Sophos NDR Early Access Program – Quick Start

July 17, 2023

Synopsis

This guide will provide initial getting started instructions to enable, deploy and test with an NDR integration.

PRE-Requisites

You must already have a Sophos Central account and XDR or XDR Trial account.

For help

Please contact us at NDREarlyAccessProgram@sophos.com for assistance if you become stuck.

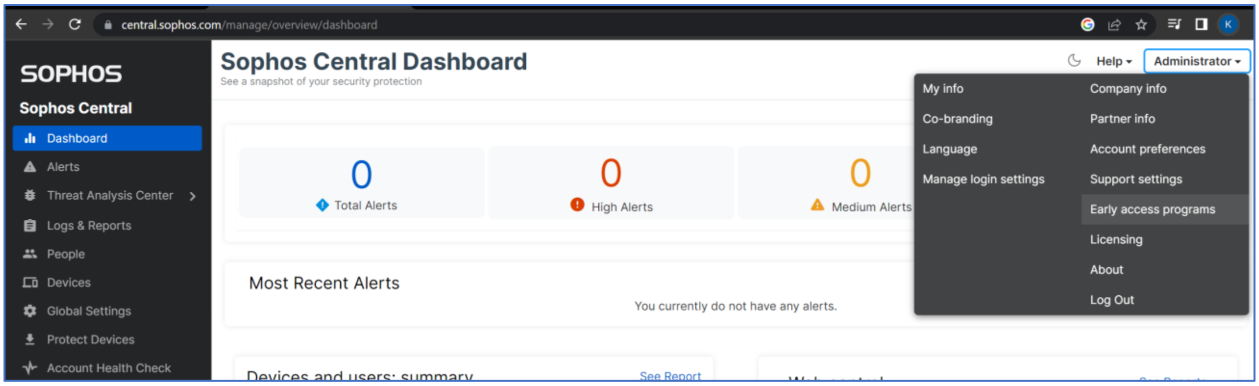
Step 1 – Register for the NDR Early Access program.

Complete the brief account and contact detail registration form. **Sophos NDR EAP Registration**

This will enable our deployment and troubleshooting teams to contact you if you need assistance during the EAP period.

Step 2- Enable the NDR for XDR EAP

From your Sophos central account navigate to the Early Access Programs and enable the 'New XDR Features' EAP.



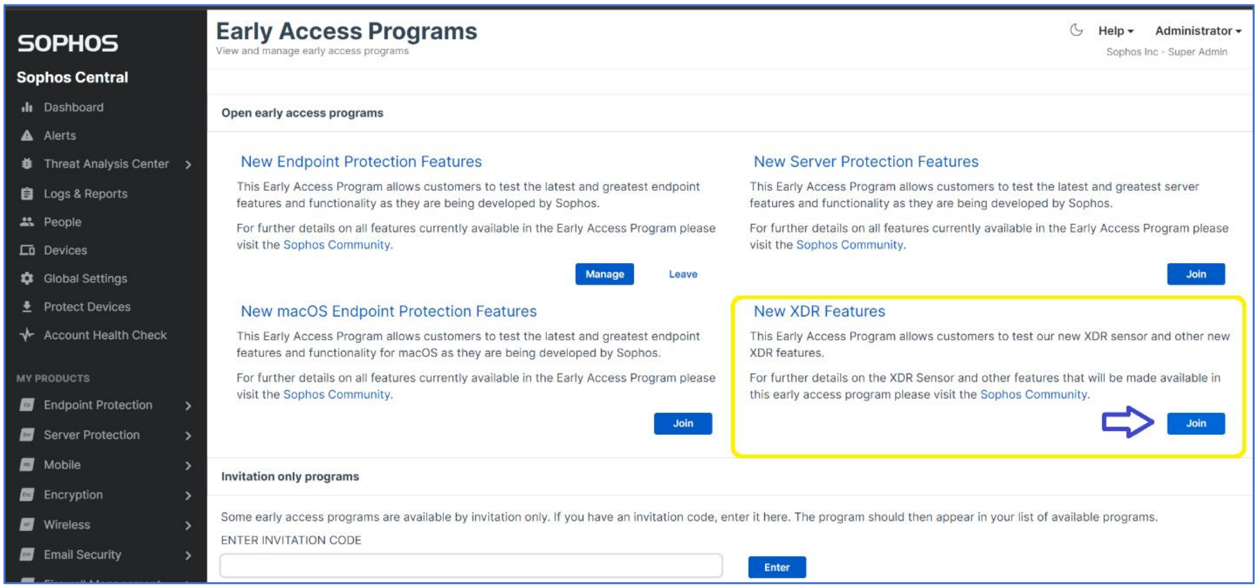
Sophos Central Dashboard

See a snapshot of your security protection

Most Recent Alerts

You currently do not have any alerts.

