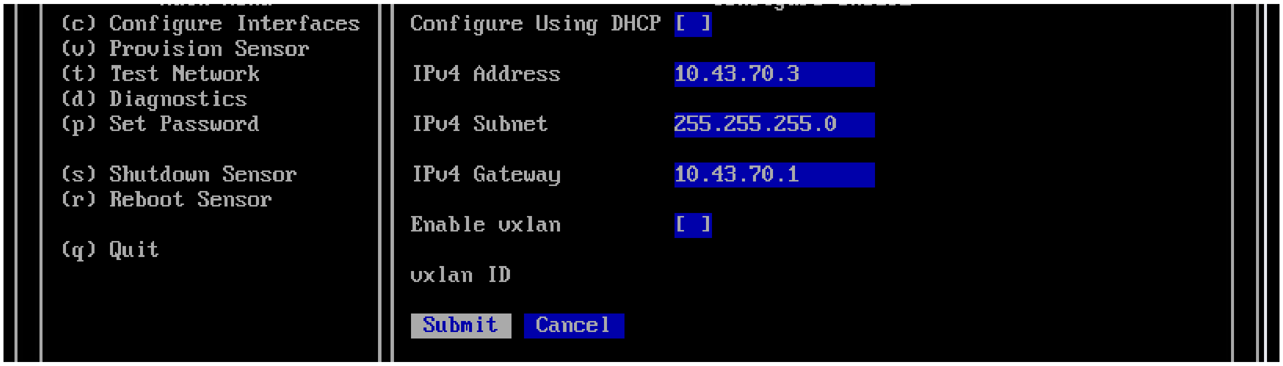
To change from DHCP to static IP:

1. On the *Main Menu* screen, select *Configure Interfaces*.
2. On the *Interfaces* screen, from the interface list, select *eno4*.



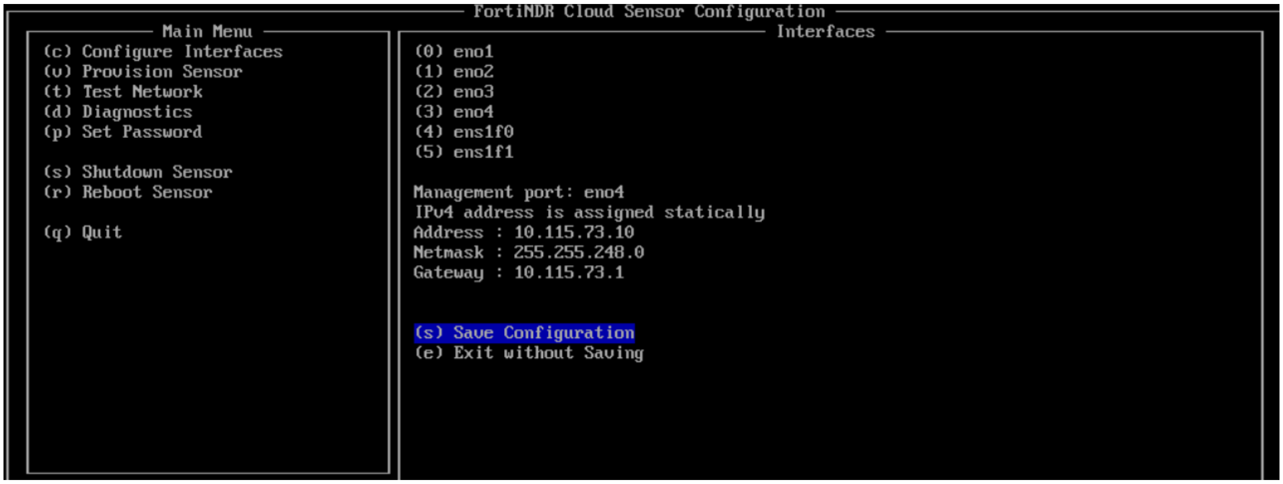
```
                          FortiNDR Cloud Sensor Configuration
 ---- Main Menu ----                      ---- Interfaces ----
 (c) Configure Interfaces        (0) eno1
 (v) Provision Sensor            (1) eno2
 (t) Test Network                (2) eno3
 (d) Diagnostics                 (3) eno4
 (p) Set Password                (4) ens1f0
                                 (5) ens1f1
 (s) Shutdown Sensor
 (r) Reboot Sensor               Management port: eno4
                                 IPv4 address acquired over DHCP
 (q) Quit



                                 (s) Save Configuration
                                 (e) Exit without Saving

 ---- Sensor Status ----
 ID:      Not Registered
 Serial:  8K1NZB3
 Type:    Hardware
 Version: 1.9.0
 Updated: 2023-04-27
 18:23:25.160754934 +0000 UTC
 Status:  Ready for registration

 Management Port: eno4
 Address: 10.43.70.52
 Netmask: 255.255.255.0
 Gateway: 10.43.70.1
```

3. On the *Configure Interface* screen, set the following options, and then click *Submit*:
   - Clear the *Configure Using DHCP* checkbox by pressing the space bar.
   - Complete the static address fields, including the *IPv4 Address*, *IPv4 Subnet*, and *IPv4 Gateway*.



```
(c) Configure Interfaces    Configure Using DHCP [ ]
(v) Provision Sensor
(t) Test Network            IPv4 Address         10.43.70.3
(d) Diagnostics
(p) Set Password            IPv4 Subnet          255.255.255.0

(s) Shutdown Sensor         IPv4 Gateway         10.43.70.1
(r) Reboot Sensor
                            Enable vxlan         [ ]
(q) Quit
                            vxlan ID

                            Submit  Cancel
```

4. On the *Interfaces* screen, select *Save Configuration*.



```
                          FortiNDR Cloud Sensor Configuration
          Main Menu                                  Interfaces
(c) Configure Interfaces   (0) eno1
(v) Provision Sensor       (1) eno2
(t) Test Network           (2) eno3
(d) Diagnostics            (3) eno4
(p) Set Password           (4) ens1f0
                           (5) ens1f1
(s) Shutdown Sensor
(r) Reboot Sensor          Management port: eno4
                           IPv4 address is assigned statically
(q) Quit                   Address : 10.115.73.10
                           Netmask : 255.255.248.0
                           Gateway : 10.115.73.1


                           (s) Save Configuration
                           (e) Exit without Saving
```

5. Reboot the sensor for the changes to take effect.

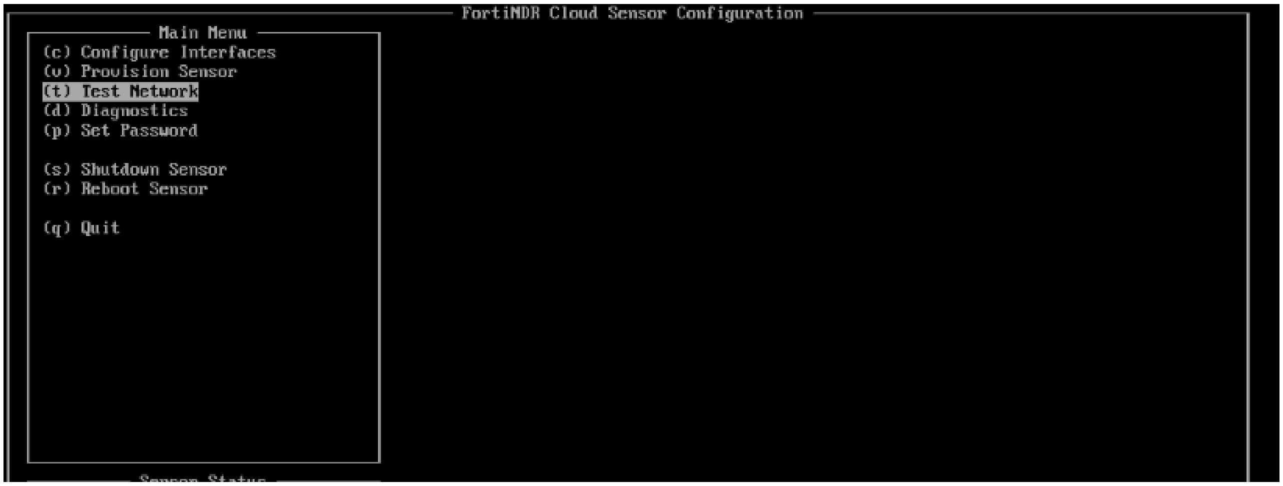
Verifying network connectivity

After installing and configuring the sensor and connecting the management interface, you will need to verify that it has connectivity to the FortiNDR Cloud network to complete the provisioning steps.

