Hyper V Sensor Deployment

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 2, 2026
FortiNDR Cloud 2.5.0 Hyper V Sensor Deployment
78-250-935121-20260204

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-04-02	Initial release version 2.5.0

Overview

FortiNDR Cloud is a scalable network security monitoring platform designed for rapid detection and investigation of security threats within your network environment. Network and Cloud sensor systems collect and process data about your network and cloud activity 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.

FortiNDR Cloud Sensors are deployed on specific locations in your physical, virtual or cloud network where security events are most likely to occur. Data collected from multiple locations provides a complete and accurate picture of potential security threats.

This guide will take you through the steps to successfully deploy a FortiNDR Cloud sensor in a Microsoft Hyper-V environment in addition to different setup for monitoring intra-VM and external span packet flow.

Requirements

Minimum VM requirements

The following table lists minimum and recommended requirements for cores, memory, and storage.

Requirement	Minimum
Minimum Cores	8
Minimum Memory	16GB
Minimum storage	100GB
Recommended Cores	16
Recommended Memory	32GB
Recommended storage	300GB

System requirements

Before deploying the FortiNDR Cloud sensor, make sure you meet the following requirements:

- A Hyper-V environment on Windows Server 2019 or later.
- A valid Fortinet sensor ISO downloaded from the portal and accessible on the host.
- Connection to the public network.
- Additional physical network interface on the host (for external span monitoring only).

Allowlist Addresses

Sensors must have access to the FortiNDR Cloud infrastructure in order to collect and process data from your network. Ensure that the following FortiNDR Cloud platform addresses are allowlisted on your firewall.

For deployment in the US and other regions

End Point	Protocol	Explanation
52.36.236.168:443	TCP	Unprovisioned VPN

End Point	Protocol	Explanation
44.239.228.141:443	TCP	Provisioned VPN
138.43.114.16:443 138.43.114.141:443	TCP	S3 endpoint

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 EU deployments:

End Point	Protocol	Description
18.153.171.115:443	TCP	Unprovisioned VPN
3.124.46.55:443	TCP	Provisioned VPN
3.72.240.234:443 3.123.116.122:443	TCP	S3 endpoint S3 endpoint

The last two IP address/port combinations (*3.72.240.234:443* and *3.123.116.122:443*) correspond to `bucket.vpce-04cca23d7dbdf8626-x2c1jp2i.s3.eu-central-1.vpce.amazonaws.com`.

Please ensure this address is not blocked in your web gateway or advanced firewall.

To provision in the APAC region:

End Point	Protocol	Description
47.131.38.17:443	TCP	Unprovisioned VPN
13.251.235.20:443	TCP	Provisioned VPN
13.215.106.143:443	TCP	S3 endpoint
13.251.181.190:443		S3 endpoint

The last two IP address/port combinations (13.215.106.143:443 and 13.251.181.190:443) correspond to *bucket.vpce-0ef3cbdf9c3b9627e-3tjxjoj7.s3.ap-southeast-1.vpce.amazonaws.com*.

Please ensure this address is not blocked in your web gateway or advanced firewall.

SSL decryption and inspection

Important!

Sensors rely on trusted communication, and all interactions with the FortiNDR Cloud platform are encrypted in transit. **SSL decryption and inspection devices may disrupt communication between the sensor and the FortiNDR Cloud platform.**

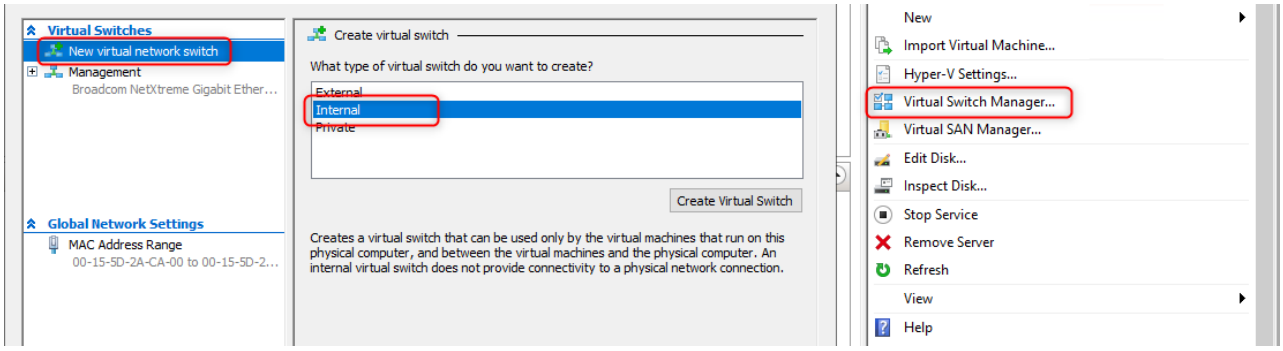
Virtual Switch creation

Intra VM monitoring

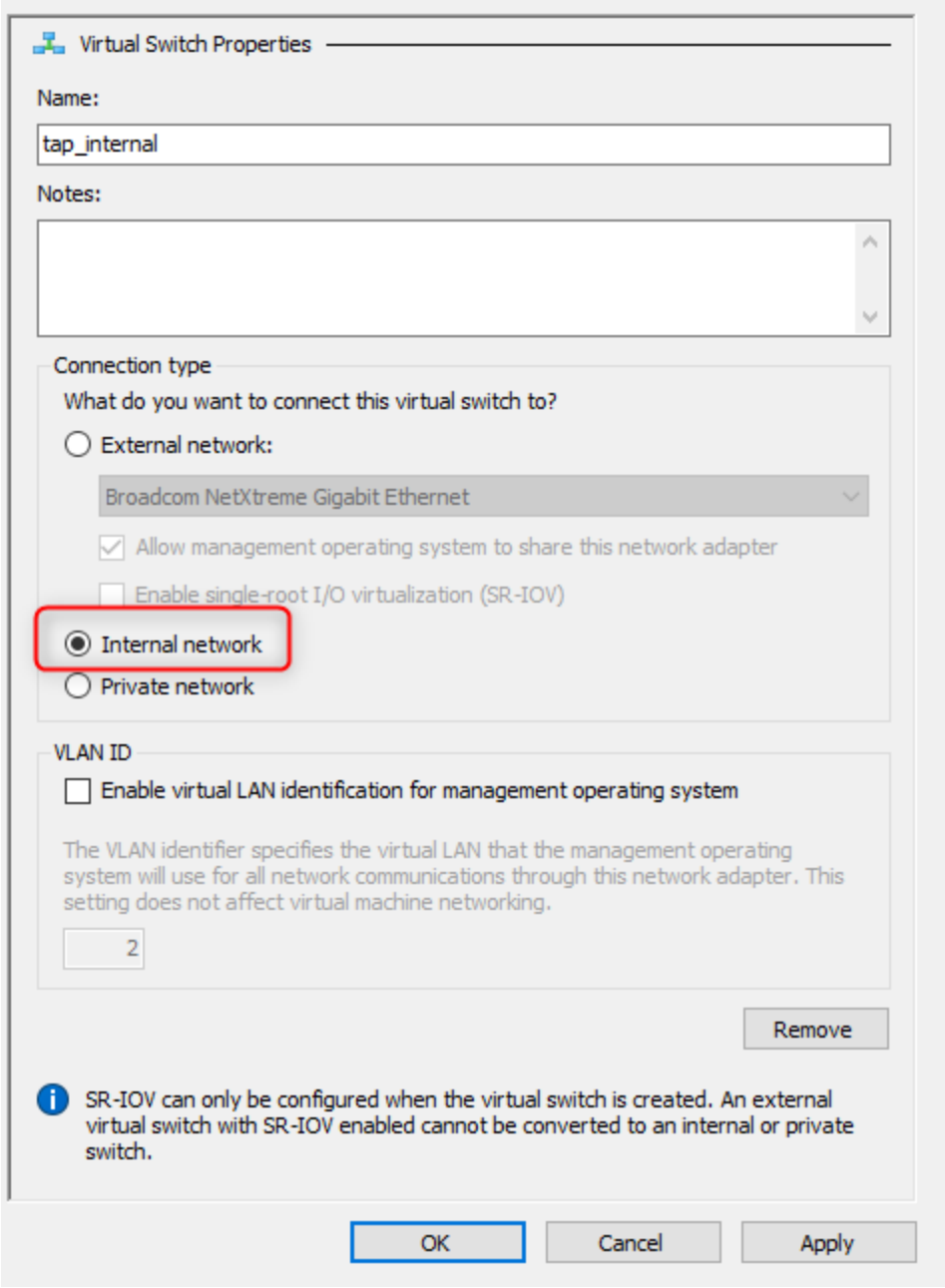
If you wish to monitor only the activity of the VMs connected to a specific virtual switch and currently no virtual switch is already present, follow the steps below:

To monitor VMs connected to a specific virtual switch when none is present:

1. In the Hyper-V manager go to *Virtual Switch Manager*.
2. Select *New Virtual network switch* highlight *Internal* in the right-side pane and click *Create virtual switch*



3. Give the switch a name and click *OK*

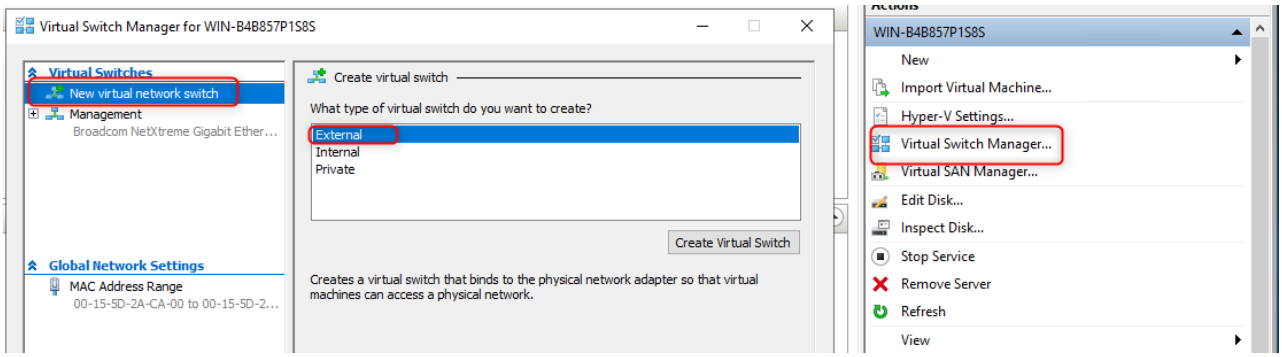


External span monitoring

If you are interested in monitoring a switch span connected to a physical interface on the Windows server hosting the Hyper-V environment, follow the steps below. Given that Windows does not support promiscuous mode, parts of configuration will need to be performed using the Windows Power shell.

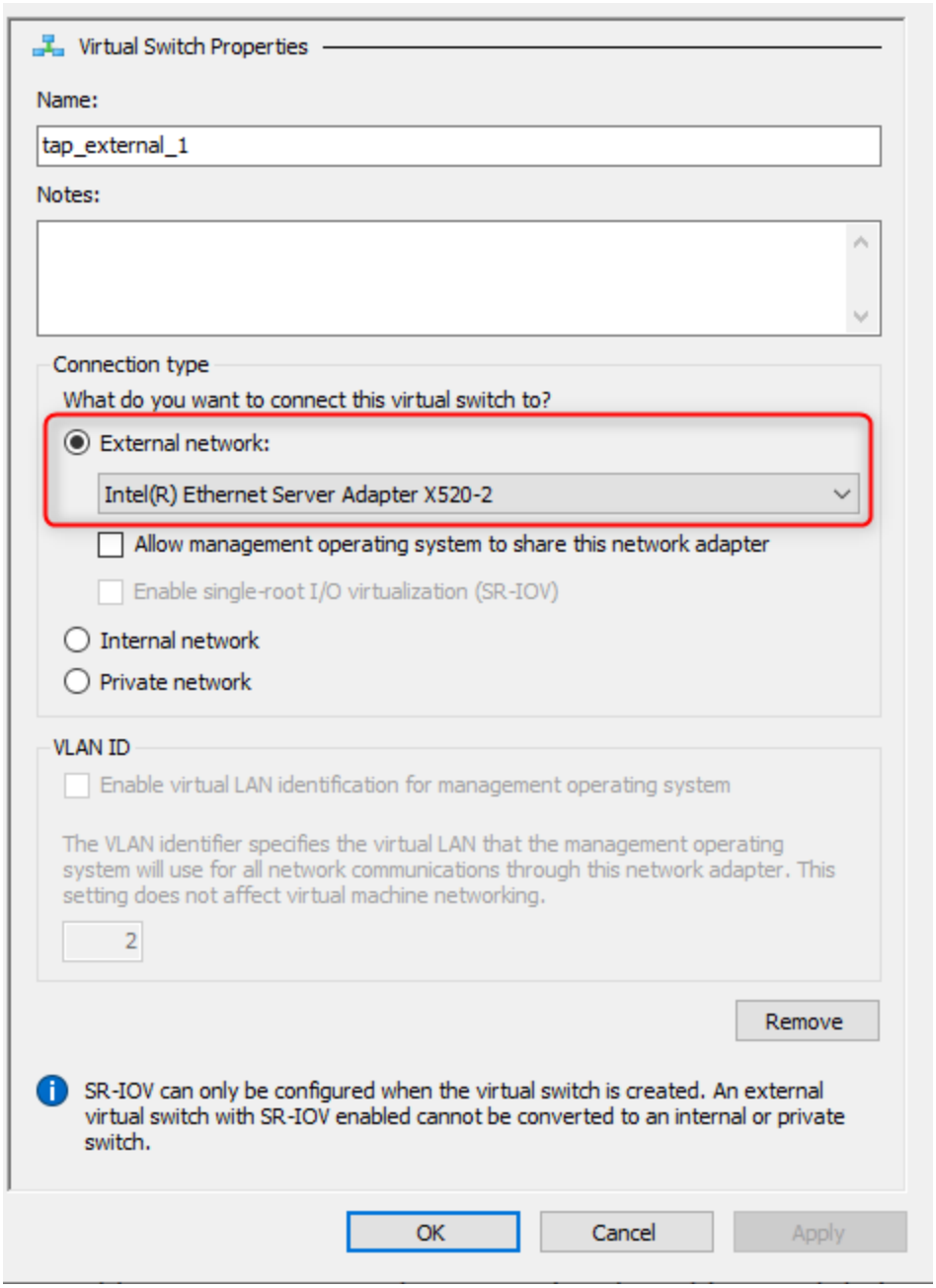
To monitor a switch span connected to a physical interface on the Windows server:

1. In the Hyper-V manager go to *Virtual Switch Manager*.
2. Select *New Virtual network switch* highlight *External* in the right-side pane and click *Create virtual switch*.