Join the New XDR Features EAP and accept the EULA.



Early Access Programs

View and manage early access programs

Open early access programs

New Endpoint Protection Features

This Early Access Program allows customers to test the latest and greatest endpoint features and functionality as they are being developed by Sophos.

For further details on all features currently available in the Early Access Program please visit the Sophos Community.

New Server Protection Features

This Early Access Program allows customers to test the latest and greatest server features and functionality as they are being developed by Sophos.

For further details on all features currently available in the Early Access Program please visit the Sophos Community.

New macOS Endpoint Protection Features

This Early Access Program allows customers to test the latest and greatest endpoint features and functionality for macOS as they are being developed by Sophos.

For further details on all features currently available in the Early Access Program please visit the Sophos Community.

New XDR Features

This Early Access Program allows customers to test our new XDR sensor and other new XDR features.

For further details on the XDR Sensor and other features that will be made available in this early access program please visit the Sophos Community.

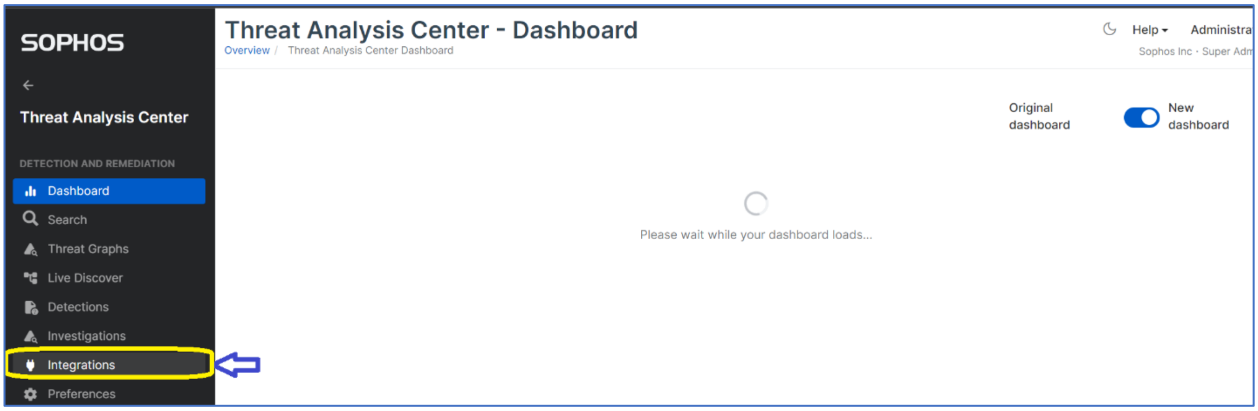
Invitation only programs

Some early access programs are available by invitation only. If you have an invitation code, enter it here. The program should then appear in your list of available programs.