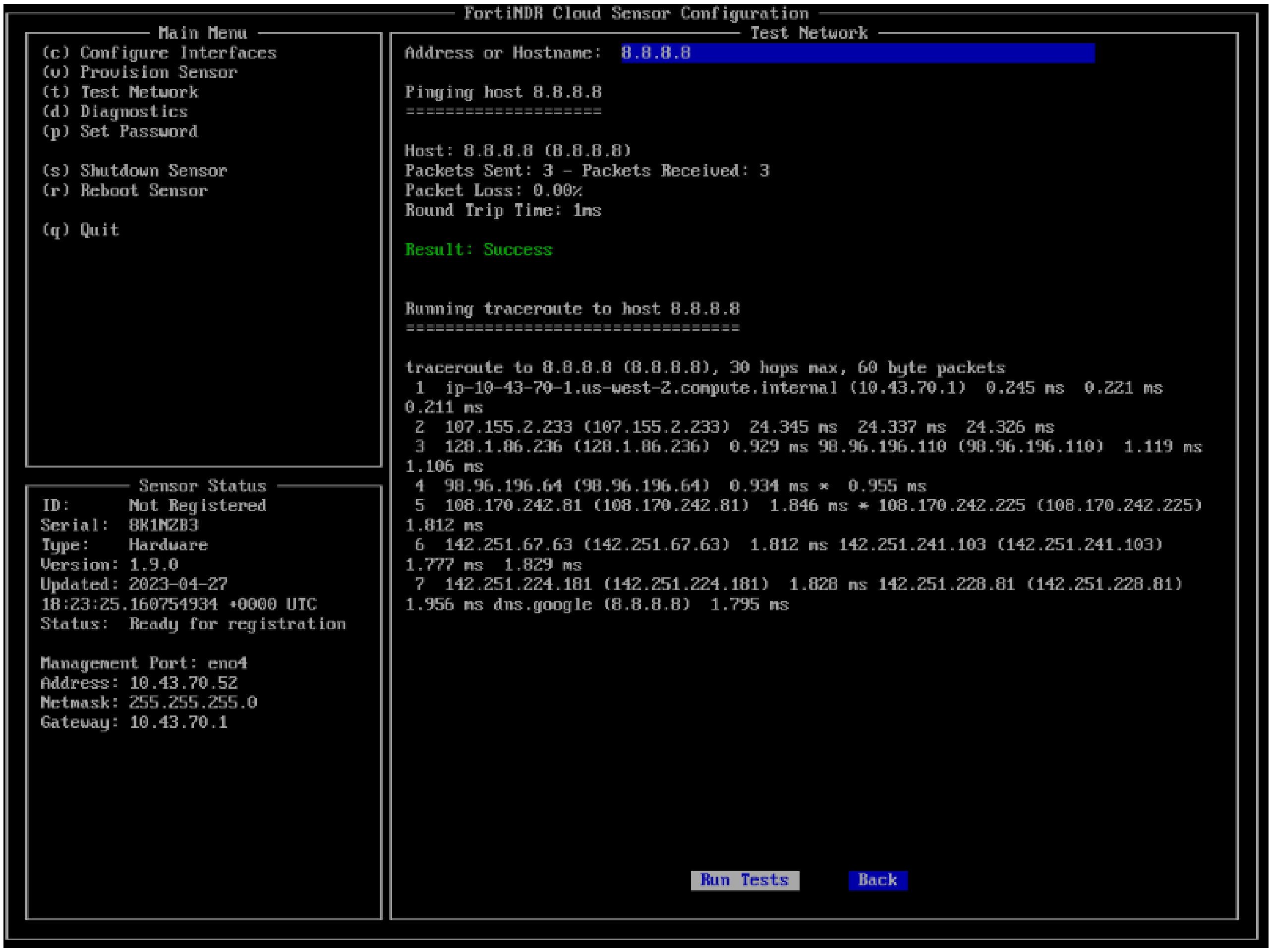
To verify network activity:

1. Log in to the configuration screen.
   - Username: `config`
   - Password: `<your password>`

2. On the *Main Menu* screen, select *Test Network*.



3. On the *Test Network* screen, enter a valid, known IP address on the internet, such as 8.8.8.8, and select *Run Tests* to verify network connectivity.



```
ID:       Not Registered
Serial:   8K1NZB3
Type:     Hardware
Version: 1.9.0
Updated: 2023-04-27
18:23:25.160754934 +0000 UTC
Status:   Ready for registration

Management Port: eno4
Address: 10.43.70.52
Netmask: 255.255.255.0
Gateway: 10.43.70.1
```

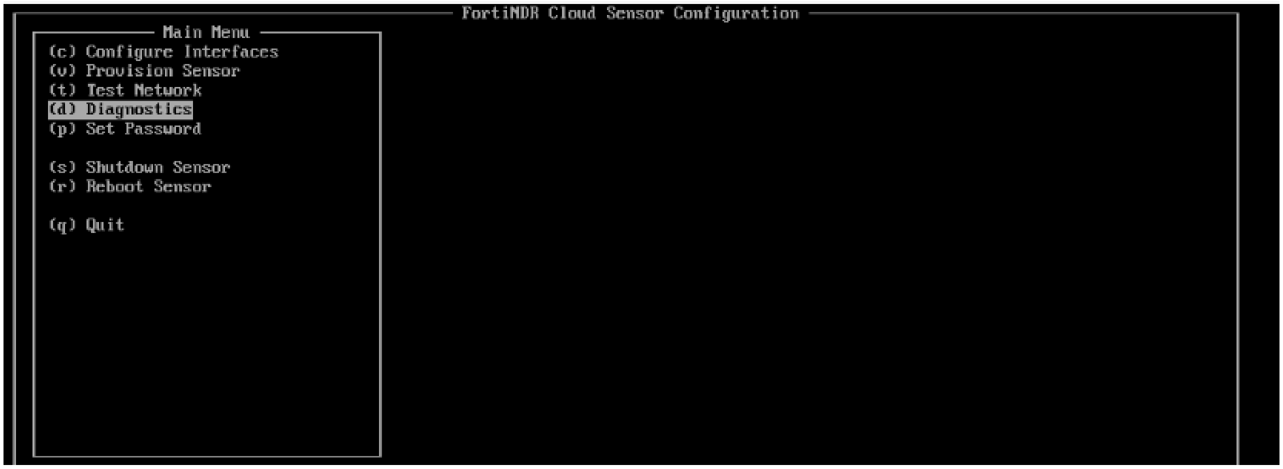
```
Address or Hostname:  8.8.8.8

Pinging host 8.8.8.8
====================

Host: 8.8.8.8 (8.8.8.8)
Packets Sent: 3 - Packets Received: 3
Packet Loss: 0.00%
Round Trip Time: 1ms

Result: Success


Running traceroute to host 8.8.8.8
==================================

traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  ip-10-43-70-1.us-west-2.compute.internal (10.43.70.1)  0.245 ms  0.221 ms
0.211 ms
 2  107.155.2.233 (107.155.2.233)  24.345 ms  24.337 ms  24.326 ms
 3  128.1.86.236 (128.1.86.236)  0.929 ms 98.96.196.110 (98.96.196.110)  1.119 ms
1.106 ms
 4  98.96.196.64 (98.96.196.64)  0.934 ms *  0.955 ms
 5  108.170.242.81 (108.170.242.81)  1.846 ms * 108.170.242.225 (108.170.242.225)
1.812 ms
 6  142.251.67.63 (142.251.67.63)  1.812 ms 142.251.241.103 (142.251.241.103)
1.777 ms  1.829 ms
 7  142.251.224.181 (142.251.224.181)  1.828 ms 142.251.228.81 (142.251.228.81)
1.956 ms dns.google (8.8.8.8)  1.795 ms
```

Verifying network data collection

Verify that the sensor is collecting data from the network data source. You can view traffic statistics for each monitoring interface in the sensor console.