3. Give the switch a name.
4. Select the physical interface connected to the switch's span port.

5. Click *OK*.



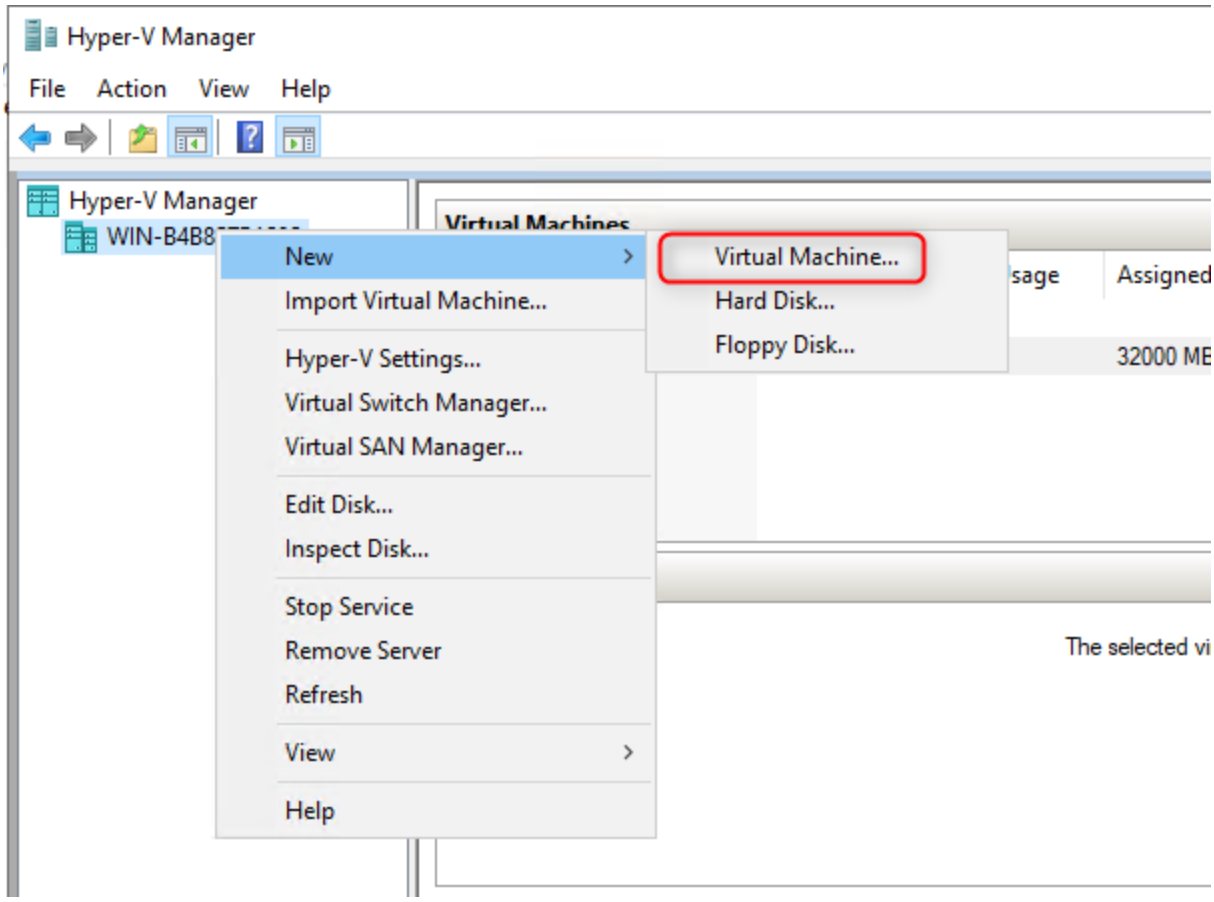
6. Start the Windows PowerShell.
7. Enter the following commands:

```
$portFeature = Get-VMSystemSwitchExtensionPortFeature -FeatureName "Ethernet Switch Port
      Security Settings"

$portFeature.SettingData.MonitorMode = 2

Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName MySwitch -VMSwitchExtensionFeature
      $portFeature
```

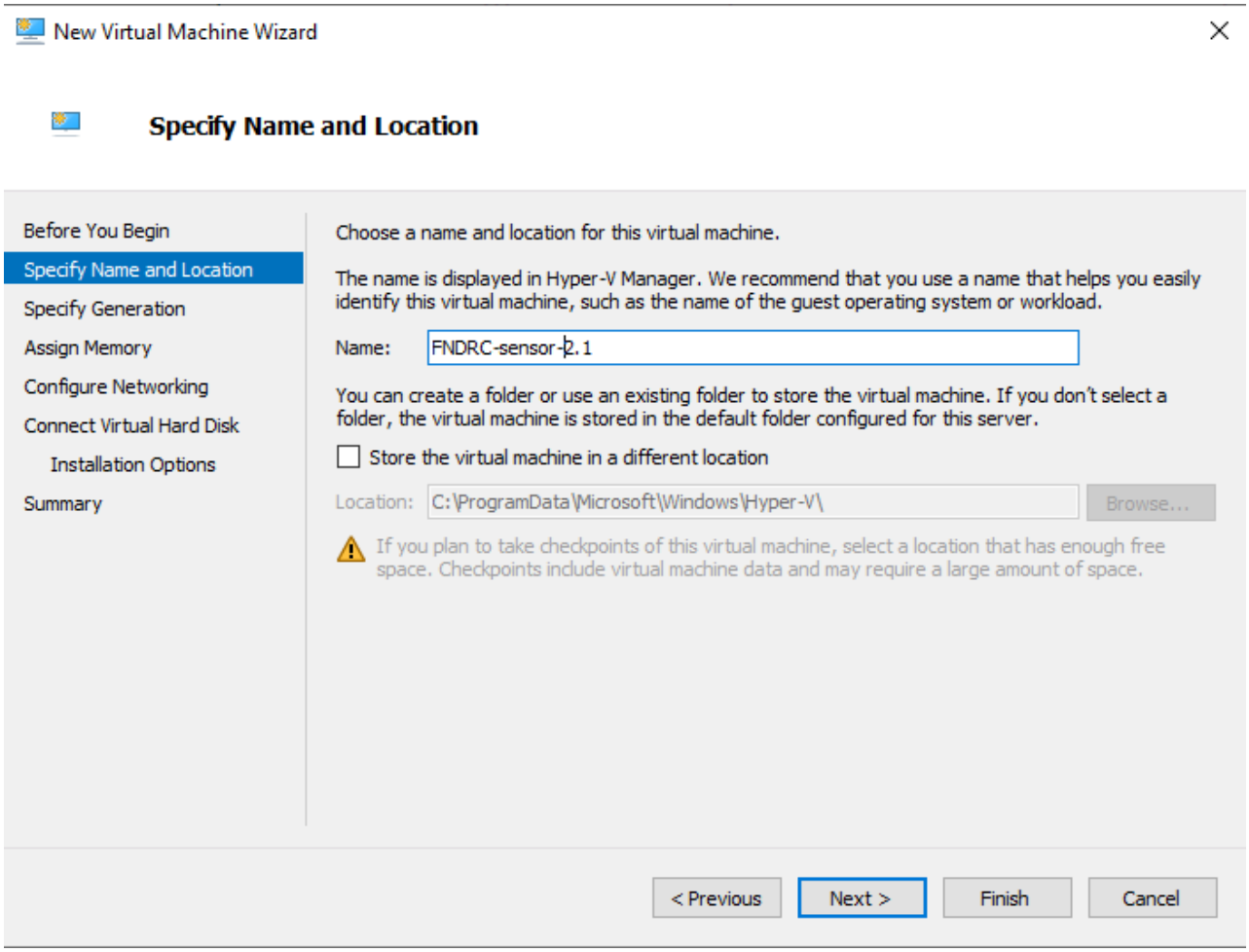
Sensor deployment

To deploy the sensor:

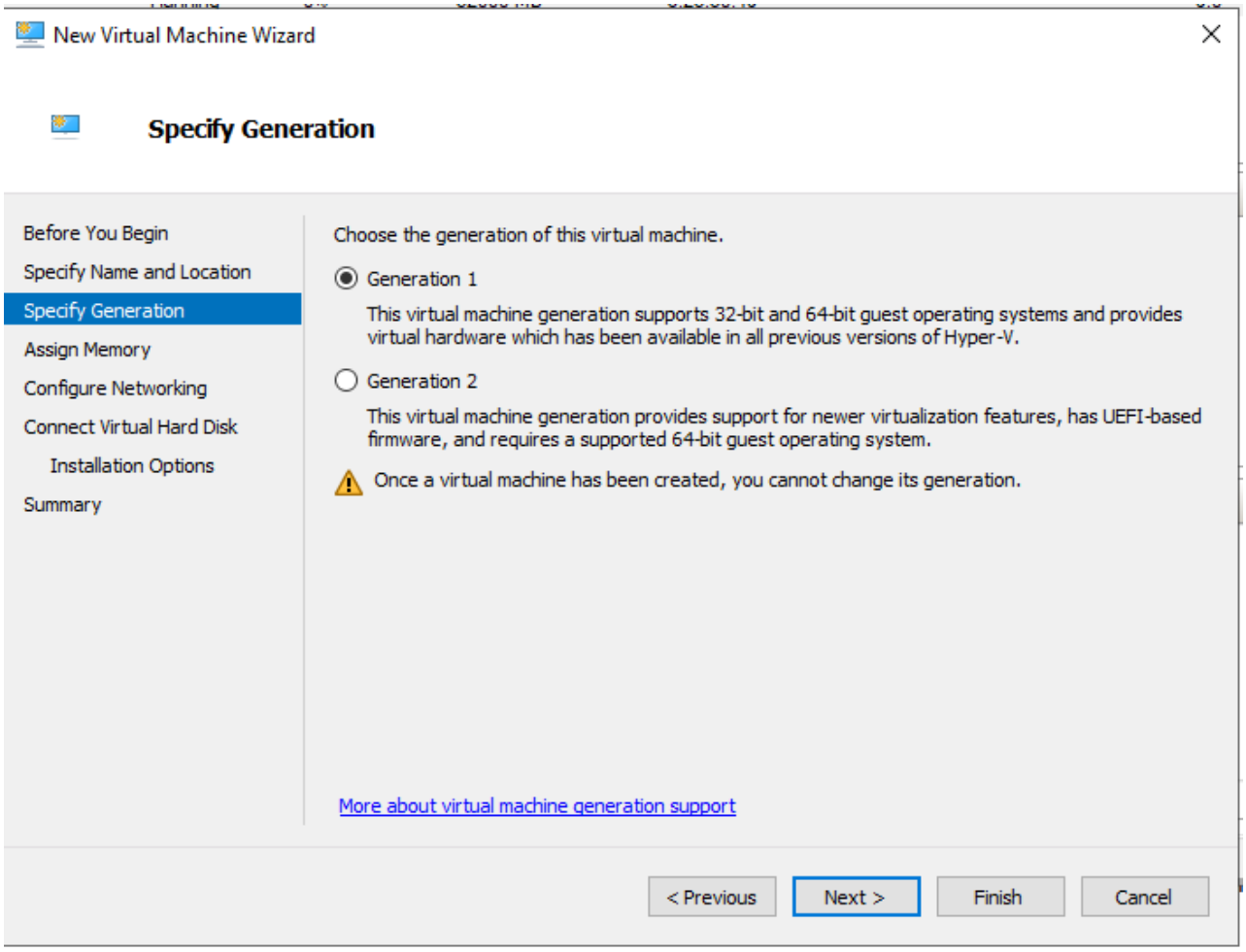
1. Download the sensor ISO image from the link provided in the Portal.
2. On the Hyper-V manager, right-click on your server and select *New -> VirtualMachine...*



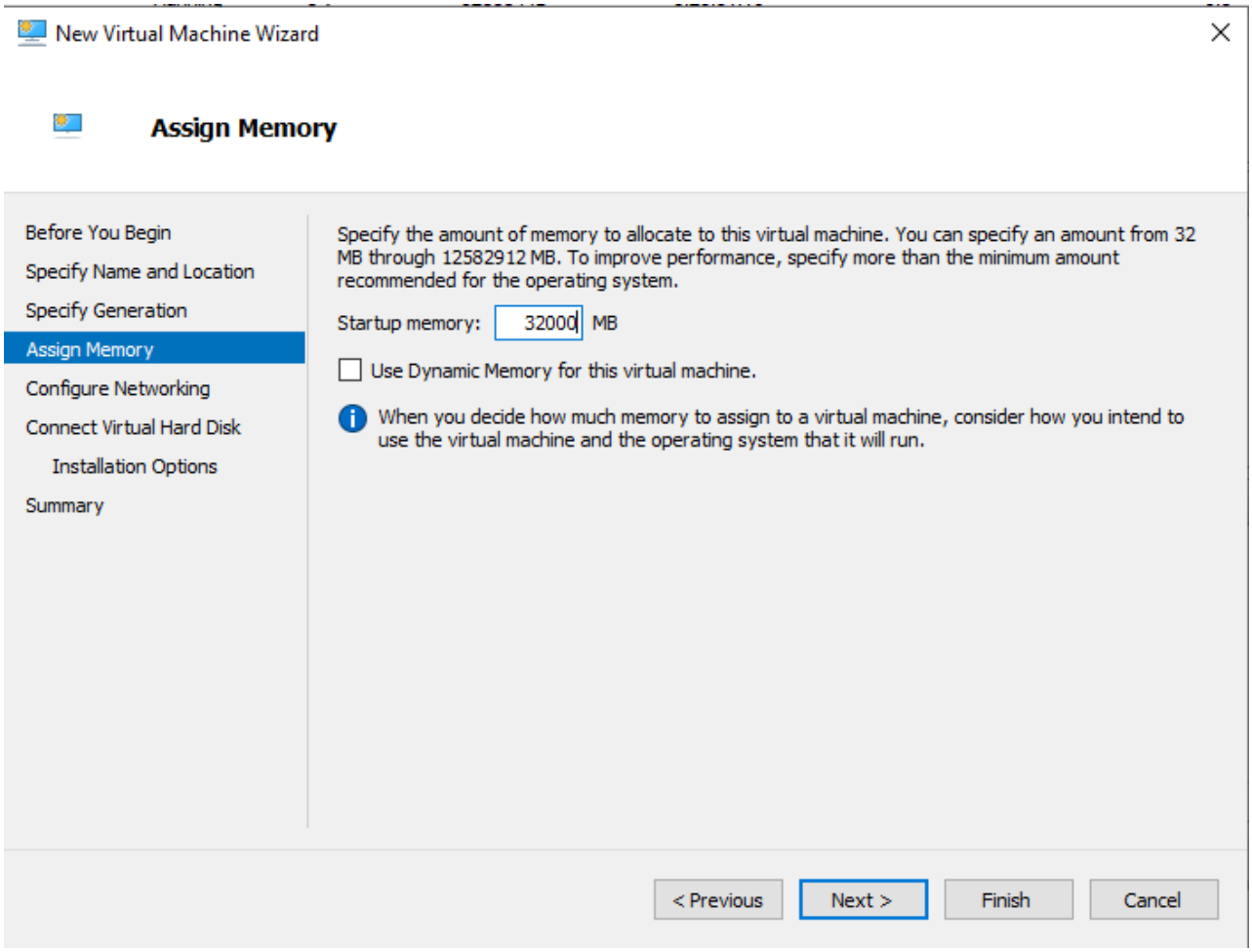
3. Assign a name to the VM and click *Next*.



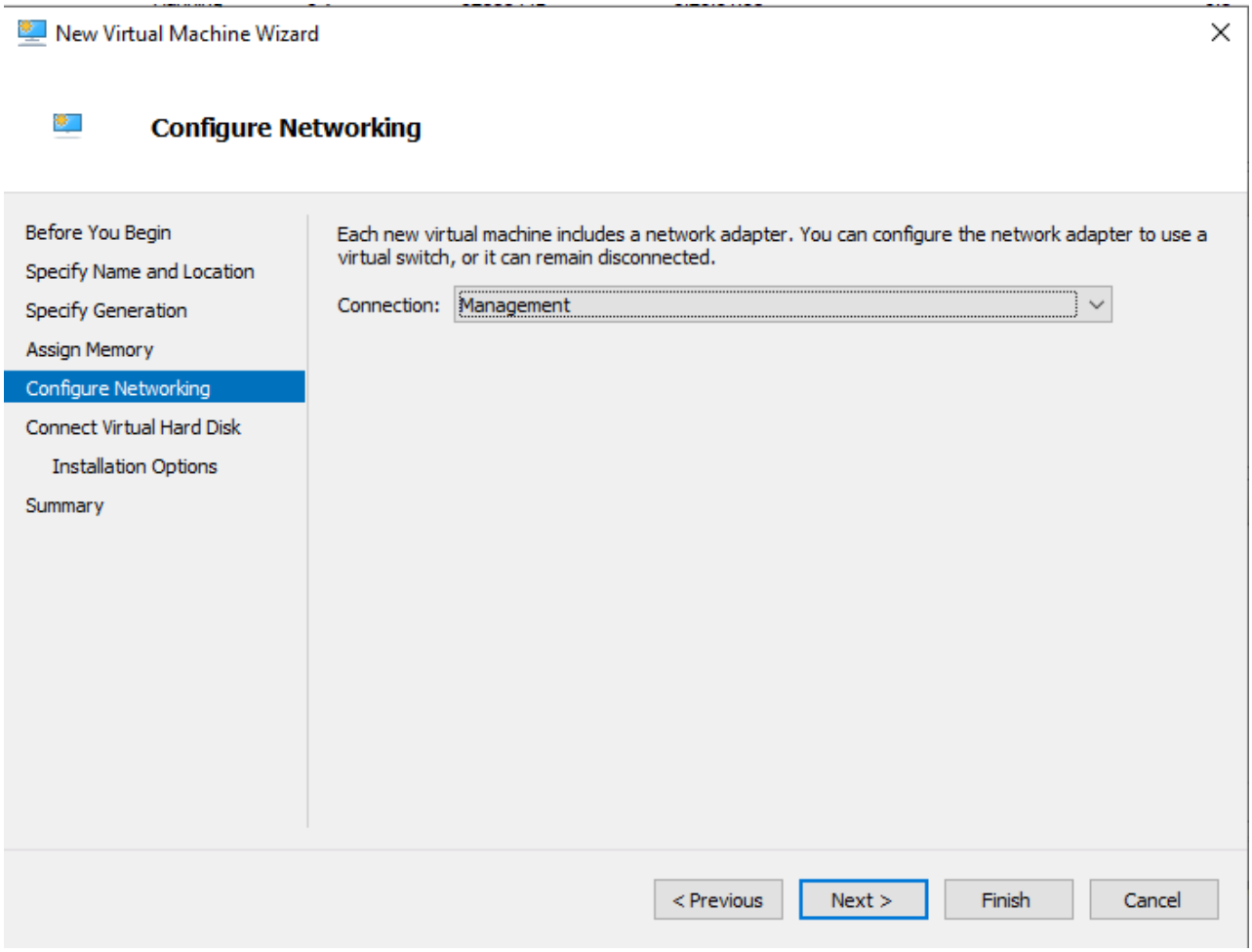
4. Select *Generation 1* and click *Next*.