ENTER INVITATION CODE

Step 3 – Create an NDR Sensor Integration

From the Threat Analysis Center select Integrations

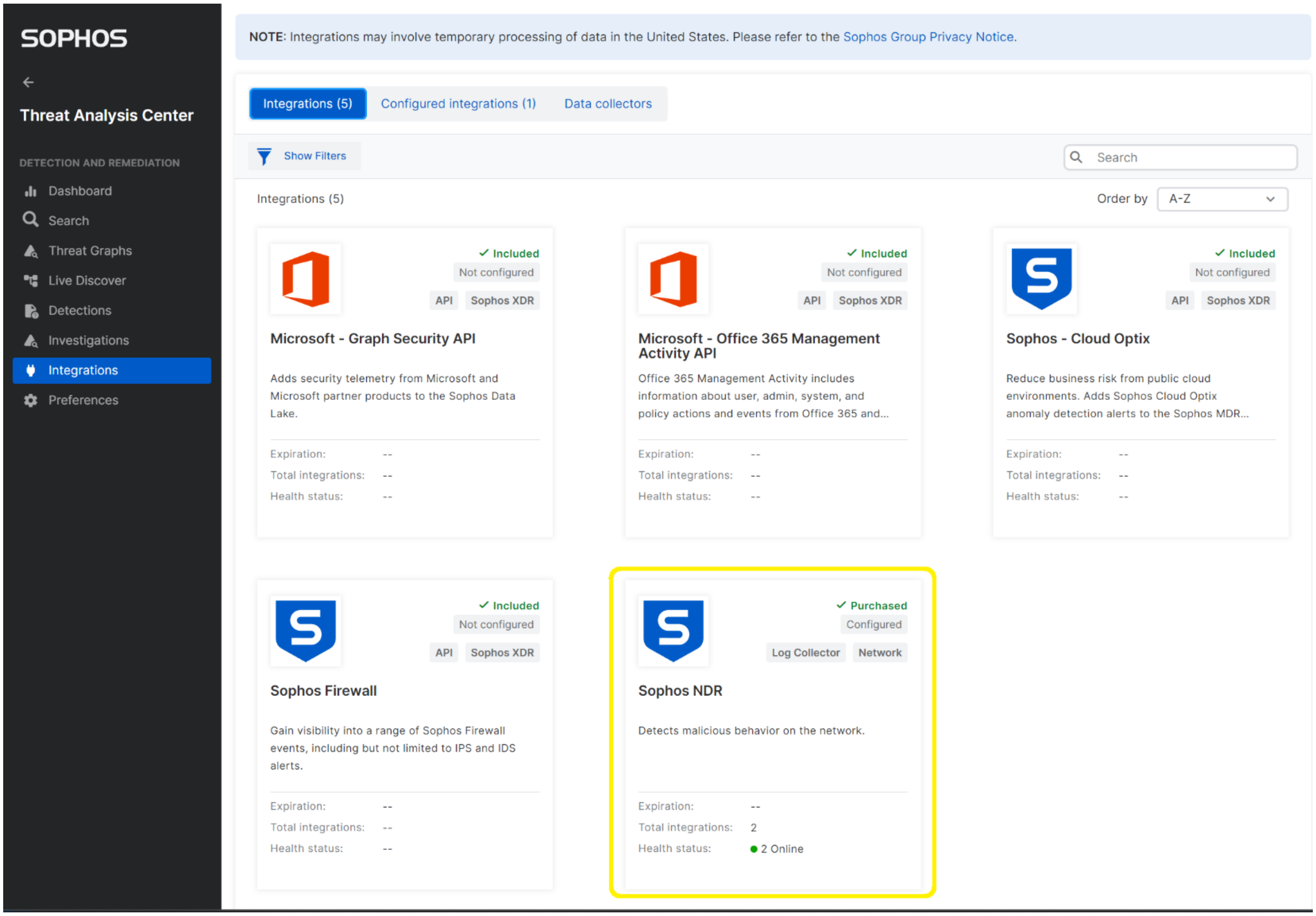


Threat Analysis Center - Dashboard

Overview / Threat Analysis Center Dashboard

Please wait while your dashboard loads...

Select Sophos NDR



NOTE: Integrations may involve temporary processing of data in the United States. Please refer to the Sophos Group Privacy Notice.

Integrations (5)

✓ Included · Not configured · API · Sophos XDR

Microsoft - Graph Security API

Adds security telemetry from Microsoft and Microsoft partner products to the Sophos Data Lake.

Expiration: --
Total integrations: --
Health status: --

✓ Included · Not configured · API · Sophos XDR

Microsoft - Office 365 Management Activity API

Office 365 Management Activity includes information about user, admin, system, and policy actions and events from Office 365 and...

Expiration: --
Total integrations: --
Health status: --

✓ Included · Not configured · API · Sophos XDR

Sophos - Cloud Optix

Reduce business risk from public cloud environments. Adds Sophos Cloud Optix anomaly detection alerts to the Sophos MDR...

Expiration: --
Total integrations: --
Health status: --

✓ Included · Not configured · API · Sophos XDR

Sophos Firewall

Gain visibilty into a range of Sophos Firewall events, including but not limited to IPS and IDS alerts.