To verify network data collection:

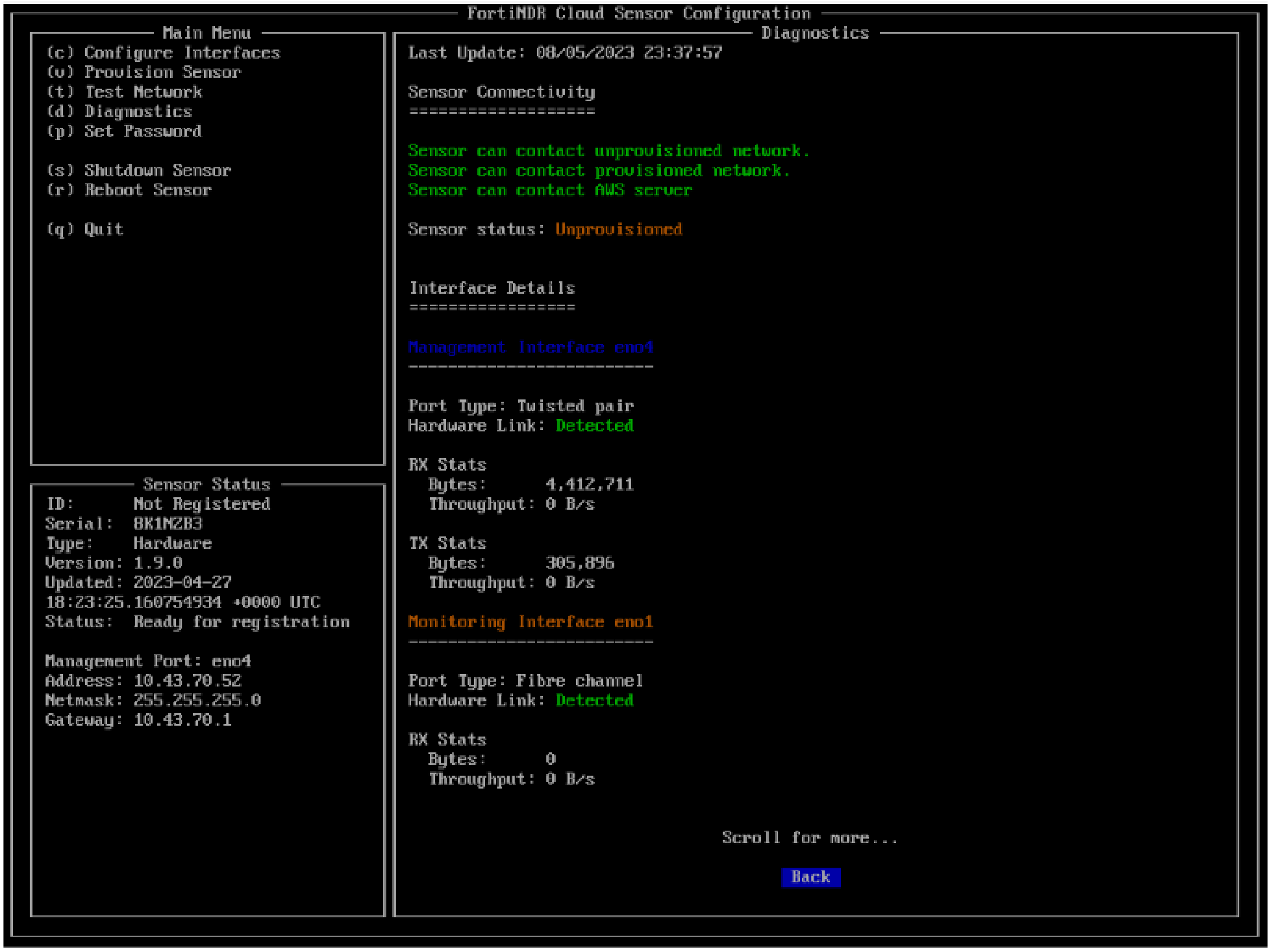
1. Log in to the configuration screen.
2. On the *Main Menu* screen, select *Diagnostics*.



```
FortiNDR Cloud Sensor Configuration
Main Menu
(c) Configure Interfaces
(v) Provision Sensor
(t) Test Network
(d) Diagnostics
(p) Set Password

(s) Shutdown Sensor
(r) Reboot Sensor

(q) Quit
```

3. On the *Diagnostics* screen, under *Sensor Status*, verify that provisioned sensor can connect to *unprovisioned*, *provisioned* and *AWS* end points.

Do not proceed until network connectivity to these end points are established.



```
FortiNDR Cloud Sensor Configuration

Main Menu
(c) Configure Interfaces
(v) Provision Sensor
(t) Test Network
(d) Diagnostics
(p) Set Password

(s) Shutdown Sensor
(r) Reboot Sensor

(q) Quit

Sensor Status
ID:      Not Registered
Serial:  8K1NZB3
Type:    Hardware
Version: 1.9.0
Updated: 2023-04-27
18:23:25.160754934 +0000 UTC
Status:  Ready for registration

Management Port: eno4
Address: 10.43.70.52
Netmask: 255.255.255.0
Gateway: 10.43.70.1
```

```
Diagnostics
Last Update: 08/05/2023 23:37:57

Sensor Connectivity
===================

Sensor can contact unprovisioned network.
Sensor can contact provisioned network.
Sensor can contact AWS server

Sensor status: Unprovisioned


Interface Details
=================

Management Interface eno4
-------------------------

Port Type: Twisted pair
Hardware Link: Detected

RX Stats
  Bytes:      4,412,711
  Throughput: 0 B/s

TX Stats
  Bytes:      305,896
  Throughput: 0 B/s

Monitoring Interface eno1
-------------------------

Port Type: Fibre channel
Hardware Link: Detected

RX Stats
  Bytes:      0
  Throughput: 0 B/s


                Scroll for more...

                     Back
```

4. Under *Interface Details*, for each connected *Monitoring Interface*, verify that *RX Stats* shows a non-zero number for both *Bytes* and *Throughput*.
   Successfully configured interfaces are highlighted in blue.

Sensor provisioning

Provisioning a sensor requires the following steps:

1. Use FortiNDR Cloud to generate a registration code. See Generating a registration code on page 18.
2. Register the sensor with the provided registration code. See Registering sensors on page 19.

Once these steps are complete, the sensor will call home, provision itself, and then be ready to ingest raw mirrored traffic.

Each account is limited to ten (10) sensors by default. To expand this limit, contact your Technical Account Manager.

If needed, you can remove all data from a sensor. See Removing all data from sensors on page 21.

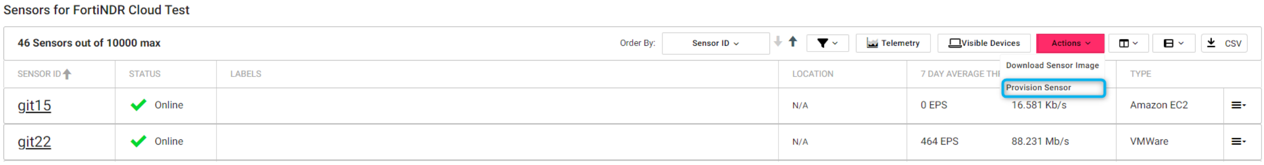
Generating a registration code

Registration codes can be generated in FortiNDR Cloud on the *Sensors* page.

- Codes expire 24 hours after creation.
- Codes can be used an unlimited number of times to provision multiple sensors prior to expiration.
- Codes work for both physical, virtual, and cloud sensors.