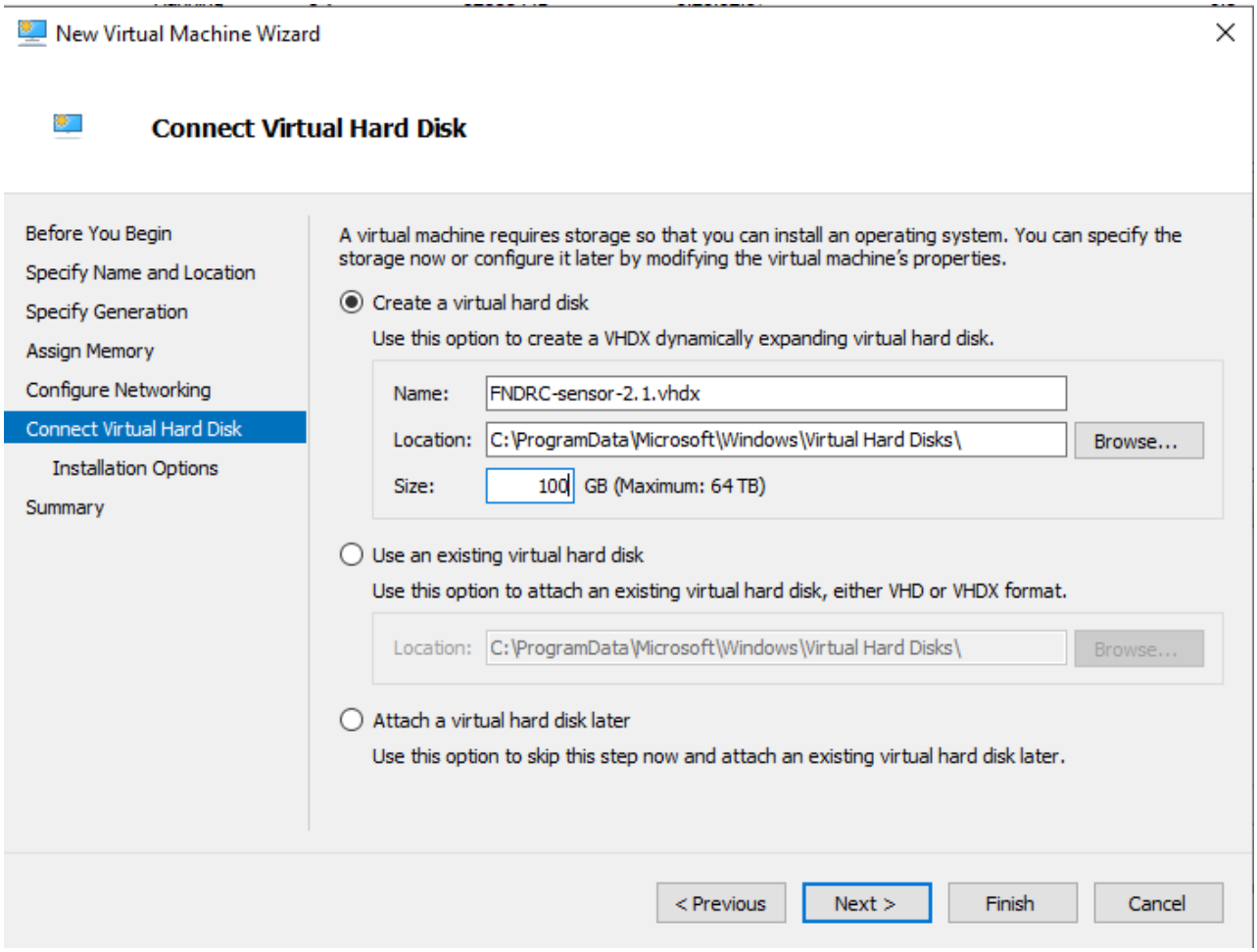
5. Enter the memory size (32000 MB recommended) and click *Next*.



6. For *Connection* select the virtual switch with access to the internet.

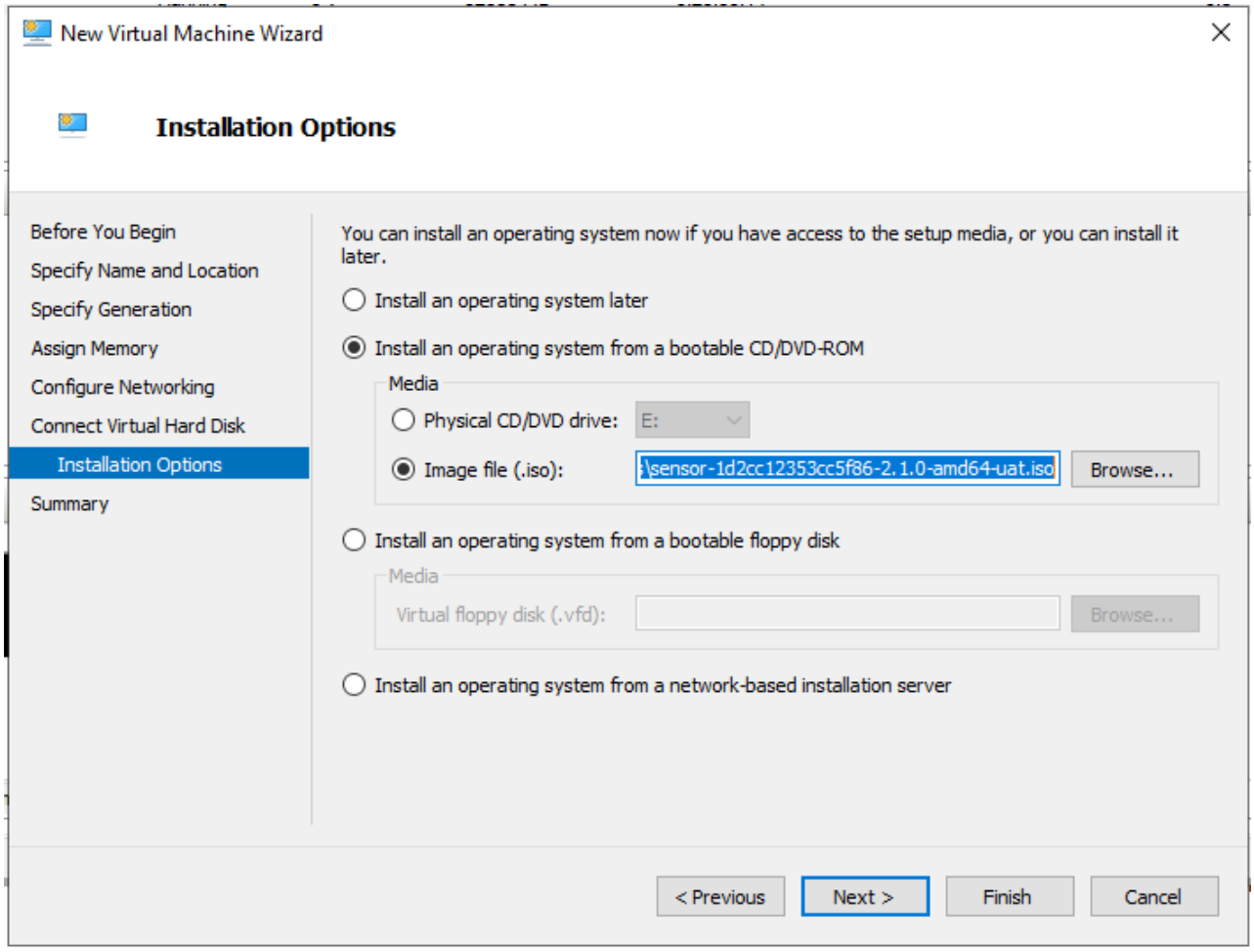


7. Select the desired VHD size (minimum required is 100GB, recommended is 300GB) and click *Next*.

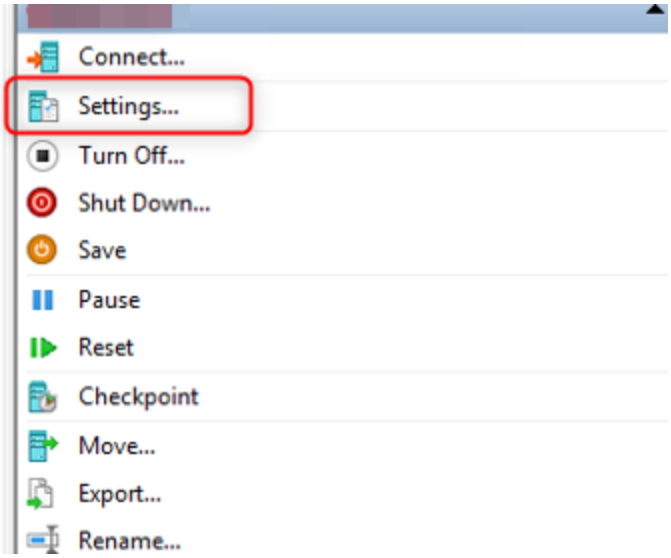


8. Select *Install an operating system from a bootable CD/DVD-ROM*.

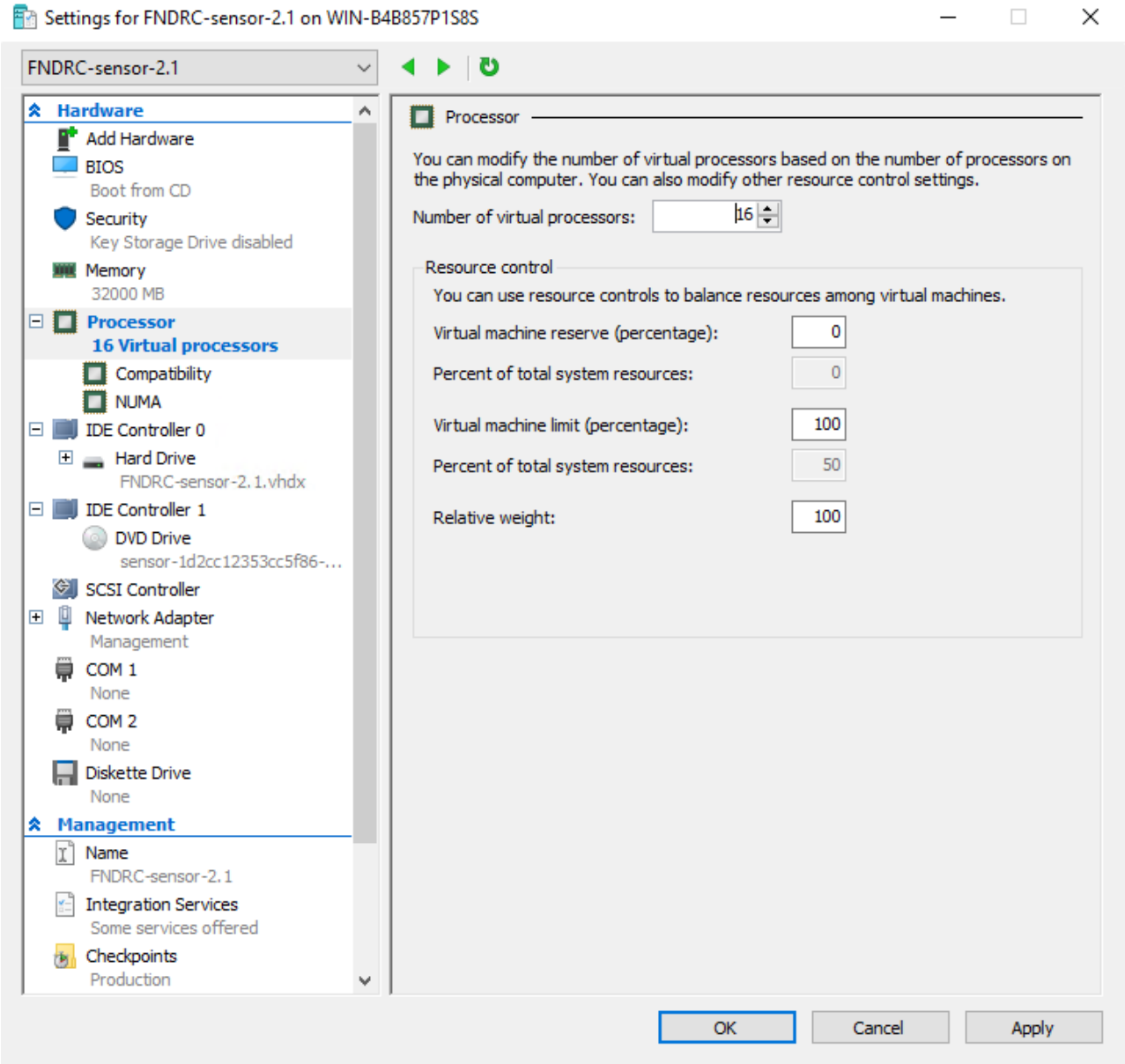
9. Select *image file (.iso)*, click *Browse*, and select the ISO image you downloaded in step 1.



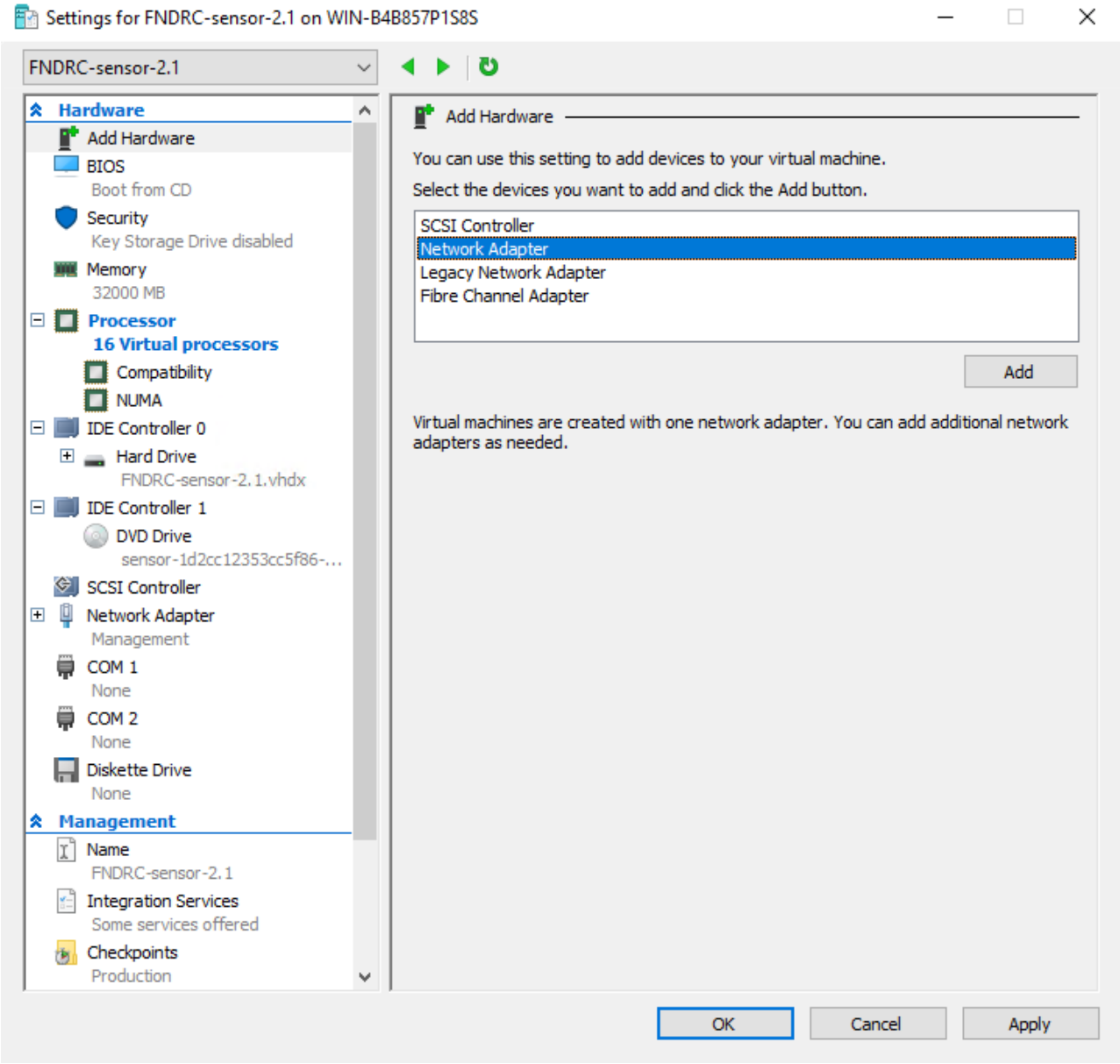
10. Review the configuration and click Finish.
11. Once the Virtual Machine has been created, select *Settings*.