Expiration: --
Total integrations: --
Health status: --

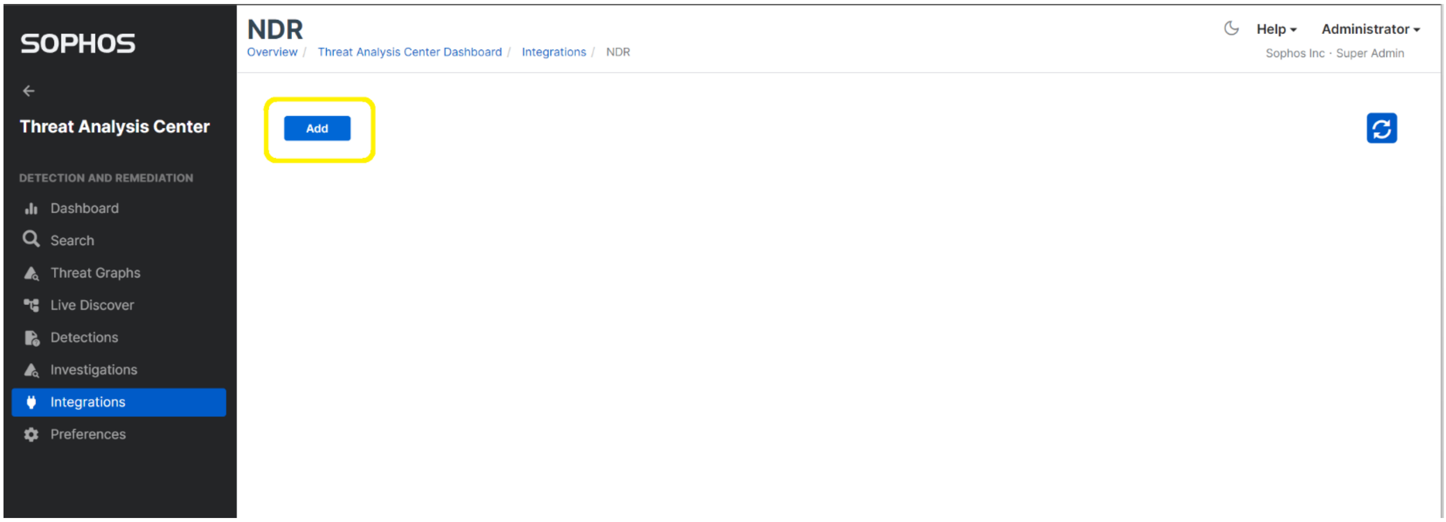
✓ Purchased · Configured · Log Collector · Network

Sophos NDR

Detects malicious behavior on the network.