To generate a registration code:

1. Log into FortiNDR Cloud.
2. From the *Sensors* page, under Actions, click *Provision Sensor*.



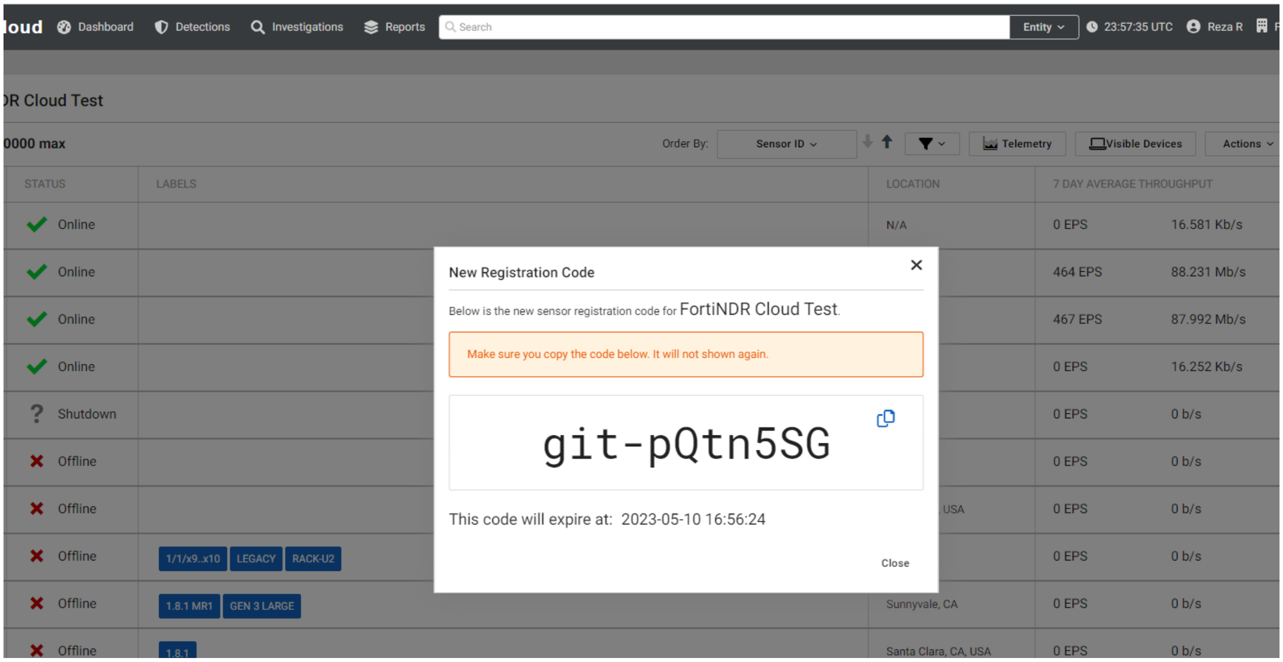
Sensors for FortiNDR Cloud Test

46 Sensors out of 10000 max

SENSOR ID	STATUS	LABELS	LOCATION	7 DAY AVERAGE THI		TYPE
git15	✓ Online		N/A	0 EPS	16.581 Kb/s	Amazon EC2
git22	✓ Online		N/A	464 EPS	88.231 Mb/s	VMWare

A popup box displays a randomly generated registration code prepended with the sensor code for its respective account.

The popup box also displays a *Download Virtual Sensor ISO* link to download a VM file for creating virtual sensors. Be sure to download the VM if you intend to install a virtual sensor.



STATUS	LABELS	LOCATION	7 DAY AVERAGE THROUGHPUT	
✓ Online		N/A	0 EPS	16.581 Kb/s
✓ Online			464 EPS	88.231 Mb/s
✓ Online			467 EPS	87.992 Mb/s
✓ Online			0 EPS	16.252 Kb/s
? Shutdown			0 EPS	0 b/s
✗ Offline			0 EPS	0 b/s
✗ Offline		USA	0 EPS	0 b/s
✗ Offline	1/1/x9..x10 LEGACY RACK-U2		0 EPS	0 b/s
✗ Offline	1.8.1 MR1 GEN 3 LARGE	Sunnyvale, CA	0 EPS	0 b/s
✗ Offline	1.8.1	Santa Clara, CA, USA	0 EPS	0 b/s

New Registration Code

Below is the new sensor registration code for FortiNDR Cloud Test.

Make sure you copy the code below. It will not shown again.

```
git-pQtn5SG
```

This code will expire at: 2023-05-10 16:56:24

3. If you have access to multiple accounts, verify that the generated code begins with the sensor code of the proper account.
4. Write down the code, or copy the code locally as it will not be shown again after the popup box is closed.
   If you accidentally close the popup box before copying the code, generate another code.

Registering sensors

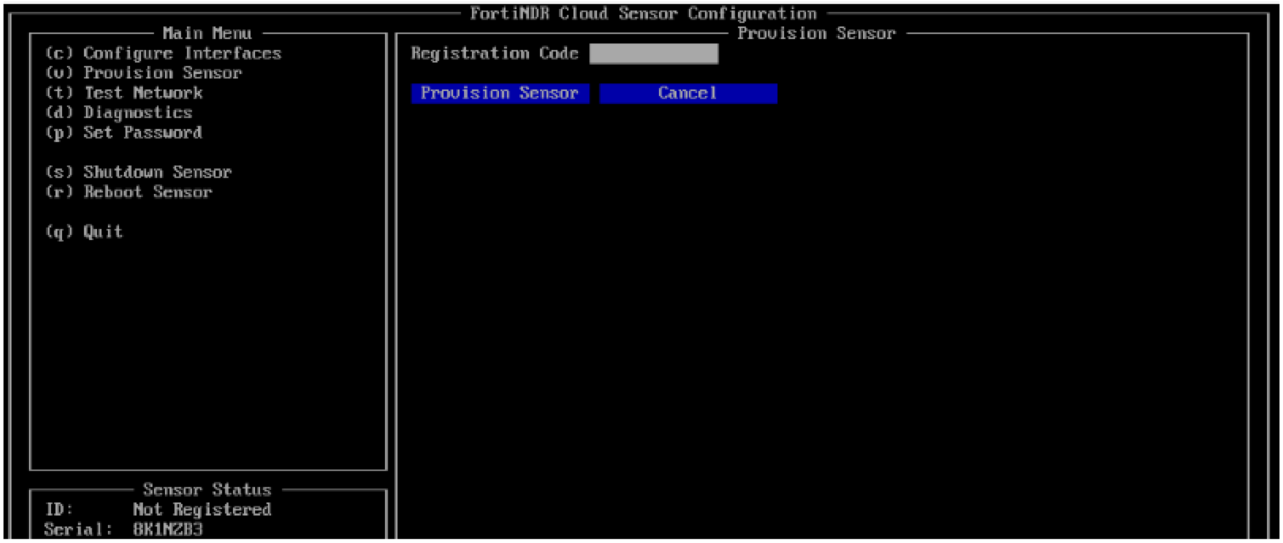
Use the sensor console to register sensors. Perform the following steps to complete the registration process.

The sensor requires Internet connectivity to perform the registration process. Ensure the appliance is connected to the Internet before proceeding.

To register sensors:

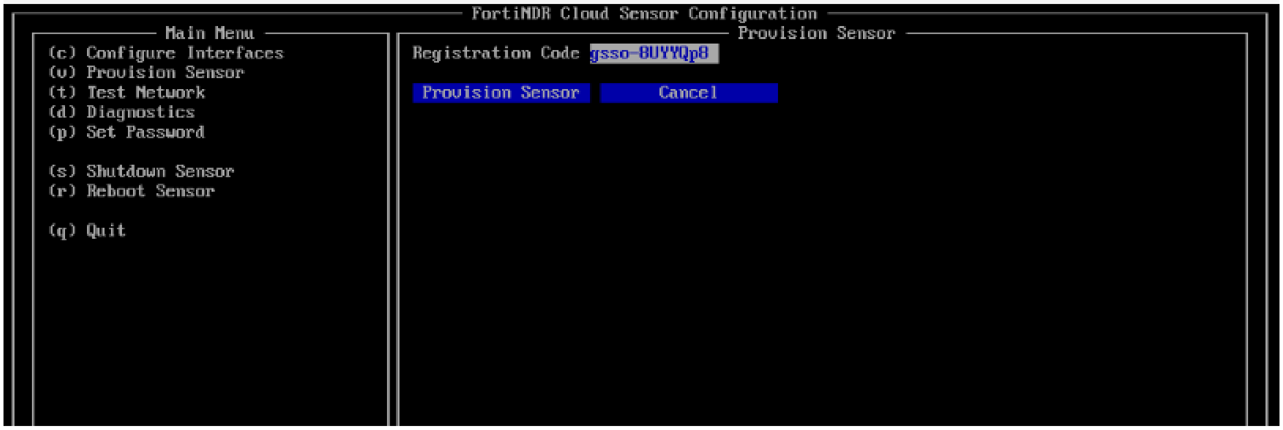
1. Login to the configuration console:
   - Username: `config`
   - Password: `<your password>`
2. Ensure sure that the sensor status is `Ready for Provisioning`.