12. Select *Processor* and set the number of virtual processors (recommended is 16 vCPUs).

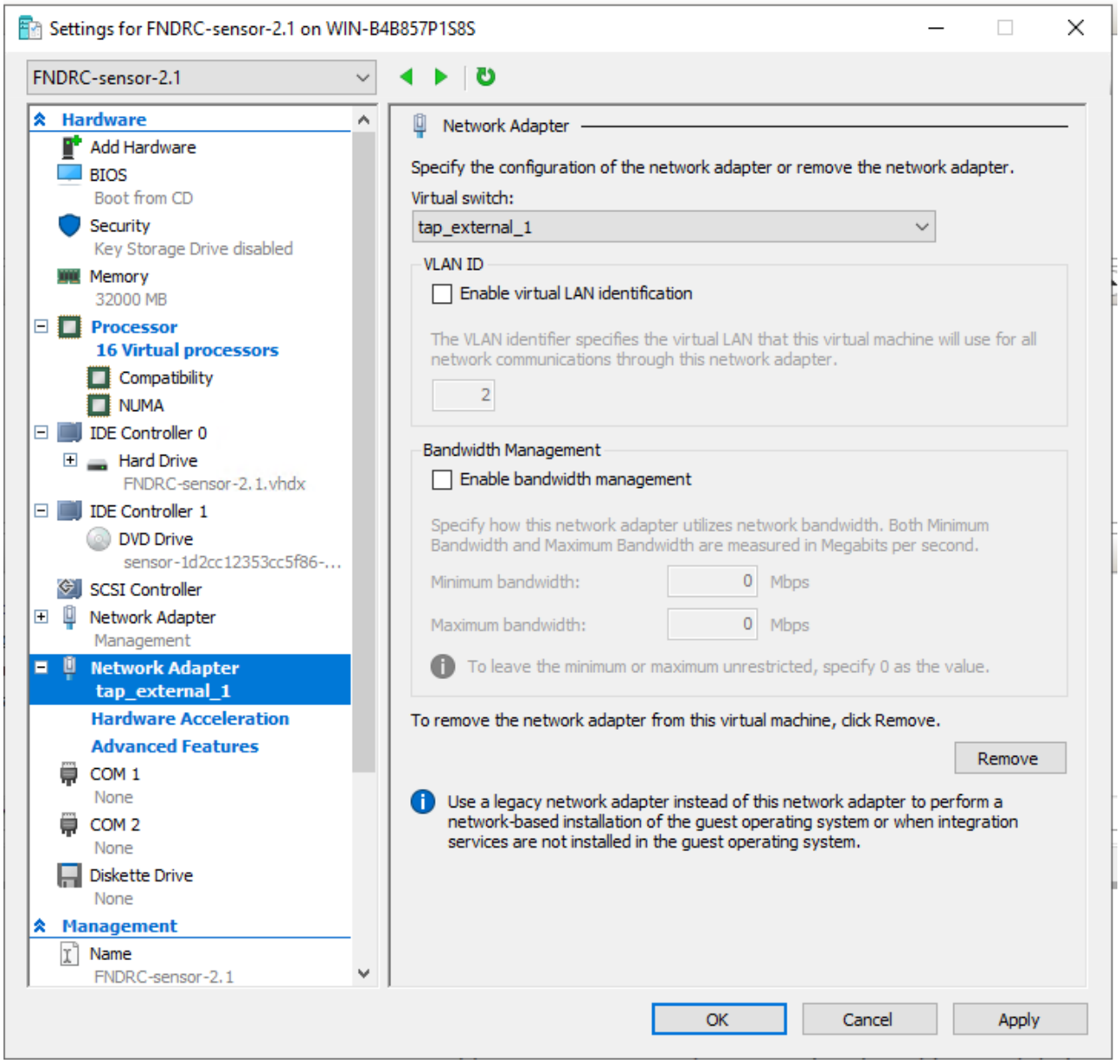


13. Click *Add Hardware*. Select *Network Adapter* and click *Add*.

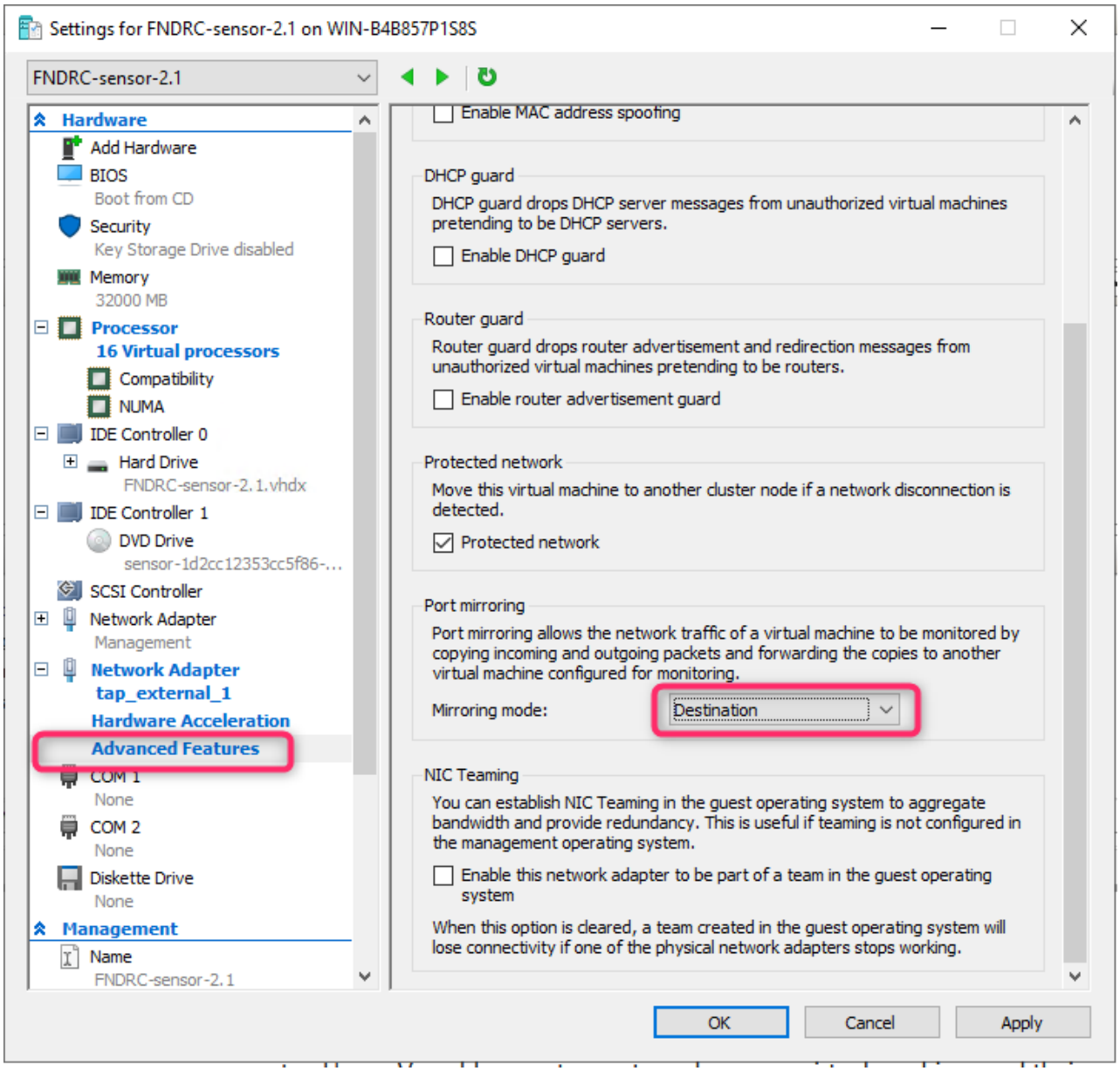


If you wish to forward packets to the sensor using a VXLAN capable vTAP, no additional interface is required, and the sensor's management port will act as the VXLAN tunnel endpoint.

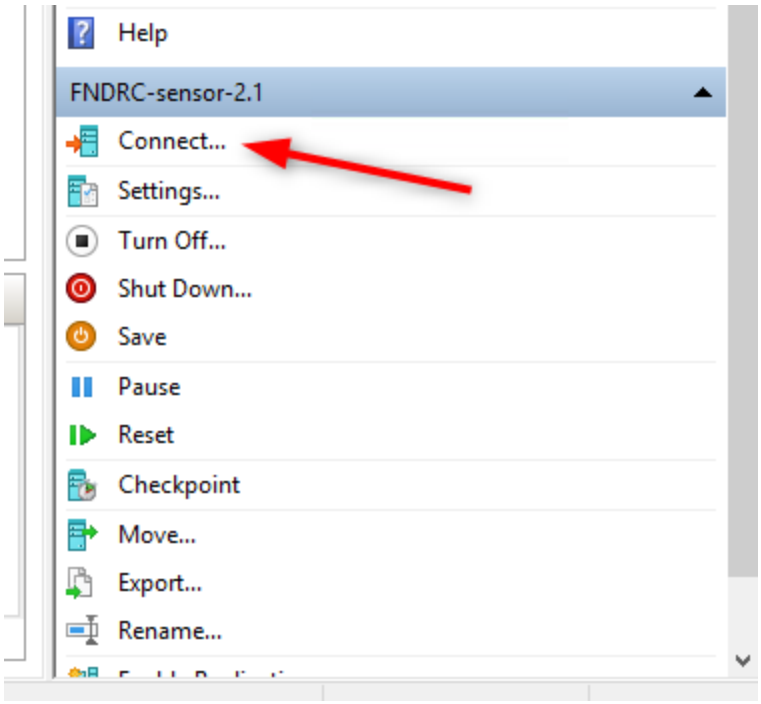
14. Select one of the Virtual switches created earlier.



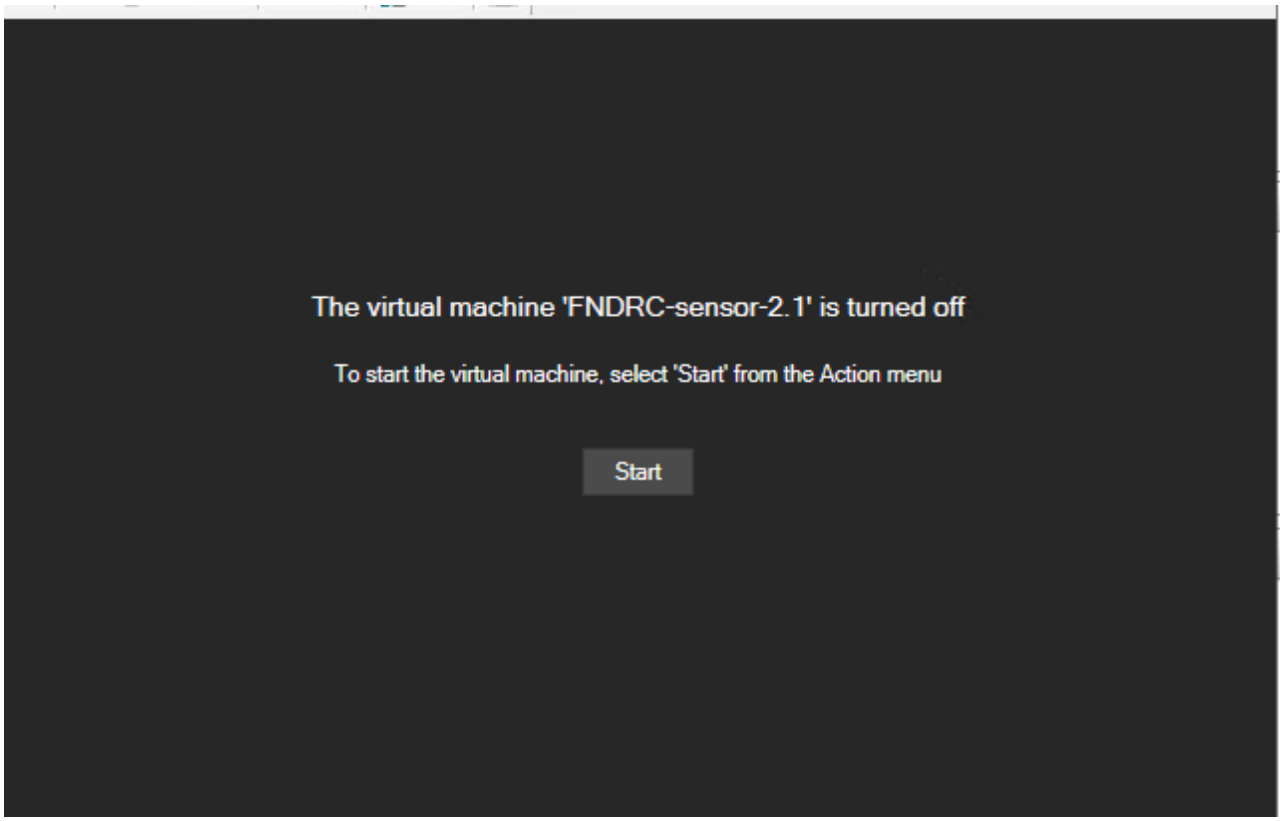
15. Select *Advanced Features* on the network adapter that was added and set the port mirroring as *Destination*. Click *OK*.


Settings for FNDRC-sensor-2.1 on WIN-B4B857P1S8S
FNDRC-sensor-2.1
Hardware
Add Hardware
BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
32000 MB
Processor
16 Virtual processors
Compatibility
NUMA
IDE Controller 0
Hard Drive
FNDRC-sensor-2.1.vhdx
IDE Controller 1
DVD Drive
sensor-1d2cc12353cc5f86-...
SCSI Controller
Network Adapter
Management
Network Adapter
tap_external_1
Hardware Acceleration
Advanced Features
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
FNDRC-sensor-2.1
Enable MAC address spoofing
DHCP guard
DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.
Enable DHCP guard
Router guard
Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.
Enable router advertisement guard
Protected network
Move this virtual machine to another cluster node if a network disconnection is detected.
Protected network
Port mirroring
Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.
Mirroring mode:
Destination
NIC Teaming
You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.
Enable this network adapter to be part of a team in the guest operating system
When this option is cleared, a team created in the guest operating system will lose connectivity if one of the physical network adapters stops working.
OK
Cancel
Apply

16. Under the sensor VM, click *Connect* ....



17. Right-click the VM and click *Start*.



18. Follow progress on the console until the VM automatically reboots and you are presented with the login prompt.

Sensor provisioning

Obtaining the provisioning code

To provision the sensor, you will need a provisioning code from the FortiNDR Cloud portal (or your designated TSM).

To obtain the provisioning code from the portal:

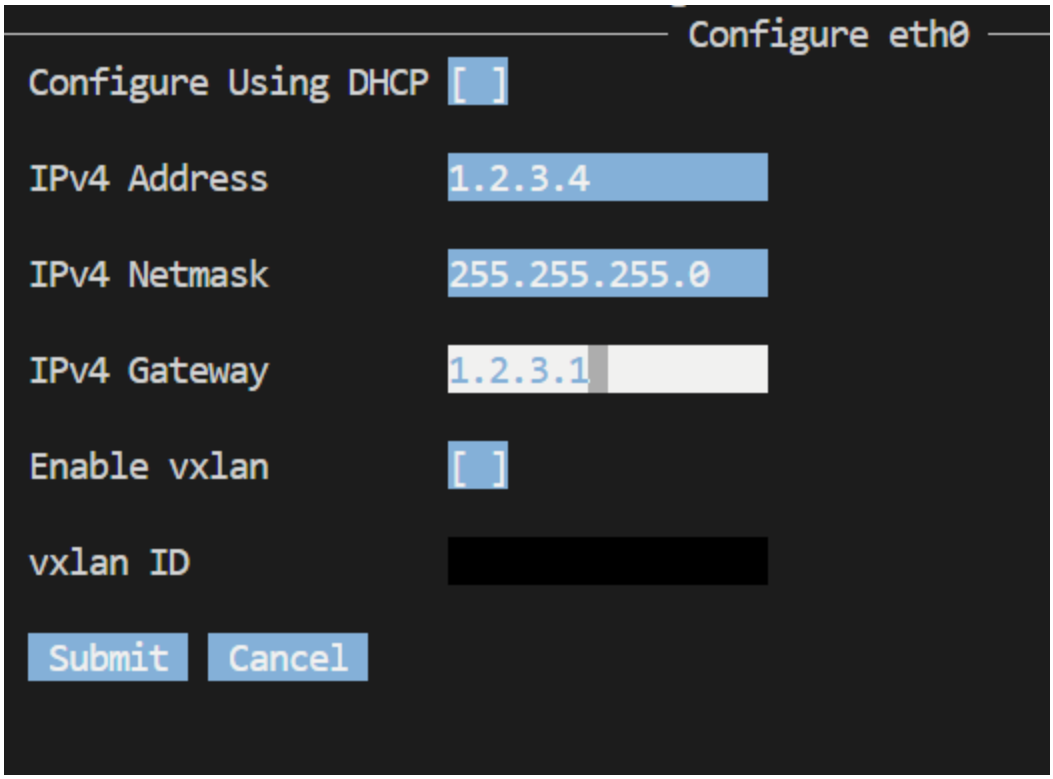
1. Go to your account in the FortiNDR cloud portal and click on the gear icon and select *Sensors*.
2. Go to *Actions > Provision Sensor*.
3. Copy the code. The code is valid for 24 hrs.