Expiration: --
Total integrations: 2
Health status: ● 2 Online

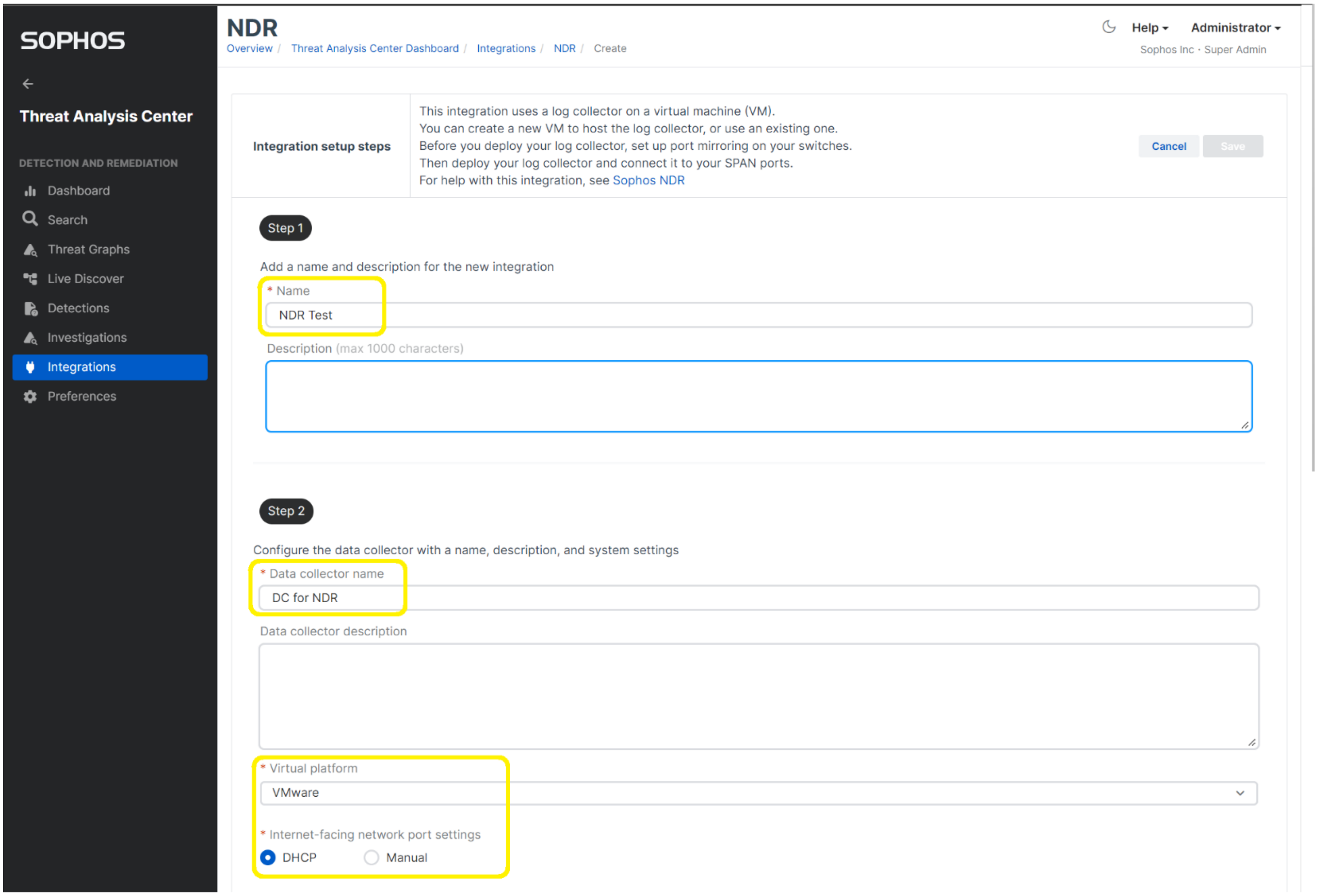
Select Add



Provide a name for the integration and the Data Collector it will run on. The data collector is the Virtual machine that will host the NDR sensor. Select the Virtual Platform (VMWare or Hyper-V). In this case I will be deploying on VMWare.

For complete install instructions see the install guide: https://doc.sophos.com/central/Customer/help/en-us/ManageYourProducts/ThreatAnalysisCenter/Integrations/Sophos/SophosNDR/index.html#configure-the-vm

Video of install on VMWare - https://techvids.sophos.com/watch/gdqE4Go54CcET9U3XErVY5
Video of install on Hyper-V - https://community.sophos.com/ndr-community-channel/m/ndr-videos/9537



Integration setup steps

This integration uses a log collector on a virtual machine (VM).
You can create a new VM to host the log collector, or use an existing one.
Before you deploy your log collector, set up port mirroring on your switches.
Then deploy your log collector and connect it to your SPAN ports.
For help with this integration, see Sophos NDR

Step 1

Add a name and description for the new integration

* Name: NDR Test

Description (max 1000 characters)

Step 2

Configure the data collector with a name, description, and system settings

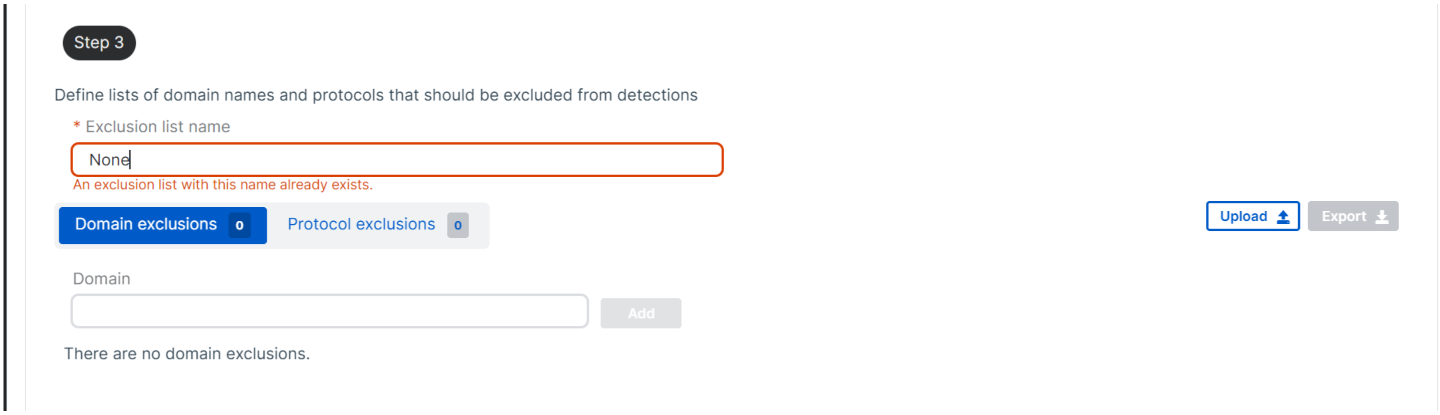
* Data collector name: DC for NDR

Data collector description

* Virtual platform: VMware

* Internet-facing network port settings
● DHCP ○ Manual

Set any exclusion and Save (NOTE Save is at the top right of the page)



Step 3

Define lists of domain names and protocols that should be excluded from detections