3. Select *Provision Sensor* (or type *v*).



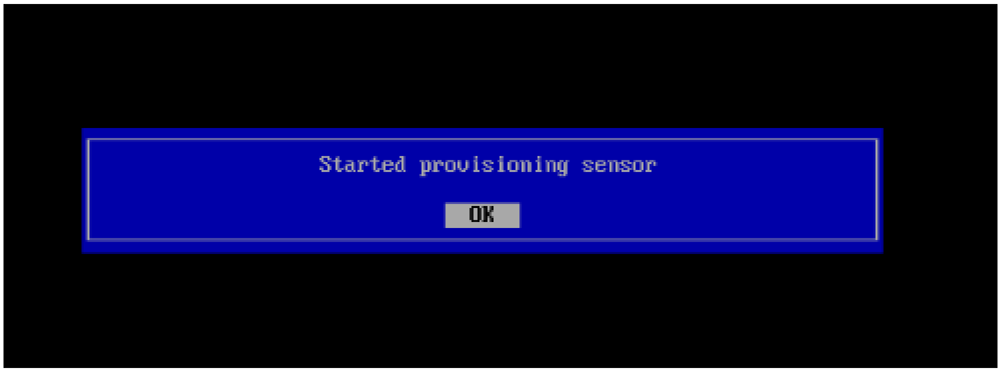
```
FortiNDR Cloud Sensor Configuration
         Main Menu                              Provision Sensor
 (c) Configure Interfaces          Registration Code
 (v) Provision Sensor
 (t) Test Network                  Provision Sensor      Cancel
 (d) Diagnostics
 (p) Set Password

 (s) Shutdown Sensor
 (r) Reboot Sensor

 (q) Quit

        Sensor Status
 ID:      Not Registered
 Serial:  8K1NZB3
```

4. Enter the registration code in the text box.



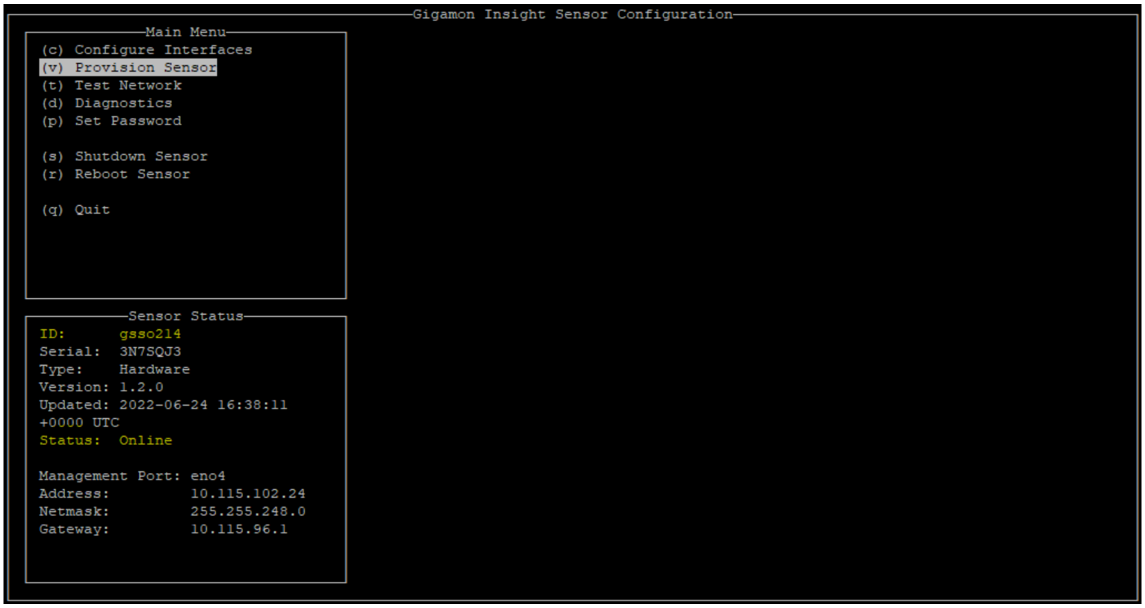
```
FortiNDR Cloud Sensor Configuration
         Main Menu                              Provision Sensor
 (c) Configure Interfaces          Registration Code gsso-8UYYQp8
 (v) Provision Sensor
 (t) Test Network                  Provision Sensor      Cancel
 (d) Diagnostics
 (p) Set Password

 (s) Shutdown Sensor
 (r) Reboot Sensor

 (q) Quit
```

5. Select *Provision Sensor* to begin the registration process.
6. Click *OK*.



```
Started provisioning sensor

            OK
```

7. Once provisioning is complete, the sensor's *ID* will be set to the next sequential sensor code available for the account, and its *Status* will be updated to *Online*, as shown in the following example:



```
                         Gigamon Insight Sensor Configuration
        Main Menu
 (c) Configure Interfaces
 (v) Provision Sensor
 (t) Test Network
 (d) Diagnostics
 (p) Set Password

 (s) Shutdown Sensor
 (r) Reboot Sensor

 (q) Quit

      Sensor Status
ID:      gsso214
Serial:  3N7SQJ3
Type:    Hardware
Version: 1.2.0
Updated: 2022-06-24 16:38:11
+0000 UTC
Status:  Online

Management Port: eno4
Address:         10.115.102.24
Netmask:         255.255.248.0
Gateway:         10.115.96.1
```

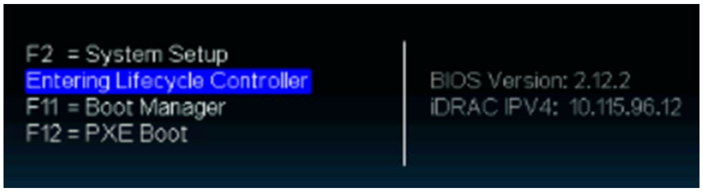
At this point sensor is fully provisioned. Select `Quit` (press `q`) to exit the console.

Removing all data from sensors

Executing this process will remove all data and configuration from the sensor. Do not complete this process unless instructed to do so.

To remove all data from sensors:

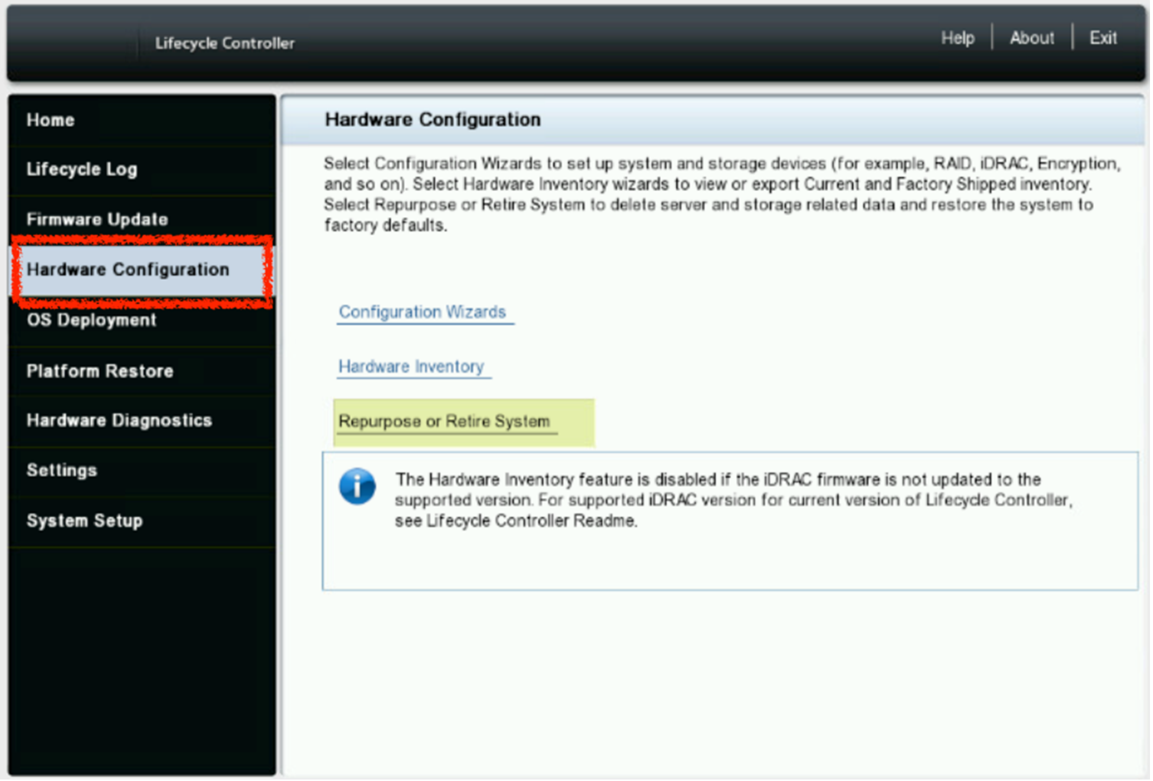
1. Plug in the sensor, and wait for a series of pages to load.
2. Press **F10** (Lifecycle Controller Config iDRAC, Update FW, Install OS).



```
F2  = System Setup              BIOS Version: 2.12.2
Entering Lifecycle Controller   iDRAC IPV4: 10.115.96.12
F11 = Boot Manager
F12 = PXE Boot
```