Sensor provisioning

To provision the sensor:

1. Log into the sensor configuration console with username: `config` and password: `configure`.
2. Change the password when prompted, and log in again with the new password.
3. By default, FortiNDR cloud sensor is configured to obtain IP address from a DHCP server. If there is no DHCP in the network connected to the sensor management port, static IP can be configure by:
   a. Go to *Set Management Interface*.
   b. Selecting the interface marked with *(configured)*.
   c. Entering the IP information.
4. If packets are forwarded to the Sensor by means of a VXLAN tunnel, you can enable the VXLAN and provide the appropriate VID.

5. Review the configuration and click *Submit*.

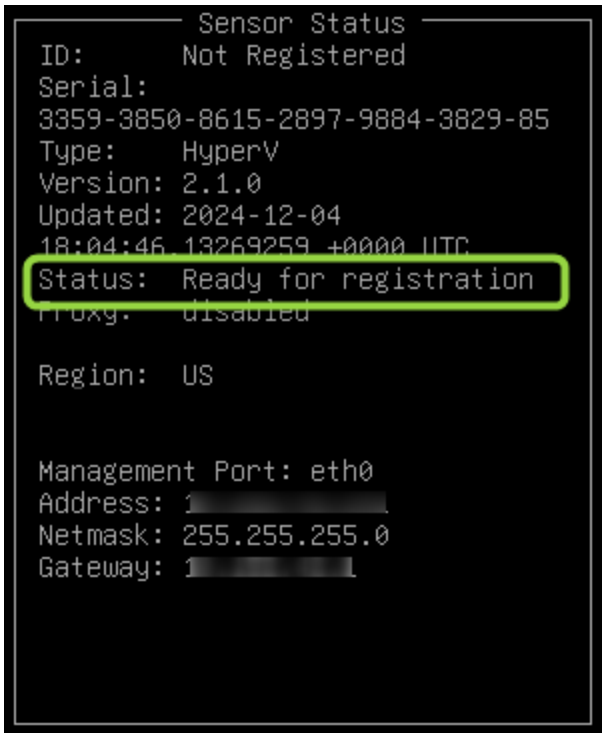


6. If there is a requirement for proxy access to reach the public network, follow the steps below, otherwise go to step 7.

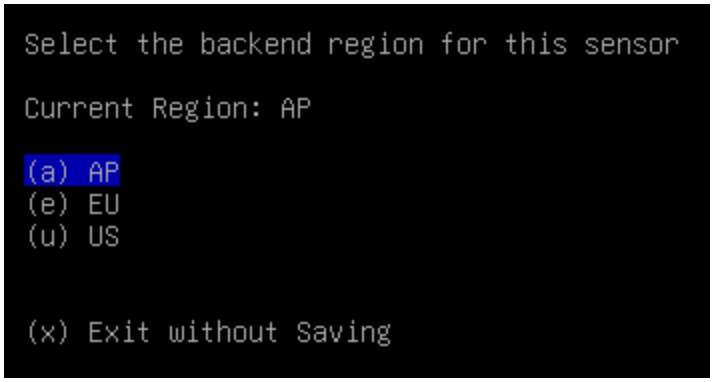
> IMPORTANT!
> If your are provisioning the sensor for the EU region follow the steps in Configuring the sensor connection through proxy before moving to step 7.

7. Obtain the provisioning code from your account page on the portal, or your Technical Success Manager.

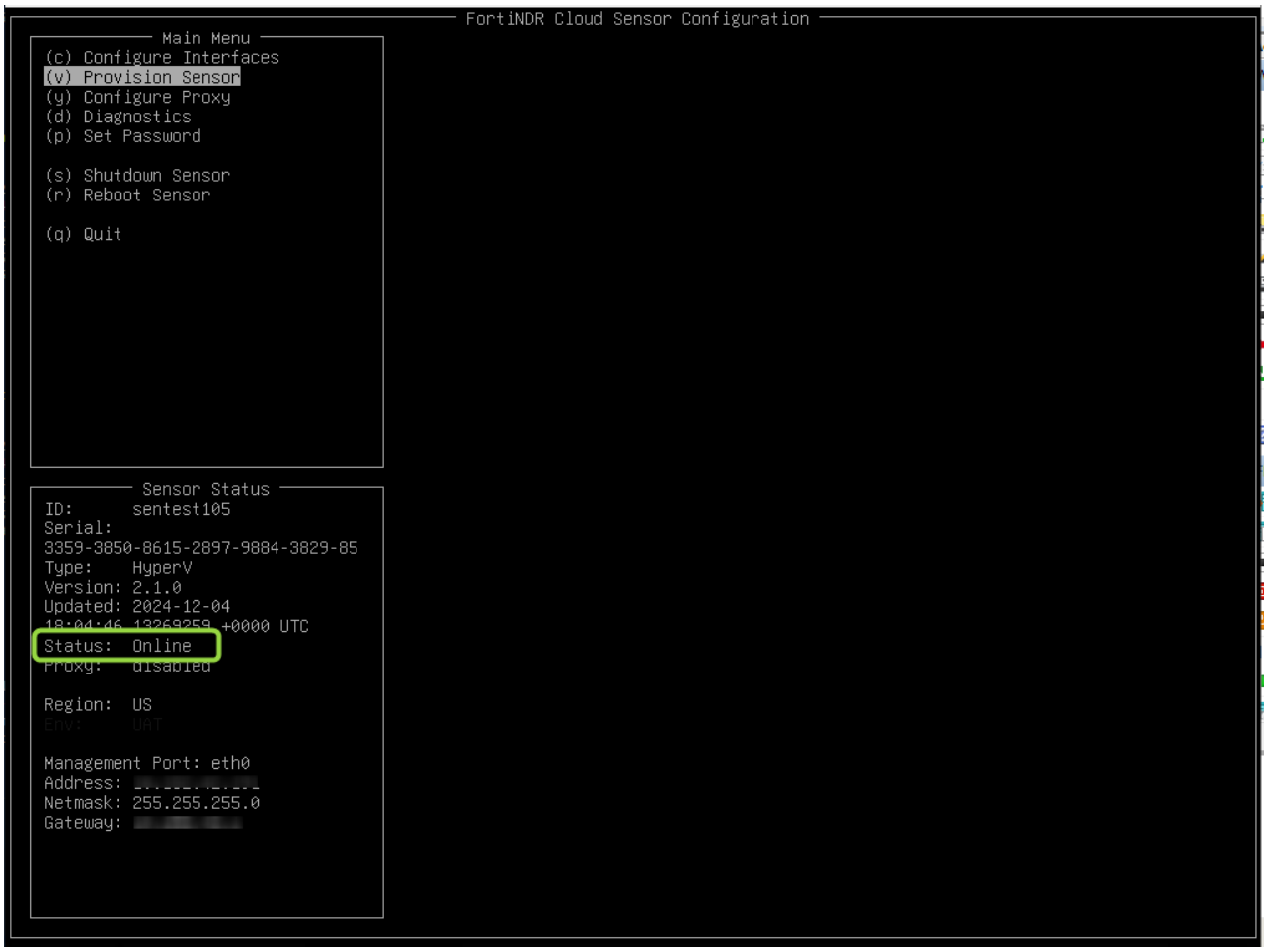
8. On the Sensor's configuration page, ensure the sensor status is *Ready for registration*.



9. Select *Provision Sensor* (or press v).
10. Select your *Current Region* (*EU* , *US* or *AP*).



11. Enter the provisioning code obtained from Step 5, then select *Provision Sensor*.
12. Allow a few minutes for sensor status to change to *Online* in the *Sensor Status* pane. Once the status has changed, the sensor has been provisioned and is analyzing the packets.



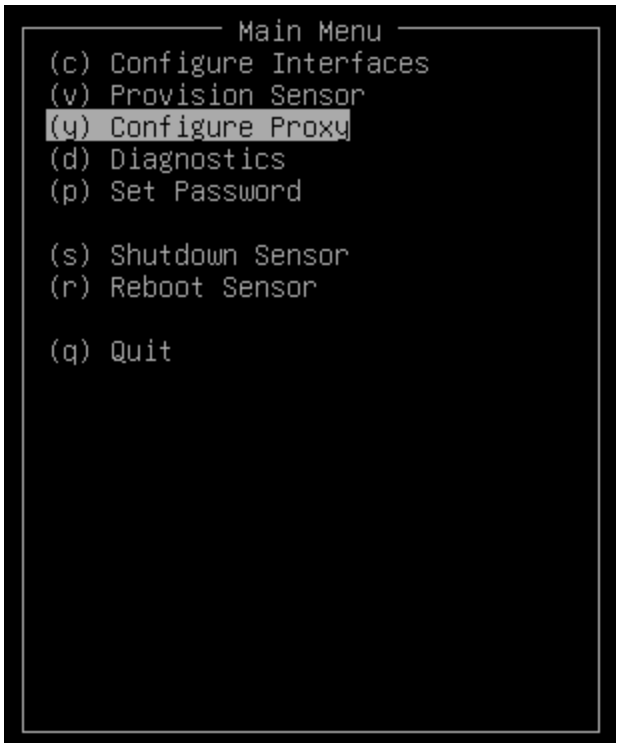
Configuring the sensor connection through proxy

If you plan to provision the sensor in the EU region, you will need to change the region to EU, before configuring the proxy. You can change the region by navigating to *provision sensor*, select EU and wait until the region has changed.

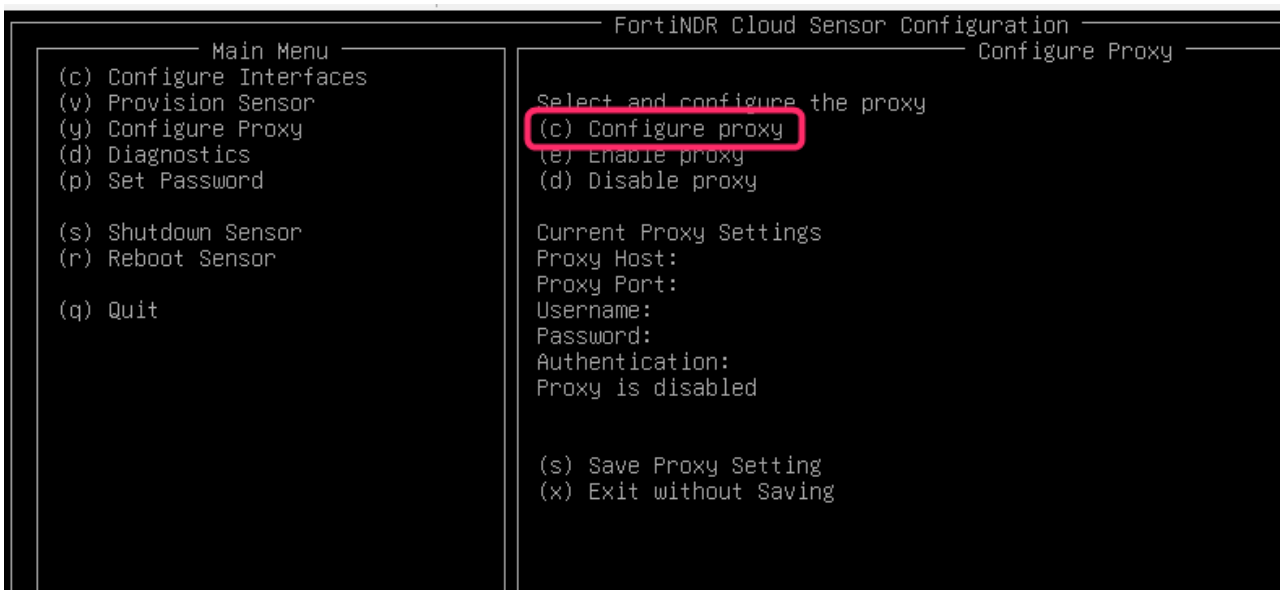
To configure the connection through proxy:

1. Make sure that your proxy has been configured to allow access from the sensor. For sample configuration of FortiProxy please, seeAppendix: FortiProxy configuration example on page 32 .

2. In the *Main Menu* go to *Configure proxy* (or type Y).

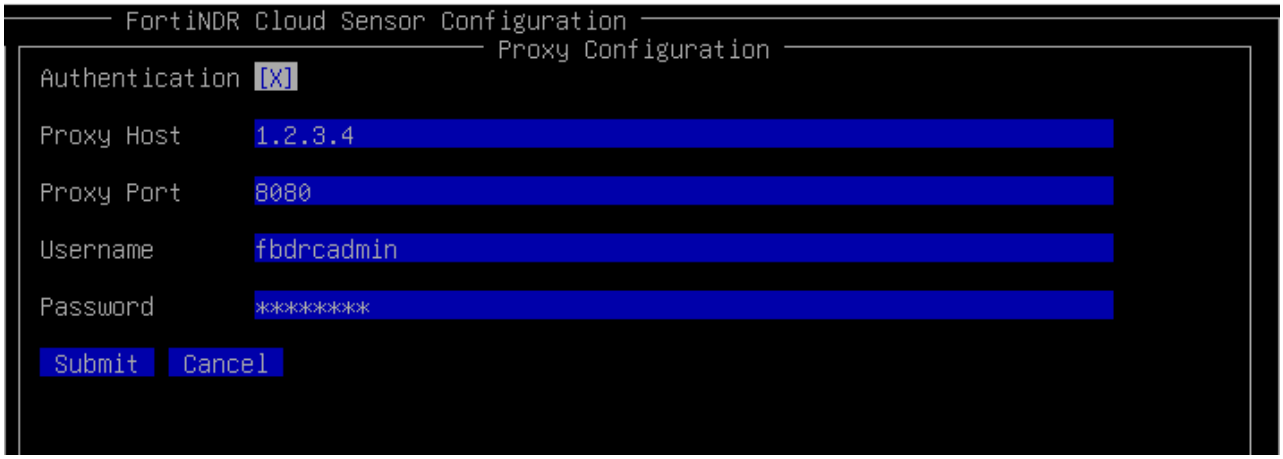


3. Select *configure proxy* (or type c).



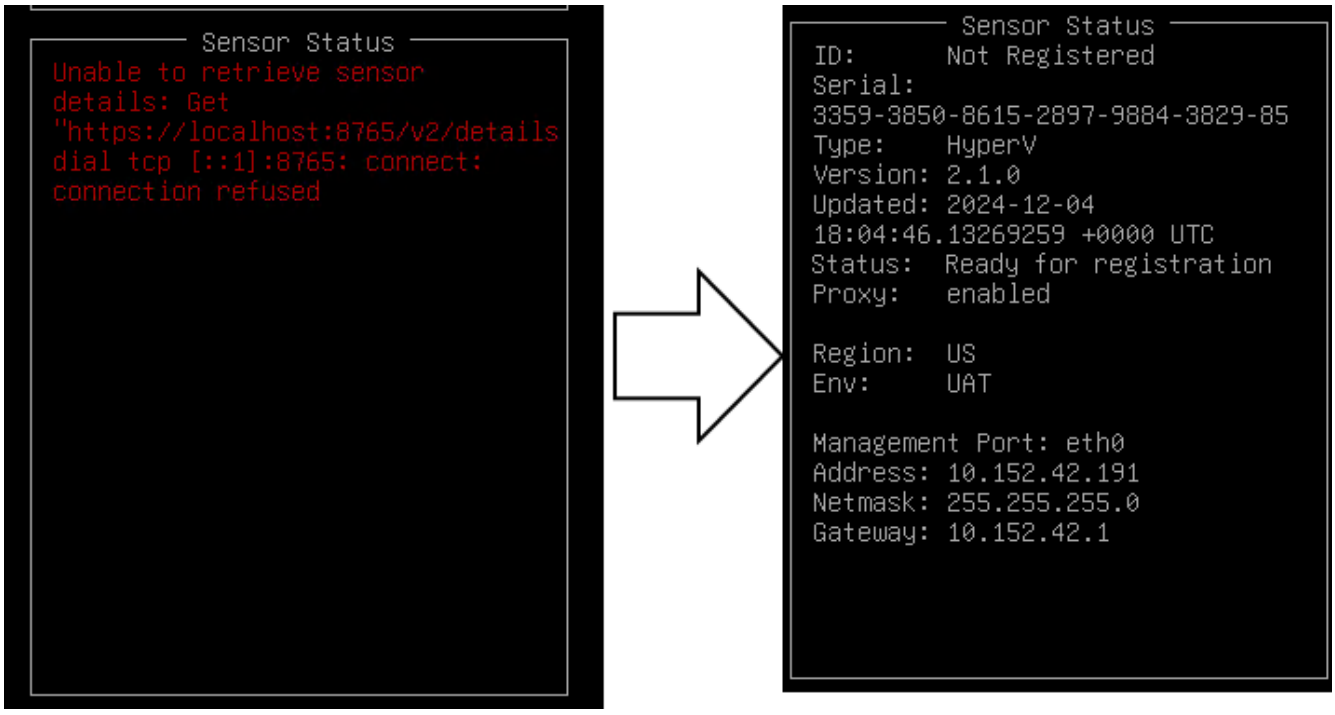
4. FortiNDR cloud sensor currently supports basic authentication. If password authentication is required for the proxy, enable *Authentication*, otherwise leave it as unselected.