* Exclusion list name

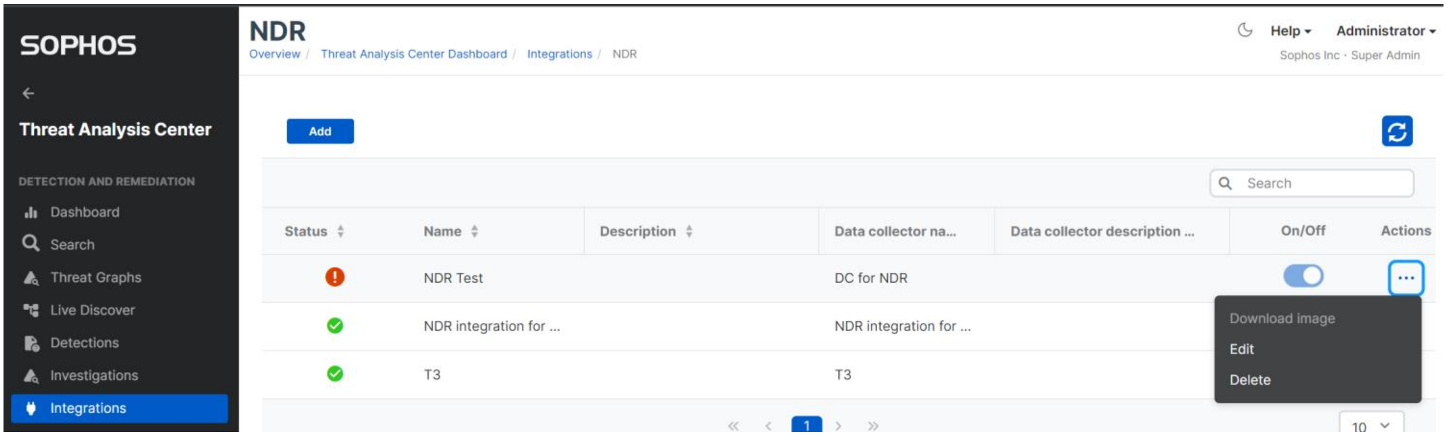
None

An exclusion list with this name already exists.

There are no domain exclusions.

STEP 4 Deploy the OVA (VMWare)

Generating the OVA image can take 5-10 min. Once available the option to download will be available.