Once the page finishes loading, the **Lifecycle Controller** page loads. (If several configuration questions are displayed, press **Next**.)

3. On the **Lifecycle Controller** page, select **Hardware Configuration**.

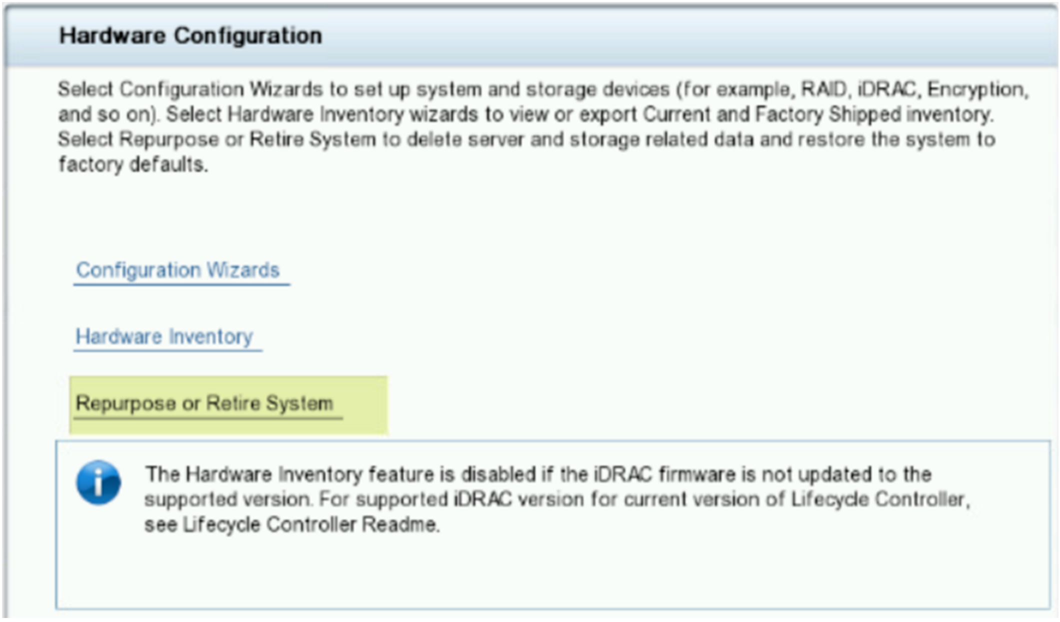


Hardware Configuration

Select Configuration Wizards to set up system and storage devices (for example, RAID, iDRAC, Encryption, and so on). Select Hardware Inventory wizards to view or export Current and Factory Shipped inventory. Select Repurpose or Retire System to delete server and storage related data and restore the system to factory defaults.

The Hardware Inventory feature is disabled if the iDRAC firmware is not updated to the supported version. For supported iDRAC version for current version of Lifecycle Controller, see Lifecycle Controller Readme.

4. On the *Hardware Configuration* page, scroll down and select *Repurpose or Retire System*.



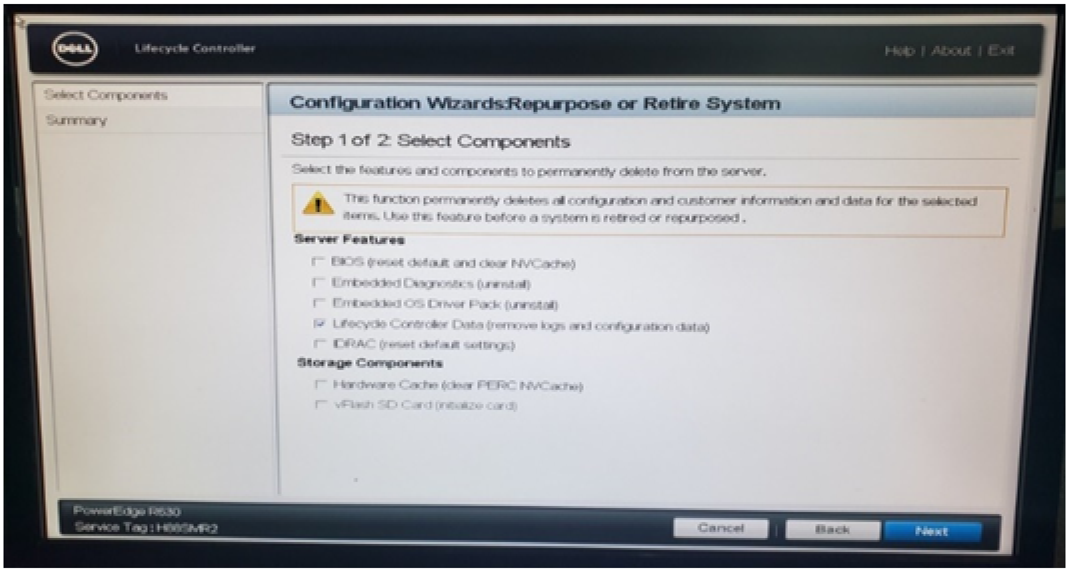
Hardware Configuration

Select Configuration Wizards to set up system and storage devices (for example, RAID, iDRAC, Encryption, and so on). Select Hardware Inventory wizards to view or export Current and Factory Shipped inventory. Select Repurpose or Retire System to delete server and storage related data and restore the system to factory defaults.

The Hardware Inventory feature is disabled if the iDRAC firmware is not updated to the supported version. For supported iDRAC version for current version of Lifecycle Controller, see Lifecycle Controller Readme.

The *Configuration Wizards: Repurpose or Retire System* displays *Step 1 of 2: Select Components*.

5. Select *Lifecycle Controller Data*, and click *Next*.



Configuration Wizards:Repurpose or Retire System

Step 1 of 2: Select Components

Select the features and components to permanently delete from the server.

This function permanently deletes all configuration and customer information and data for the selected items. Use this feature before a system is retired or repurposed .

Server Features

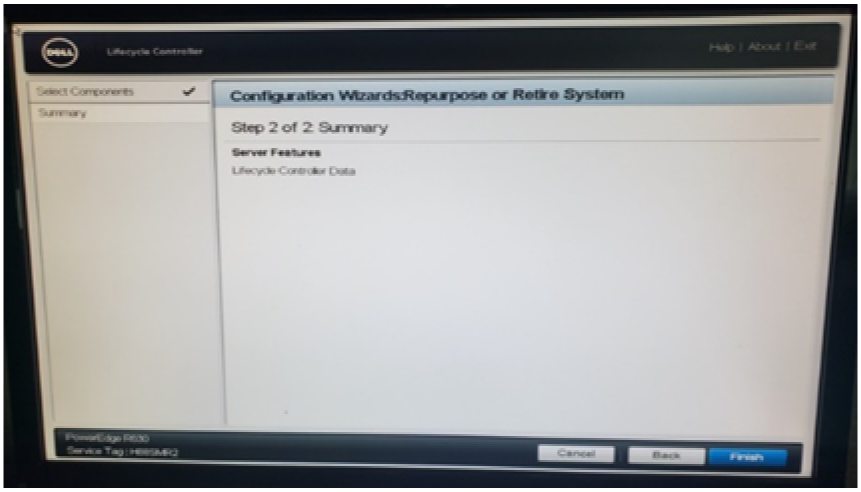
- □ BIOS (reset default and clear NVCache)
- □ Embedded Diagnostics (uninstall)
- □ Embedded OS Driver Pack (uninstall)
- ☑ Lifecycle Controller Data (remove logs and configuration data)
- □ iDRAC (reset default settings)

Storage Components

- □ Hardware Cache (clear PERC NVCache)
- □ vFlash SD Card (initialize card)

The *Configuration Wizards: Repurpose or Retire System* displays *Step 2 of 2: Summary*.