5. Fill in the required information and click *Submit*.



6. Select *Enable proxy* (or type e), press enter and wait for the sensor service to be restarted.

You might see the message below in the status pane, which means the service is not available yet, continue waiting until you see the sensor status is populated with sensor status



If the proxy is shown as *Enabled* in the status pane and sensor status is stuck at *Initializing* but shows *Ready for registration* when the proxy is disabled, it is an indication that sensor cannot reach the FortiNDR Cloud backend in the AWS cloud in presence of the proxy. Please refer to your proxy's logs for further troubleshooting.

Optional features

Feature	Desctiption
Proxy	FortiNDR Cloud Sensor supports communication through a proxy, to see an example configuration, please refer to Sensor provisioning on page 25 .
Netflow	FortiNDR Cloud sensor can act as a Netflow collector, Netflow records will be logged and analyzed for threat detection by the FortiNDR cloud solution. To be able to configure Netflow record collection on the OCI sensor, you will need to add an additional interface to the sensor VM. For more information on the Netflow record collection, please refer to the Netflow topic in the *FortiNDR User Guide*.
ERSPAN	Starting with version 2.4.0, FortiNDR sensors support ERSPAN as a method for forwarding packets to the sensor for analysis. Similar to NetFlow, ERSPAN uses the collector port to receive ERSPAN packets. For additional information on ERSPAN, see the ERSPAN section in the *FortiNDR Cloud User Guide*.

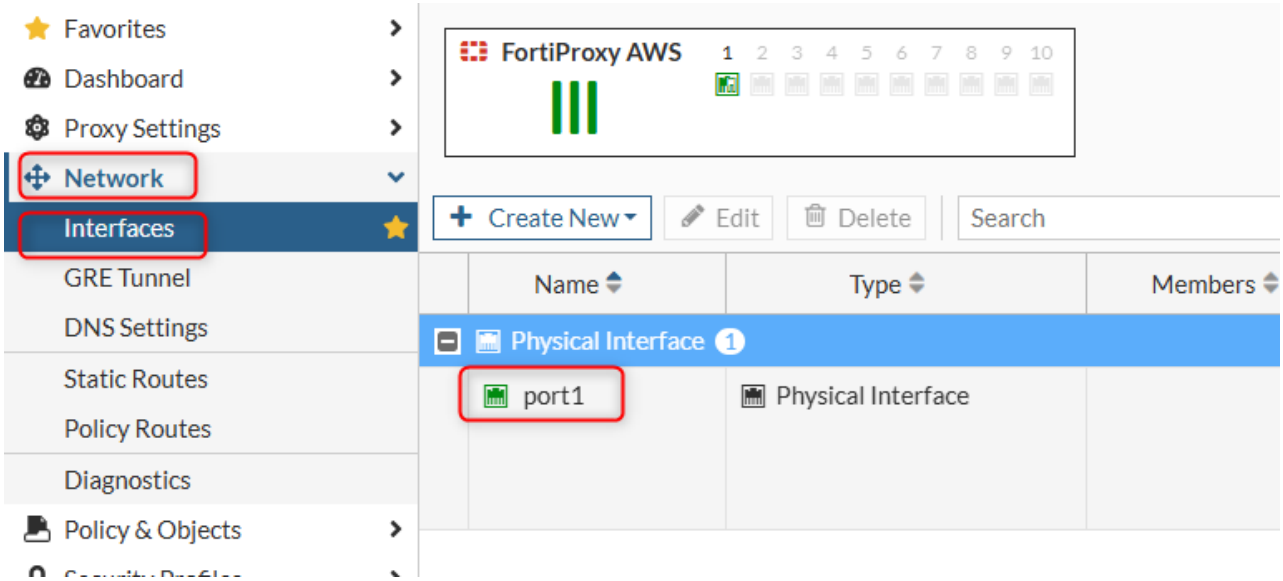
Appendix: FortiProxy configuration example

Below is an example of FortiProxy configuration for FortiNDR Cloud sensor access through proxy with and without authentication.

- For access without authentication on page 32
- For access with authentication on page 38

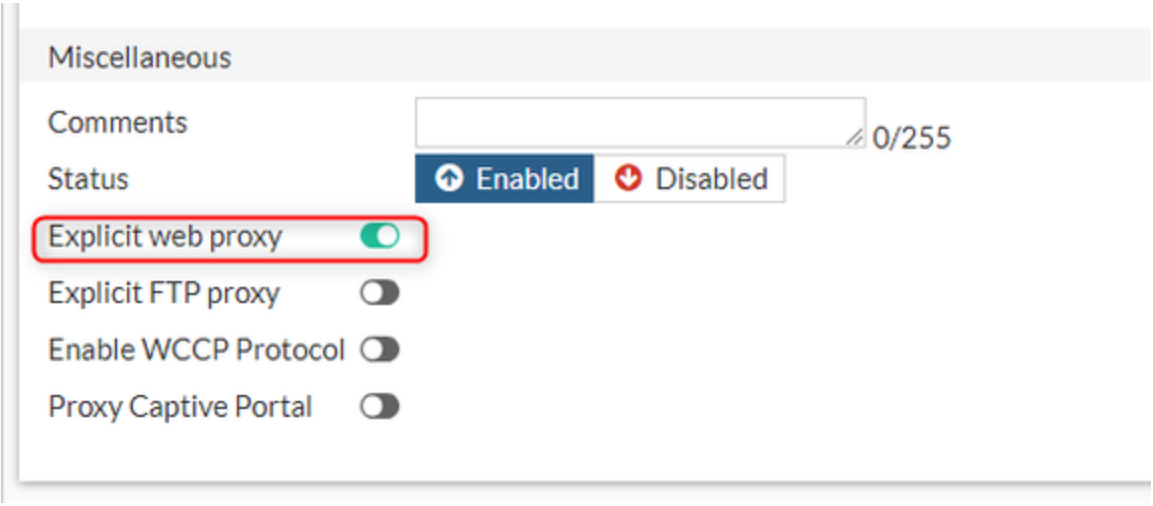
For access without authentication

1. Go to *Proxy Settings* > *Explicit Proxy*.
2. Click *web-proxy* and select *Edit*.
3. For *Physical Interface* select *port 1* (or any other physical port that is specific to your environment) .
4. Keep the rest of the default settings and click *OK*.
5. Go to *Network* > *Interfaces*.
6. Highlight the designated port and click *Edit*.



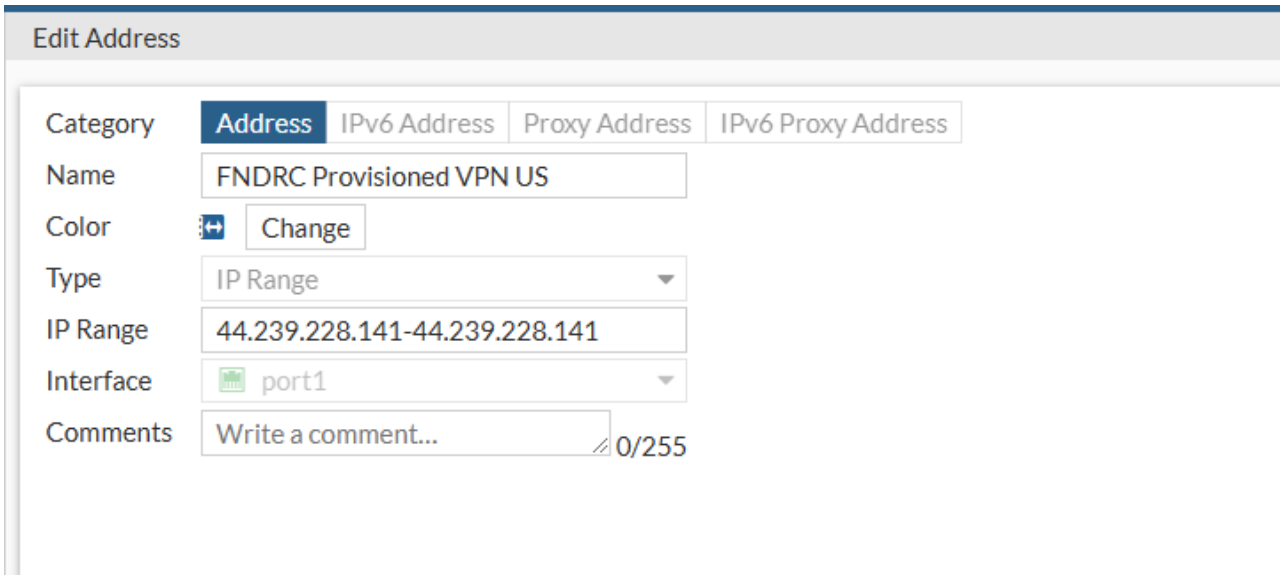
7. If required, change the default HTTP and HTTPS port.

8. Enable *Explicit web proxy* and click *OK*.



9. Go to *Policy and Objects > Addresses*.
10. Add the VPN and S3 upload end point IP addresses as shown below:

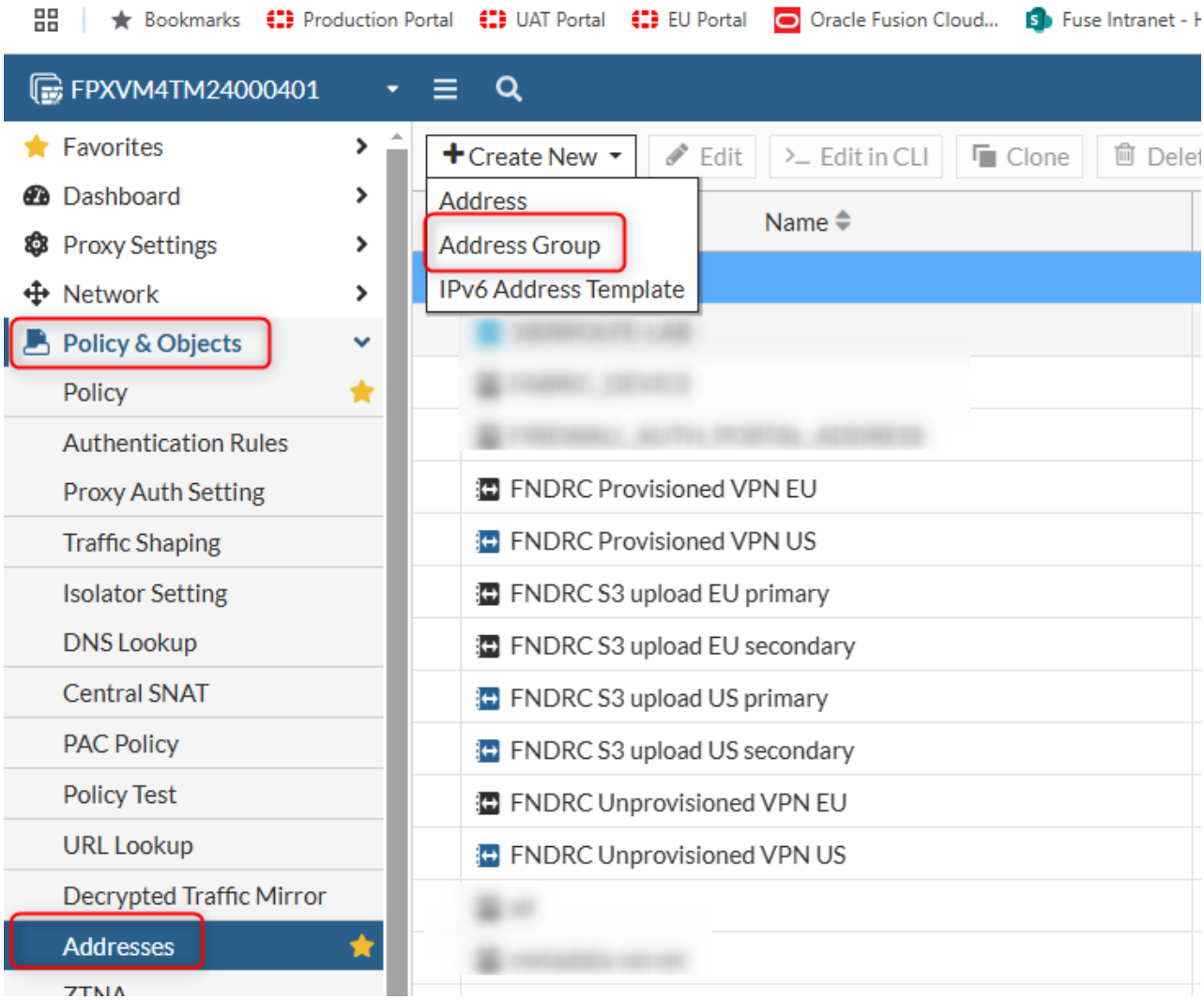
North America	52.36.236.168 (Unprovisioned VPN US) 44.239.228.141 (Provisioned VPN US) 138.43.114.16 (S3 endpoint Primary US) 138.43.114.141 [S3 endpoint backup US]
EU region	18.153.171.115 (Unprovisioned VPN EU) 3.124.46.55 (Provisioned VPN EU) 3.72.240.234 (S3 endpoint Primary EU) 3.123.116.122 [S3 endpoint backup EU]
APAC region	47.131.38.17 (Unprovisioned VPN AP) 13.251.235.20 (Provisioned VPN AP) 13.215.106.143 (S3 endpoint Primary AP) 13.251.181.190 [S3 endpoint backup AP]



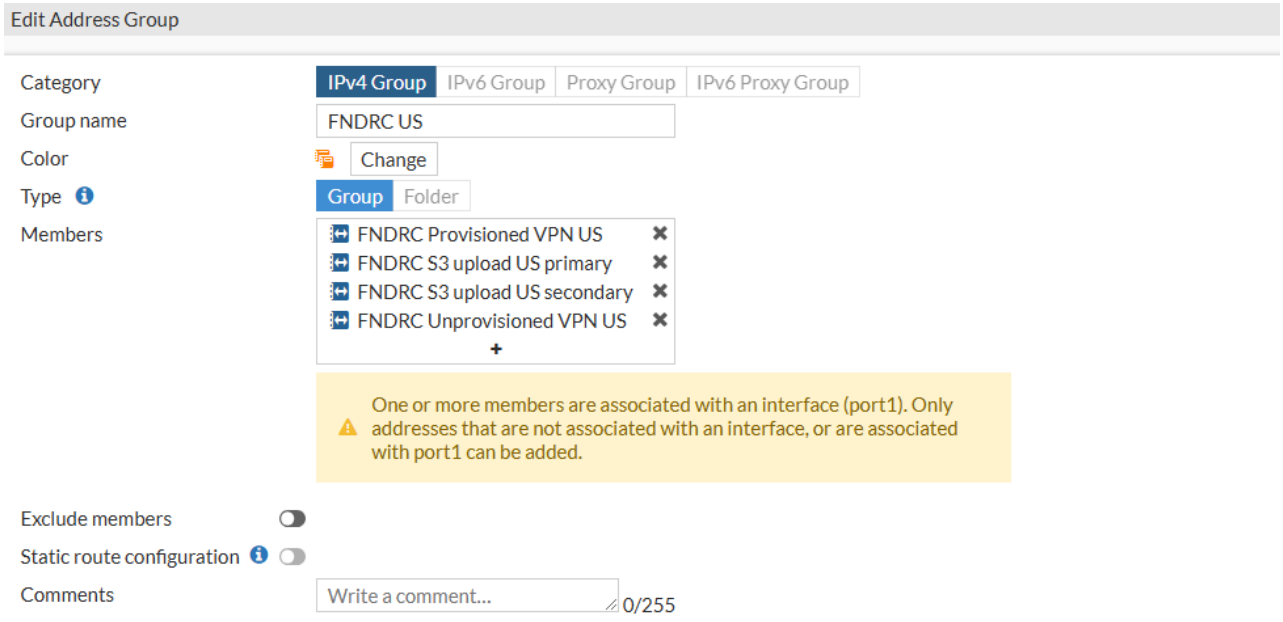
11. If the sensor is to be provisioned in EU or APAC region, create endpoint IP addresses designated for EU or APAC region respectively.