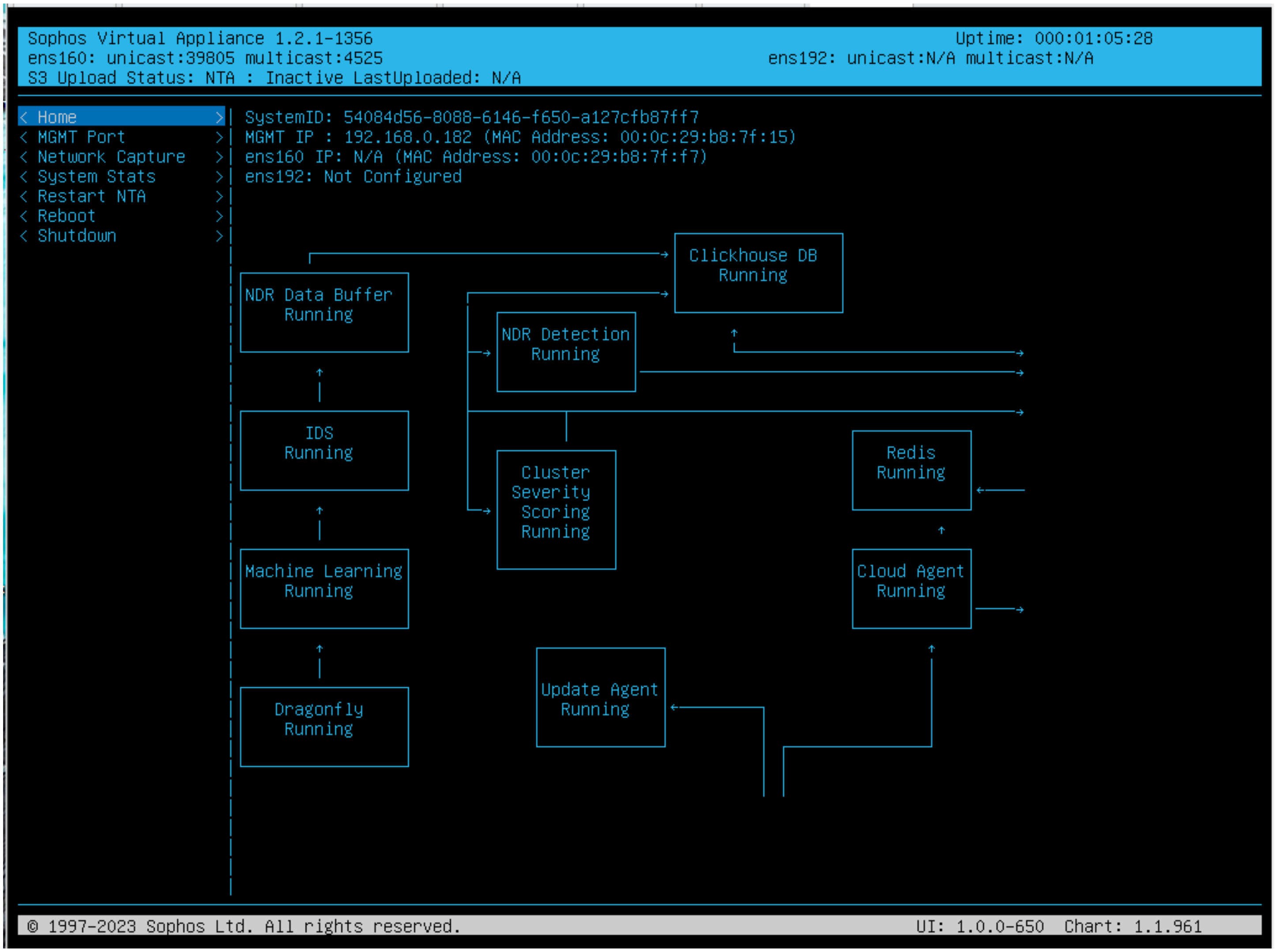


Status	Name	Description	Data collector na...	Data collector description ...	On/Off	Actions
!	NDR Test		DC for NDR		●	···
✓	NDR integration for ...		NDR integration for ...			
✓	T3		T3			

Once available load the OVA in VMWare and power on the virtual machine

Install can take 15-30 min before you get to the default console on the VM showing the status of the VM.

You should start seeing packet capture information (Unicast > Multicast) depending on the network configuration. This is a default install on VMWare with the appliance's network adaptors set to bridged.



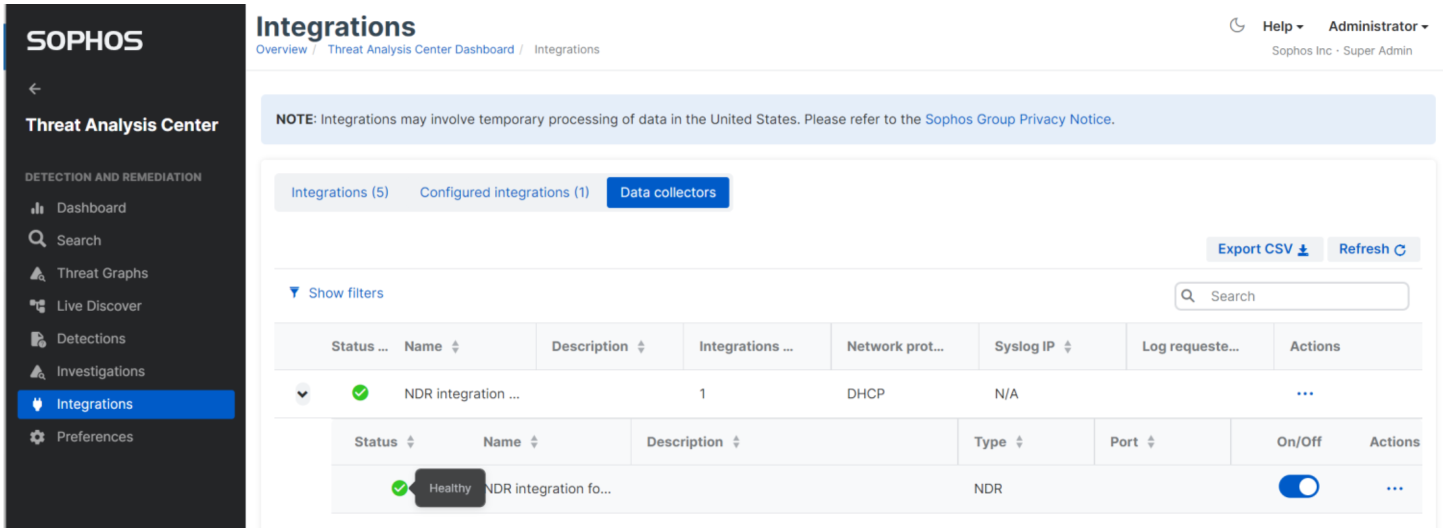
```
Sophos Virtual Appliance 1.2.1-1356                              Uptime: 000:01:05:28
ens160: unicast:39805 multicast:4525                      ens192: unicast:N/A multicast:N/A
S3 Upload Status: NTA : Inactive LastUploaded: N/A

< Home             >| SystemID: 54084d56-8088-6146-f650-a127cfb87ff7
< MGMT Port        >| MGMT IP : 192.168.0.182 (MAC Address: 00:0c:29:b8:7f:15)
< Network Capture  >| ens160 IP: N/A (MAC Address: 00:0c:29:b8:7f:f7)
< System Stats     >| ens192: Not Configured
< Restart NTA      >|
< Reboot           >|
< Shutdown         >|

© 1997-2023 Sophos Ltd. All rights reserved.                 UI: 1.0.0-650  Chart: 1.1.961
```

Step 5 Confirm that central shows the data connector and NDR Sensor as healthy.