6. Click *Finish*.



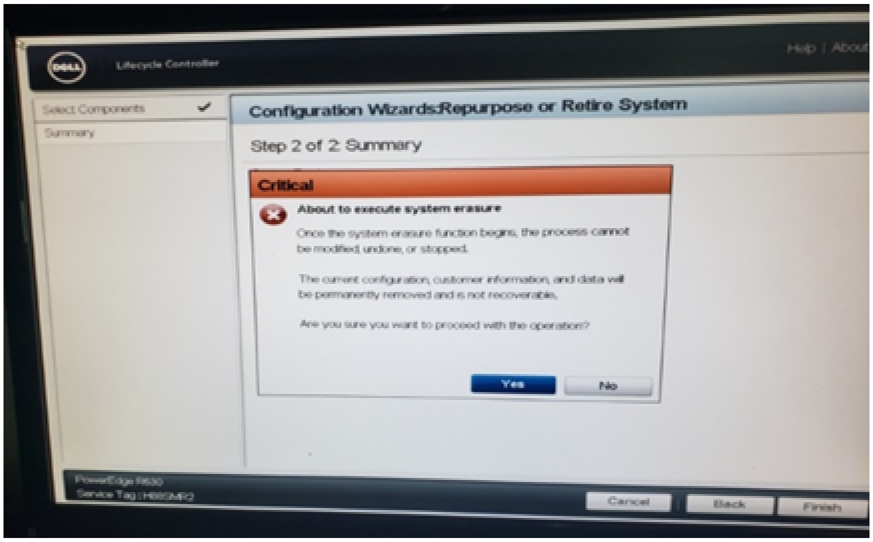
Configuration Wizards:Repurpose or Retire System

Step 2 of 2: Summary

Server Features

Lifecycle Controller Data

A Critical message is displayed.



Configuration Wizards:Repurpose or Retire System

Step 2 of 2: Summary

Critical

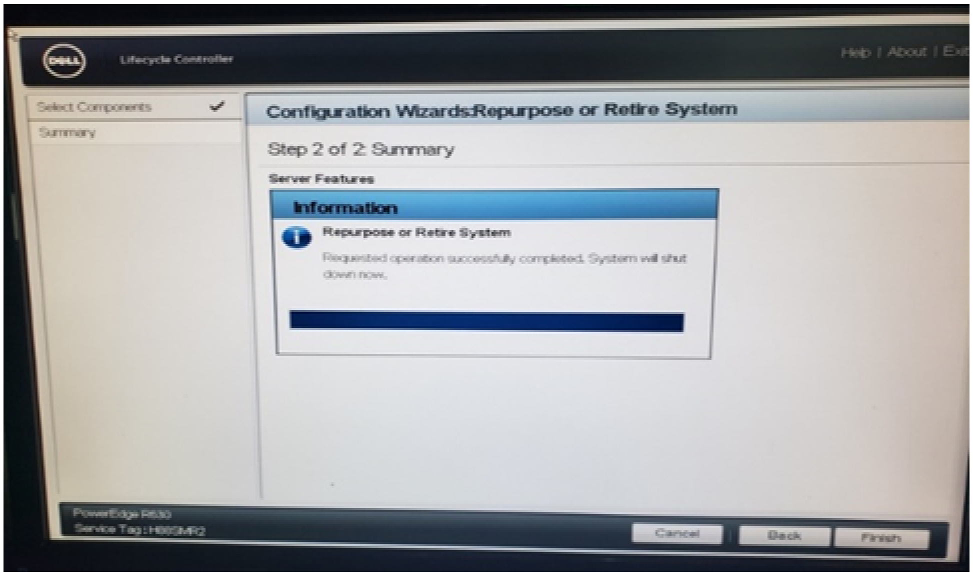
About to execute system erasure

Once the system erasure function begins, the process cannot be modified, undone, or stopped.

The current configuration, customer information, and data will be permanently removed and is not recoverable.

Are you sure you want to proceed with the operation?

7. Select *Yes* to confirm and proceed to the next step.
8. Click *Finish* to execute data removal.



Configuration Wizards:Repurpose or Retire System

Step 2 of 2: Summary

Server Features

Information

Repurpose or Retire System

Requested operation successfully completed. System will shut down now.

9. After the *Configuration Wizards: Repurpose or Retire System* finishes, restart the sensor manually.
   You may need to restart the sensor twice.

Sensor Troubleshooting

General Sensor Information

Sensors only need a management IP, subnet mask, and gateway. No DNS configuration information is necessary. Sensors will respond to ping requests to confirm that they are connected to the network, and they can also execute ping and traceroute requests to verify outbound connectivity. You must physically log in to the sensor, it cannot be accessed remotely.

Access to FortiNDR Cloud Infrastructure

Sensors must have access to the FortiNDR Cloud infrastructure in order to collect and process data from your network. You may need to add the following FortiNDR Cloud platform addresses to any firewall allow lists, specifically for TCP/443, to enable this access:

- 199.85.7.22
- 199.85.7.23
- 35.166.203.96

If the sensor version is 1.8 and above, the following IP and ports should be whitelisted:

End Point	Protocol	Explanation
52.36.236.168:443	TCP	Provisioned VPN
44.239.228.141:443	TCP	Unprovisioned VPN
138.43.114.141:443 138.43.114.16:443	TCP	High availability public S3 [proxy which sensor operations hosts.
icebrg-preprod-sensor-ingest.s3.us-west-2.amazonaws.com	TCP	S3 endpoint

If your firewall is not capable of allowing DNS names, you would need to whitelist all the outbound traffic over port 443 with the sensor's management IP address as source.

In modern senors, the version number is displayed in the `Sensor Status` pane.

SSL Decryption and Inspection

Sensors depend on trusted communication and all communications with the FortiNDR Cloud platform are encrypted in transit. SSL decryption and inspection devices will break communication between the sensor and the FortiNDR Cloud platform and the sensor management IP will need an exclusion from such devices.

Outgoing Traffic Volume

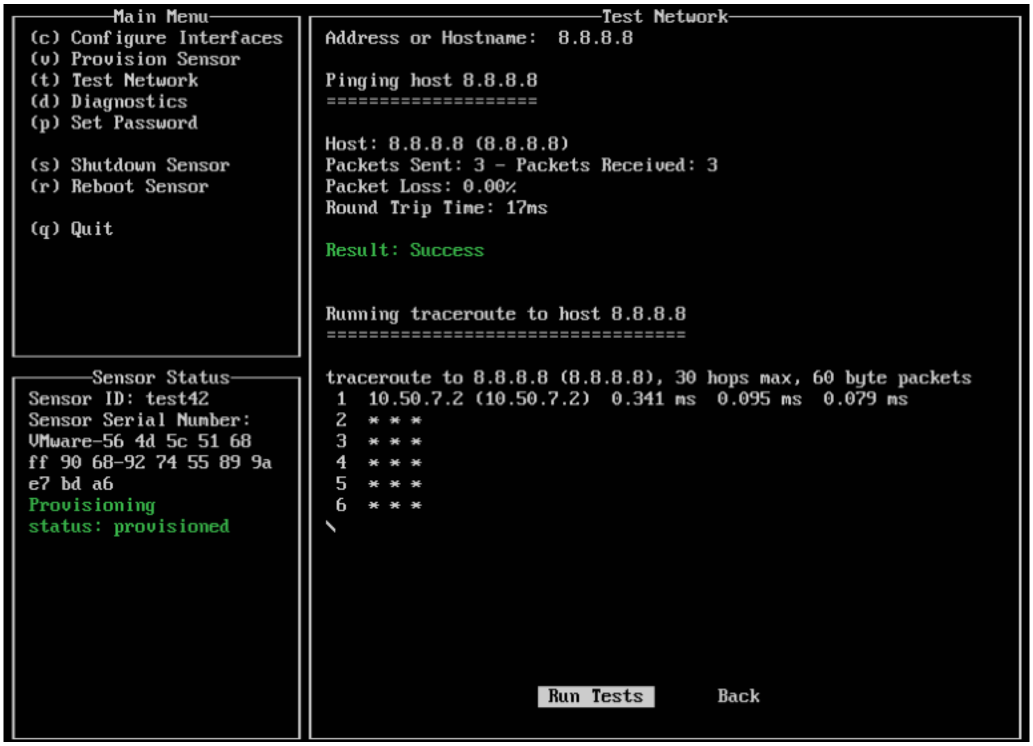
You should expect a volume of traffic outbound from your network to the FortiNDR Cloud infrastructure equal to approximately 1% of the total monitored bandwidth. For example, a sensor monitoring 1Gbps connection will upload approximately 10 Mbps of data for analysis.