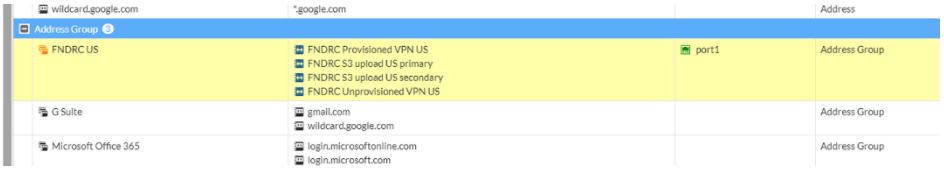
Name	IP Address	Port
FNDRC Provisioned VPN AP	13.251.235.20	port1
FNDRC Provisioned VPN EU	3.124.46.55	port1
FNDRC Provisioned VPN US	44.239.228.141	port1
FNDRC S3 endpoint Primary AP	13.215.106.143	port1
FNDRC S3 endpoint Primary EU	3.72.240.234	port1
FNDRC S3 endpoint Primary US	138.43.114.16	port1
FNDRC S3 endpoint backup AP	13.251.181.190	port1
FNDRC S3 endpoint backup EU	3.123.116.122	port1
FNDRC S3 endpoint backup US	138.43.114.141	port1
FNDRC Unprovisioned VPN AP	47.131.38.17	port1
FNDRC Unprovisioned VPN EU	18.153.171.115	port1
FNDRC Unprovisioned VPN US	52.36.236.168	port1

12. Go to *Policy and Objects* > *Addresses* > *Create New* > *Address group*.



13. Give the group a name, then add the addresses created above to the group, and click *OK*.





14. Click the CLI icon (**>_**) at the upper-right side of the page to open the CLI console.
15. Copy and paste the CLI below into the console. Close the console when done.

```
config system dns-database
    edit "my-dns"
        set domain "vpce.amazonaws.com"
        config dns-entry
            edit 1
                set hostname "icebrg-preprod-sensor-ingest.bucket.vpce-0e8d47840a7ffbf5f-
hedlogmh.s3.us-west-2.vpce.amazonaws.com"
                set ip 138.43.114.141
            next
            edit 2
                set hostname "icebrg-preprod-sensor-ingest.bucket.vpce-0e8d47840a7ffbf5f-
hedlogmh.s3.us-west-2.vpce.amazonaws.com"
                set ip 138.43.114.16
            next
        end
    next
end
```

If the sensor(s) are to be provisioned in the EU region the configuration will look like below:

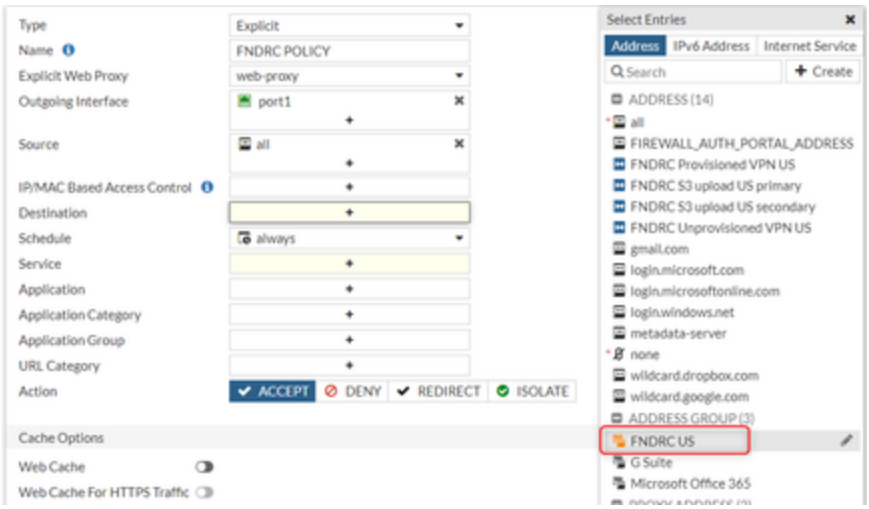
```
config system dns-database
    edit "my-dns-FNDRC-EU"
        set domain "vpce.amazonaws.com"
        config dns-entry
            edit 1
                set hostname "fortindr-cloud-eu-sensor-etl-production-sensor-
ingest.bucket.vpce-04cca23d7dbdf8626-x2c1jp2i.s3.eu-central-1.vpce.amazonaws.com"
                set ip 3.72.240.234
            next
            edit 2
                set hostname "fortindr-cloud-eu-sensor-etl-production-sensor-
ingest.bucket.vpce-04cca23d7dbdf8626-x2c1jp2i.s3.eu-central-1.vpce.amazonaws.com"
                set ip 3.123.116.122
            next
        end
    next
end
```

If the sensor(s) are to be provisioned in the APAC region the configuration will look like below:

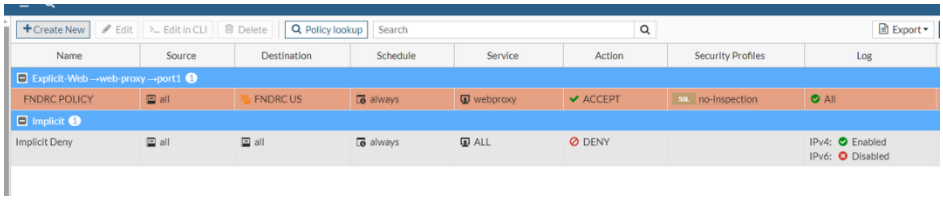
```
config system dns-database edit
    "my-dns-FNDRC-AP"
        set domain "vpce.amazonaws.com"
        config dns-entry
            edit 1
                set hostname "fortindr-cloud-ap-sensor-etl-production-sensor-
ingest.bucket.vpce-0ef3cbdf9c3b9627e-3tjxjoj7.s3.ap-southeast-
1.vpce.amazonaws.com"
                set ip 13.215.106.143
            next edit 2
                set hostname "fortindr-cloud-ap-sensor-etl-production-sensor-
ingest.bucket.vpce-0ef3cbdf9c3b9627e-3tjxjoj7.s3.ap-southeast-
1.vpce.amazonaws.com"
                set ip 13.251.181.190
            next
        end
    next
end
```

16. Go to *Policy and Objects > Policy*. Configure the policy.

Type	Select *Explicit*
Name	Give the policy a name.
Outgoing interface	Select the same as the addresses added.
Source	Select the sensor address (needs to be added as an address) or choose All for any source.
Destination	Select the address group that was created earlier.
Service	Select *webproxy*.



17. Make sure *SSL/SSH Inspection* is set to *no-inspection*.
18. Click *OK*.



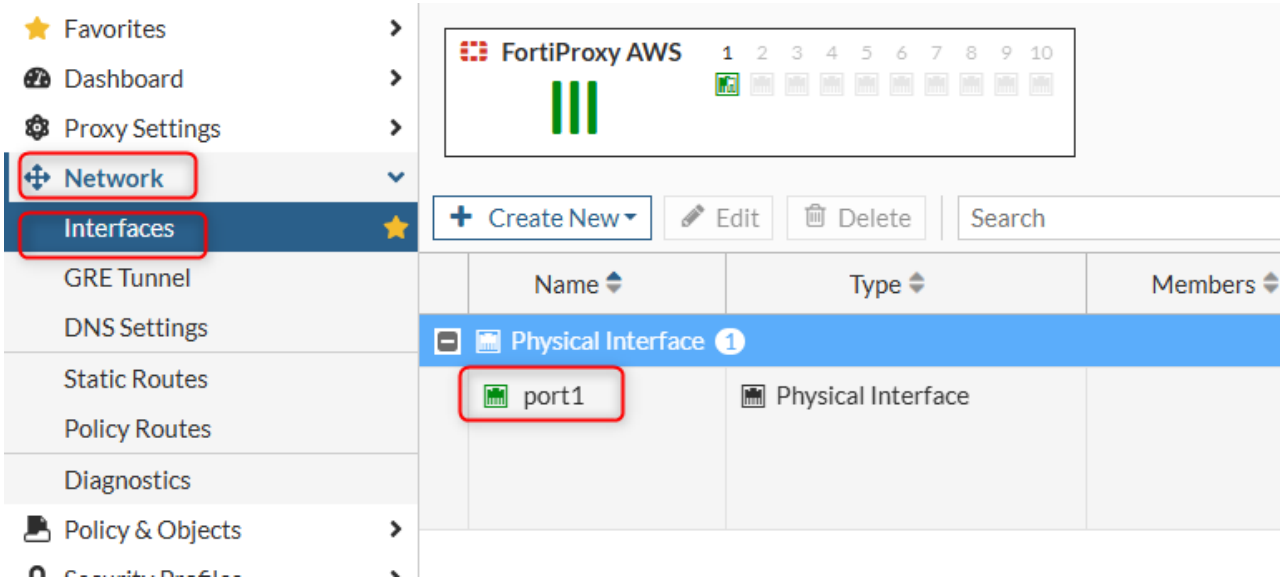
The proxy is now ready to forward requests from the sensor to appropriate end points *without authentication*

For access with authentication

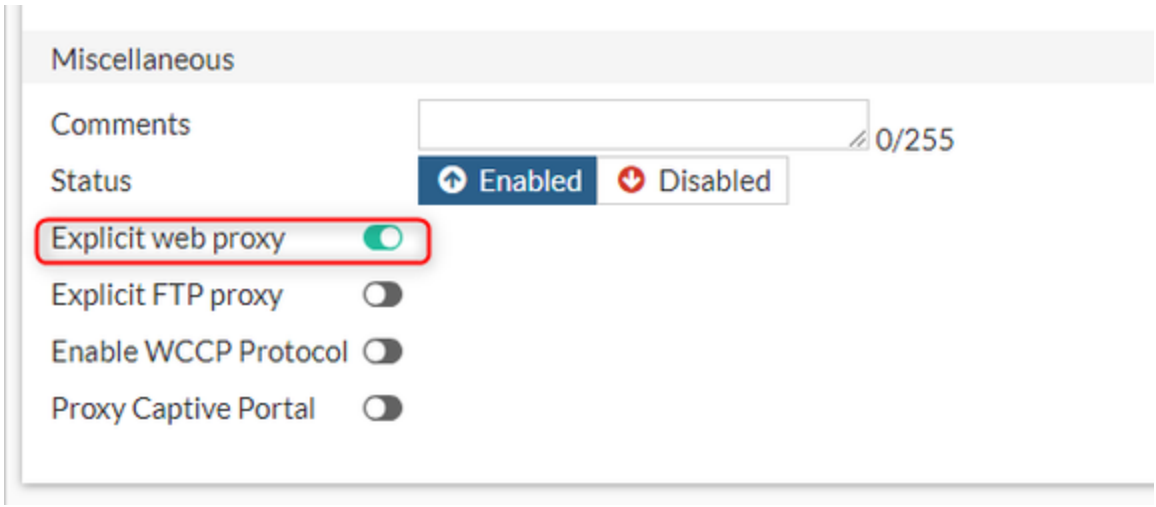
The current version of the FortiNDR Cloud sensor only supports Basic authentication.

1. Go to *Proxy Settings* > *Explicit Proxy*.
2. Click the web-proxy and select *Edit*.
3. For *Interface* select *port 1* (or any other physical port that is specific to your environment).
4. Keep the rest of the default settings and click *OK*.
5. Go to *Network* > *Interfaces*.

6. Highlight the designated port and click *Edit*.



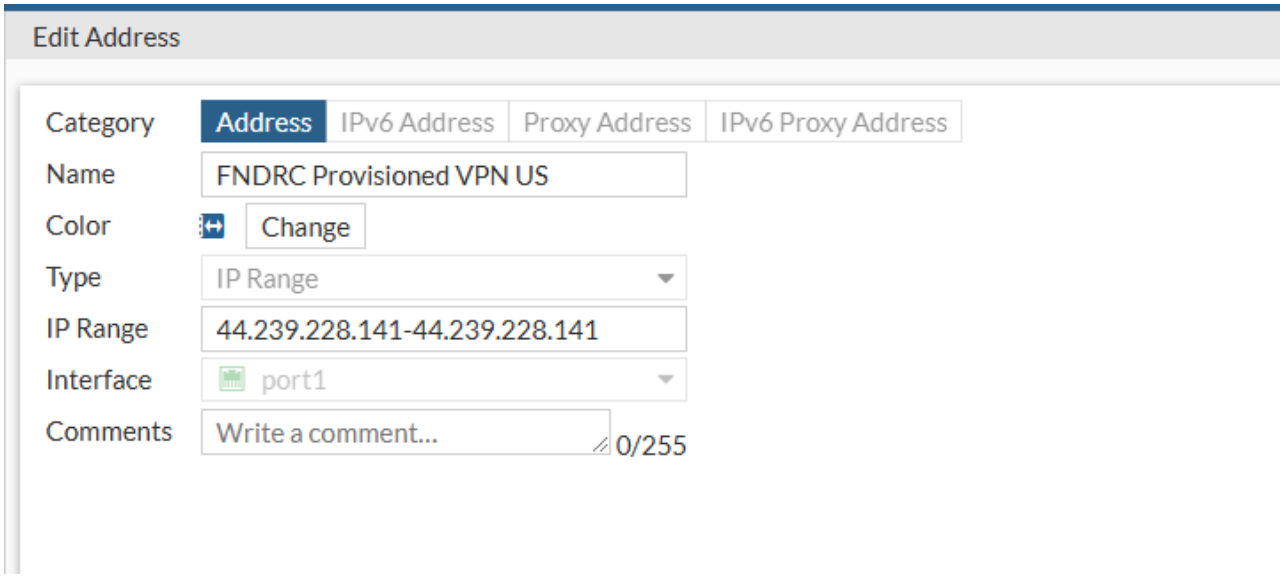
7. If required, change the default HTTP and HTTPS port.
8. Enable *Explicit web proxy* and click *OK*.