Verify Internet Connectivity

The sensor includes a test tool that utilizes ping and traceroute to test Internet connectivity between the sensor and any network address. This tool is useful for verifying connectivity to the network gateway or the FortiNDR Cloud platform addresses. If the sensor is able to reach the Internet but not the FortiNDR Cloud infrastructure, this could indicate that an appliance sitting in the middle, such as an SSL inspector, is breaking the connection.

To Verify Internet Connectivity:

1. On the `Main Menu` screen, select `Test Network` (or press `t`).
2. On the `Test Network` screen, add an address in the `Address or Hostname` field and selects `Run Test` to check for connectivity with the specified address.
3. On the `Test Network` screen, view the output of a standard Ping and Traceroute command as well as a status of the test.



```
Sensor Status
Sensor ID: test42
Sensor Serial Number:
VMware-56 4d 5c 51 68
ff 90 68-92 74 55 89 9a
e7 bd a6
Provisioning
status: provisioned
```

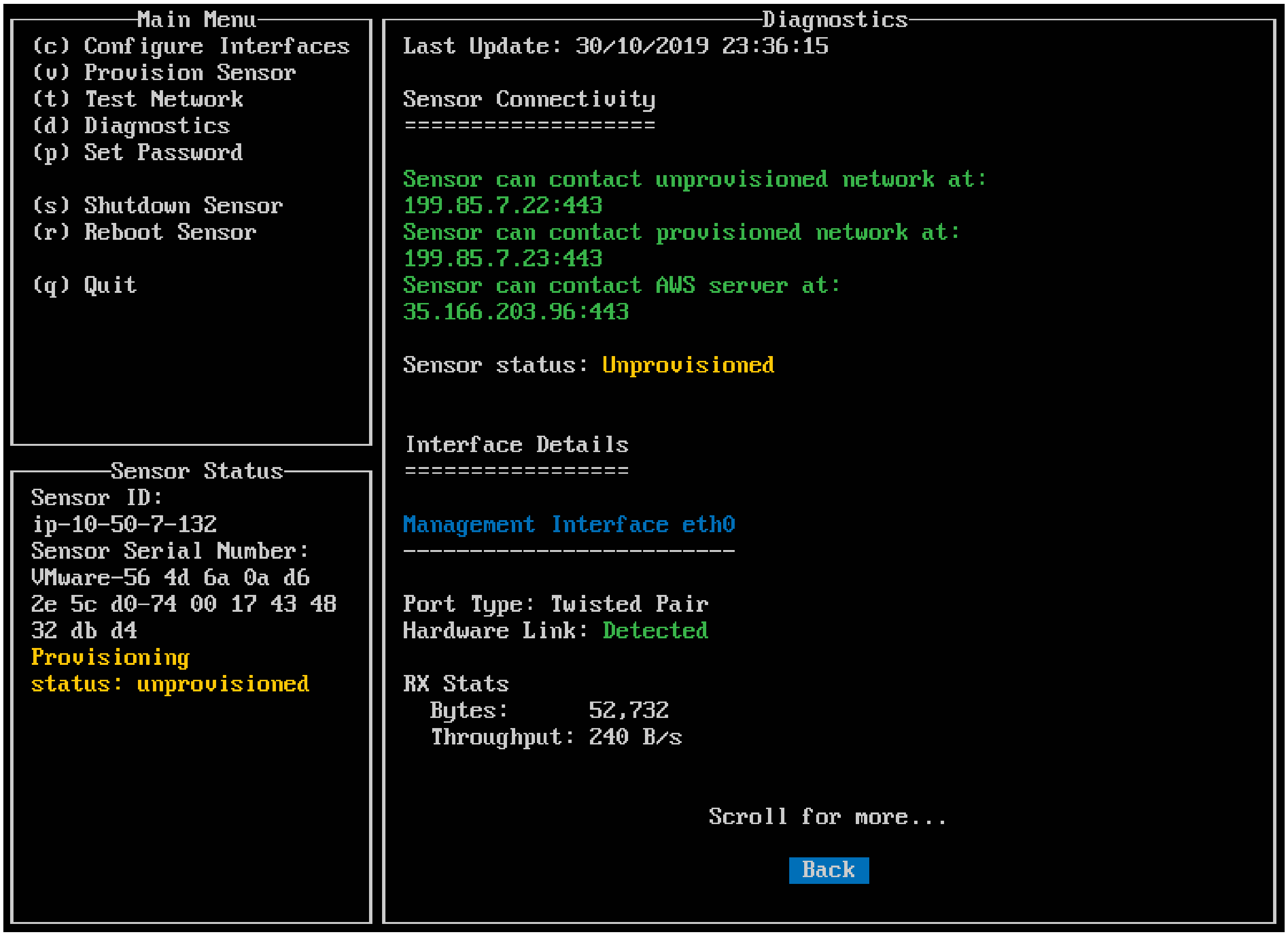
```
Address or Hostname:  8.8.8.8

Pinging host 8.8.8.8
====================

Host: 8.8.8.8 (8.8.8.8)
Packets Sent: 3 - Packets Received: 3
Packet Loss: 0.00%
Round Trip Time: 17ms

Result: Success


Running traceroute to host 8.8.8.8
==================================

traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.50.7.2 (10.50.7.2)  0.341 ms  0.095 ms  0.079 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
\
```

Run Diagnostics

The *Diagnostics* options will first test connectivity to FortiNDR Cloud infrastructure and then test all interfaces for links and traffic.

To run diagnostics:

1. On the `Main Menu` screen, select `Diagnostics` (or press `d`).
2. Under `Sensor Connectivity`, verify that the sensor can reach the FortiNDR Cloud network including the unprovisioned network, provisioned network, and AWS S3 Server. Successful connections will be highlighted in green and include the address and port.
3. Under `Interface Details`, confirm that the necessary interfaces (the management interface and at least one monitoring interface) have a link detected and an expected amount of throughput.



```
Main Menu
(c) Configure Interfaces
(v) Provision Sensor
(t) Test Network
(d) Diagnostics
(p) Set Password

(s) Shutdown Sensor
(r) Reboot Sensor

(q) Quit

Sensor Status
Sensor ID:
ip-10-50-7-132
Sensor Serial Number:
VMware-56 4d 6a 0a d6
2e 5c d0-74 00 17 43 48
32 db d4
Provisioning
status: unprovisioned
```

```
Diagnostics
Last Update: 30/10/2019 23:36:15

Sensor Connectivity
===================

Sensor can contact unprovisioned network at:
199.85.7.22:443
Sensor can contact provisioned network at:
199.85.7.23:443
Sensor can contact AWS server at:
35.166.203.96:443

Sensor status: Unprovisioned


Interface Details
=================

Management Interface eth0
-------------------------

Port Type: Twisted Pair
Hardware Link: Detected

RX Stats
  Bytes:      52,732
  Throughput: 240 B/s


                       Scroll for more...

                             Back
```

www.fortinet.com