9. Go to *Policy and Objects* > *Addresses*.
10. Add the VPN and S3 upload end point IP addresses as shown below:

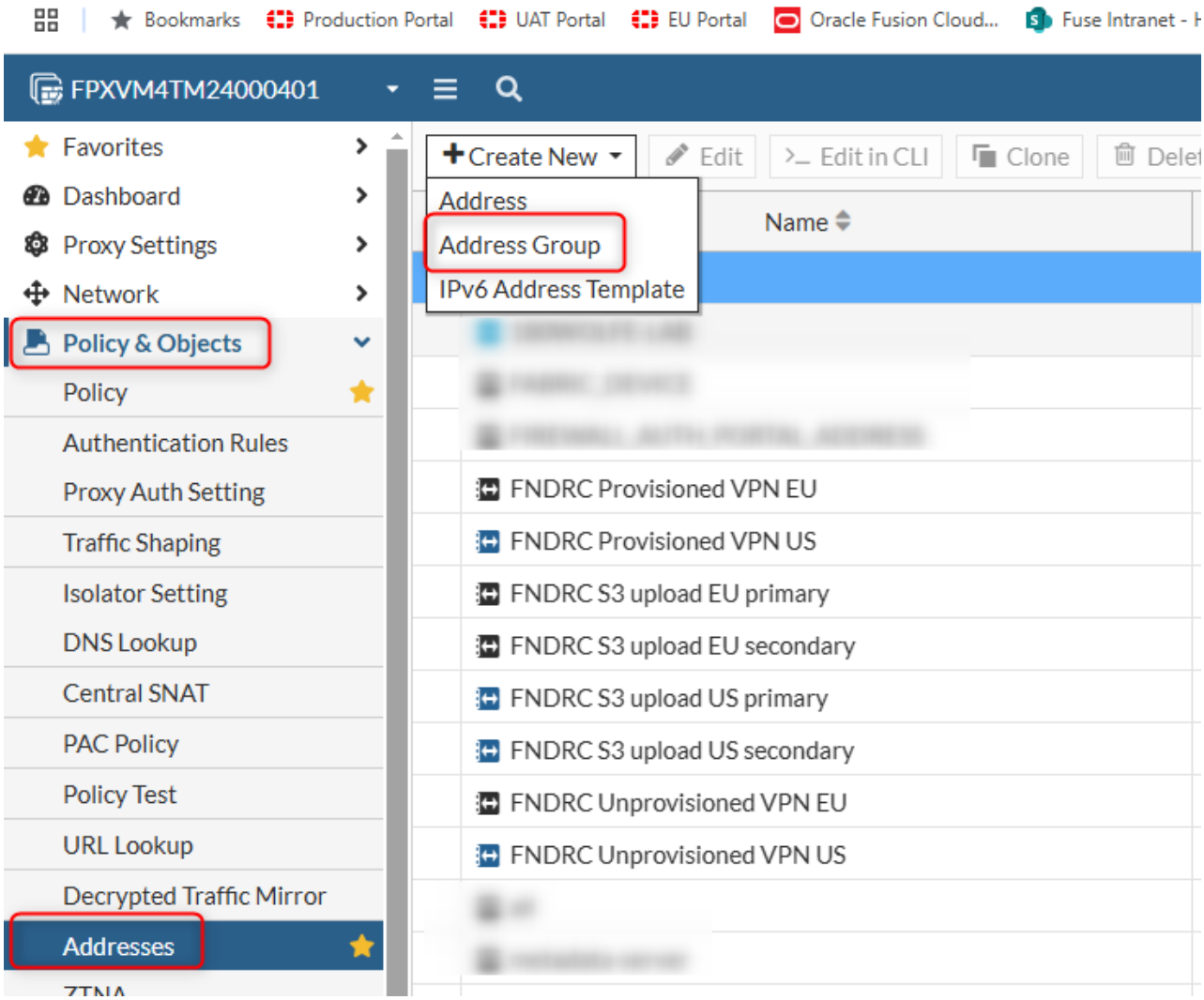
North America	52.36.236.168 (Unprovisioned VPN US) 44.239.228.141 (Provisioned VPN US) 138.43.114.16 (S3 endpoint Primary US) 138.43.114.141 [S3 endpoint backup US]
EU region	18.153.171.115 (Unprovisioned VPN EU) 3.124.46.55 (Provisioned VPN EU) 3.72.240.234 (S3 endpoint Primary EU) 3.123.116.122 [S3 endpoint backup EU]

AP region	47.131.38.17 (Unprovisioned VPN AP) 13.251.235.20 (Provisioned VPN AP) 13.215.106.143 (S3 endpoint Primary AP) 13.251.181.190 [S3 endpoint backup AP]

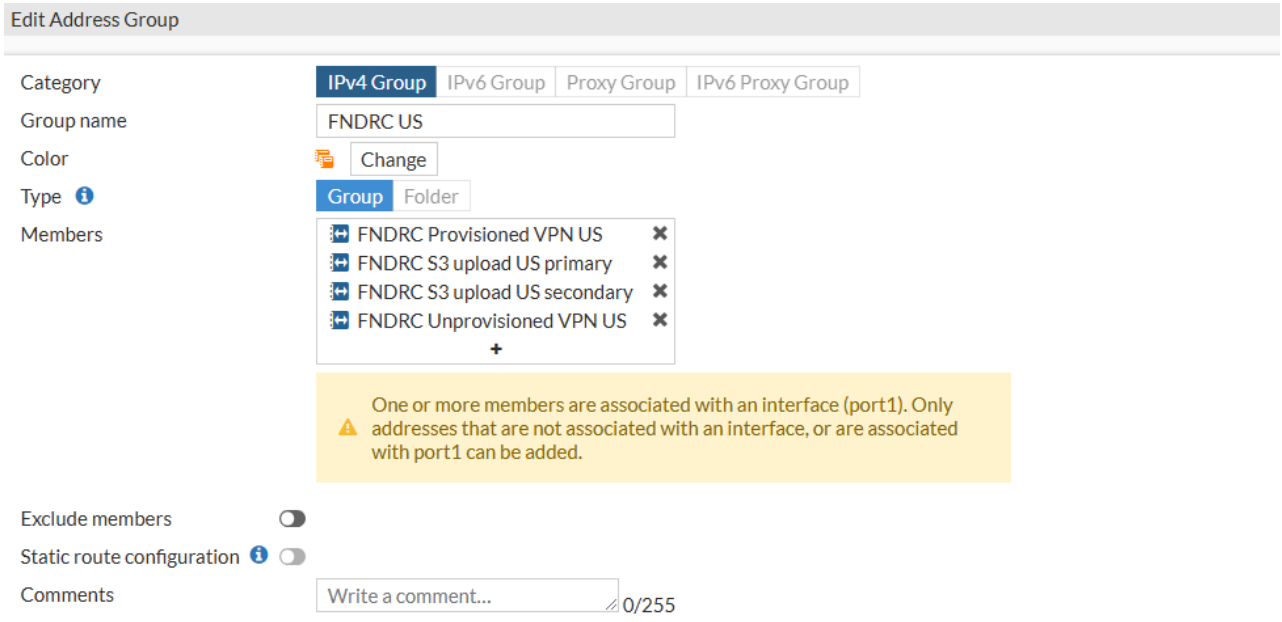


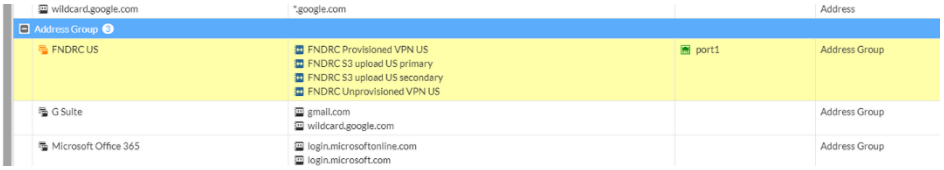
Name	IP Address	Port
FNDRC Provisioned VPN AP	13.251.235.20	port1
FNDRC Provisioned VPN EU	3.124.46.55	port1
FNDRC Provisioned VPN US	44.239.228.141	port1
FNDRC S3 endpoint Primary AP	13.215.106.143	port1
FNDRC S3 endpoint Primary EU	3.72.240.234	port1
FNDRC S3 endpoint Primary US	138.43.114.16	port1
FNDRC S3 endpoint backup AP	13.251.181.190	port1
FNDRC S3 endpoint backup EU	3.123.116.122	port1
FNDRC S3 endpoint backup US	138.43.114.141	port1
FNDRC Unprovisioned VPN AP	47.131.38.17	port1
FNDRC Unprovisioned VPN EU	18.153.171.115	port1
FNDRC Unprovisioned VPN US	52.36.236.168	port1

11. Go to *Policy and Objects* > *Addresses* > *Create New* > *Address group*.



12. Give the group a name and add the addresses created above to the group and click *OK*.





13. Click the CLI icon (**>_**)at the upper-right side of the page to open the CLI console.
14. Copy and paste the below to the console. Close the console when done.

```
config system dns-database
    edit "my-dns"
        set domain "vpce.amazonaws.com"
        config dns-entry
            edit 1
                set hostname "icebrg-uat-sensor-ingest.bucket.vpce-0e8d47840a7ffbf5f-
hedlogmh.s3.us-west-2.vpce.amazonaws.com"
                set ip 138.43.114.141
            next
            edit 2
                set hostname "icebrg-uat-sensor-ingest.bucket.vpce-0e8d47840a7ffbf5f-
hedlogmh.s3.us-west-2.vpce.amazonaws.com"
                set ip 138.43.114.16
            next
        end
    next
end
```

If the sensor(s) are to be provisioned in the EU region the configuration will look like below:

```
config system dns-database
    edit "my-dns-FNDRC-EU"
        set domain "vpce.amazonaws.com"
        config dns-entry
            edit 1
                set hostname "fortindr-cloud-eu-sensor-etl-production-sensor-
ingest.bucket.vpce-04cca23d7dbdf8626-x2c1jp2i.s3.eu-central-1.vpce.amazonaws.com"
                set ip 3.72.240.234
            next
            edit 2
                set hostname "fortindr-cloud-eu-sensor-etl-production-sensor-
ingest.bucket.vpce-04cca23d7dbdf8626-x2c1jp2i.s3.eu-central-1.vpce.amazonaws.com"
                set ip 3.123.116.122
            next
        end
    next
end
```

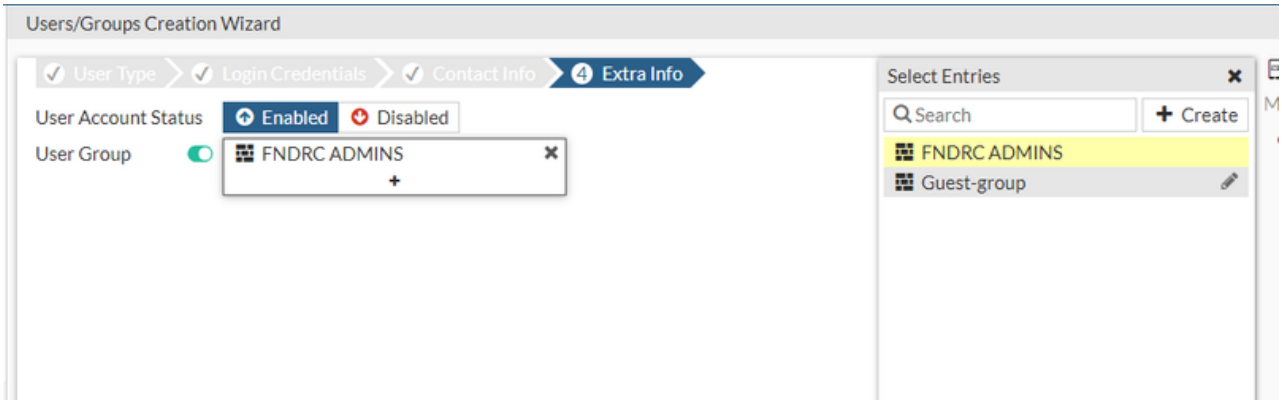
If the sensor(s) are to be provisioned in the APAC region the configuration will look like below:

```
config system dns-database edit
    "my-dns-FNDRC-AP"
        set domain "vpce.amazonaws.com"
        config dns-entry
            edit 1
                set hostname "fortindr-cloud-ap-sensor-etl-production-sensor-
ingest.bucket.vpce-0ef3cbdf9c3b9627e-3tjxjoj7.s3.ap-southeast-
1.vpce.amazonaws.com"
                set ip 13.215.106.143
            next edit 2
                set hostname "fortindr-cloud-ap-sensor-etl-production-sensor-
ingest.bucket.vpce-0ef3cbdf9c3b9627e-3tjxjoj7.s3.ap-southeast-
1.vpce.amazonaws.com"
                set ip 13.251.181.190
            next
        end
    next
end
```

15. Go to *User & Authentication> User Groups > Create New*.
16. Give the group a name and make sure the *Group Type* is *Firewall*.
17. Click *OK* to create the group.

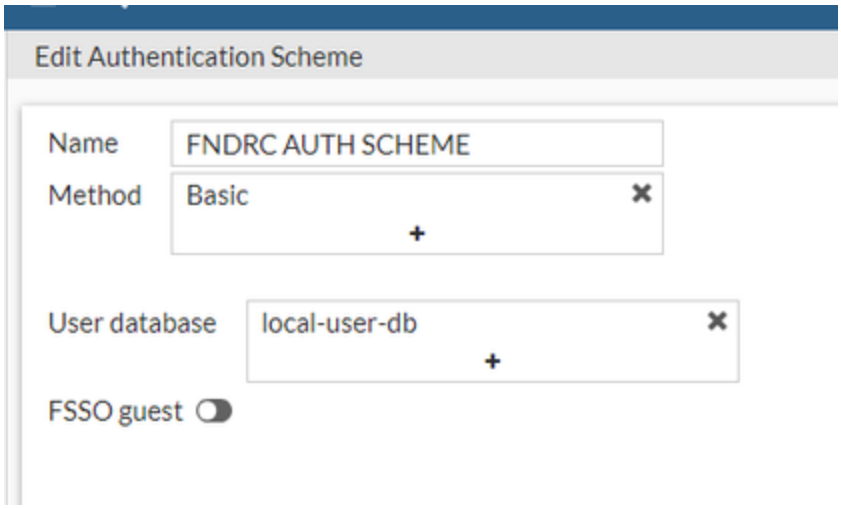
18. Go to *User & Authentication > User Definition > Create New*.
19. Select *Local User*.

20. Create a username and password.
21. Make sure *2FA* is disabled.
22. Enable the user group, then select the user group you created above, and submit



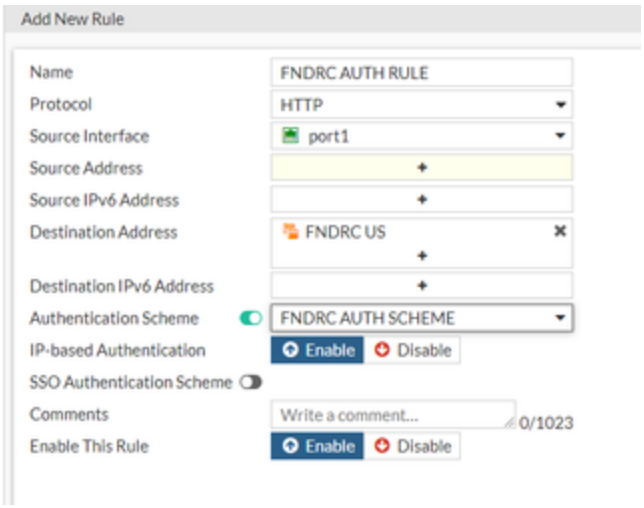
23. Go to *Policy and Objects* > *Authentication Rules* > *New* > *Authentication scheme*. Configure the scheme and click *OK*.

Name	Give the scheme a name.
Method	Select *Basic*.
User database	Select *local-user-db*.



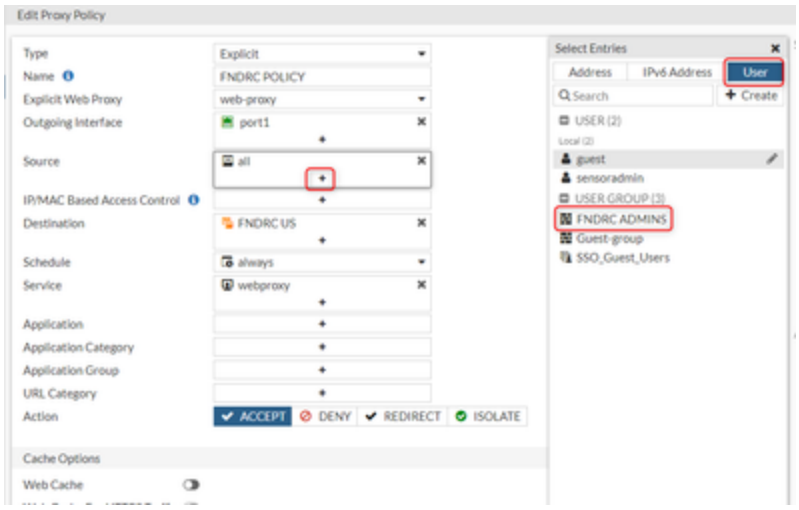
24. Go to *Policy and Objects* > *Authentication Rules* > *New* > *Authentication Rule*. Configure the rule settings and click *OK*.

Name	Give the rule a name.
Protocol	Select *HTTP* .
Source interface	Select the source interface.
Source address	Select the sensor address or leave it unchanged.
Destination address	Select the address group that was created earlier.
Authentication scheme	Enable and select the scheme created above



25. Go to *Policy and Objects* > *Policy* > *Create New*. Configure the policy and click *OK*.

Type	Select *Explicit*.
Name	Give the policy a name.
Outgoing interface	Select the same as the addresses added.
Source	Select the sensor address (needs to be added as an address) or choose All for any source.
Destination	Select the address group that was created earlier.
Service	Select *webproxy*.
User	Add the user group that was created earlier



At this point Proxy is ready to forward packets from the sensor(s) to the FortiNDR Cloud backend services using Basic Authentication.

Change Log

Date	Change Description
2023-04-02	Initial release version 2.5.0

www.fortinet.com