This can take some time (10-30 min) before the NDR sensor is fully online and reported as healthy. It is installing, downloading any updates, and restarting various containers on the virtual appliance.



Integrations

Overview / Threat Analysis Center Dashboard / Integrations

NOTE: Integrations may involve temporary processing of data in the United States. Please refer to the Sophos Group Privacy Notice.

Integrations (5) | Configured integrations (1) | Data collectors

Export CSV | Refresh

Show filters | Search

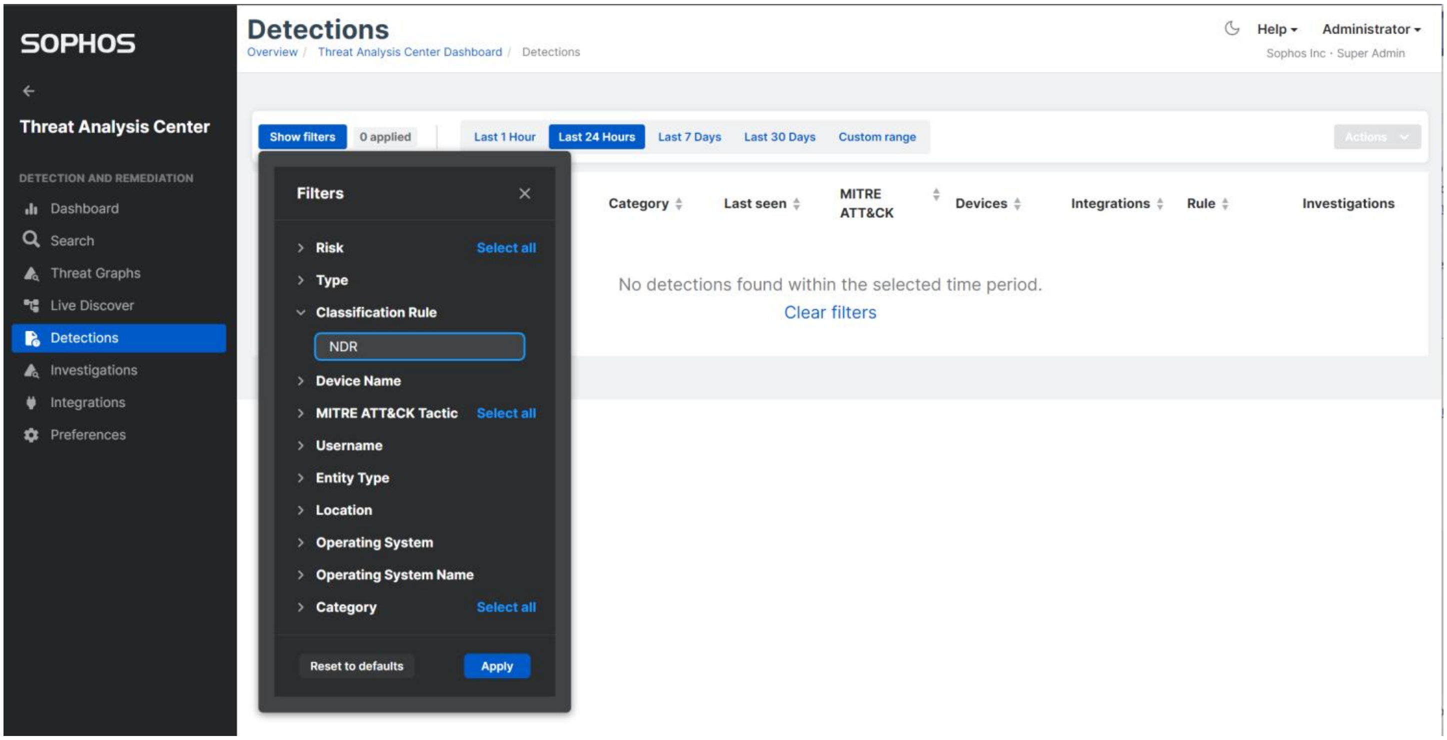
Status ...	Name	Description	Integrations ...	Network prot...	Syslog IP	Log requeste...	Actions
✓	NDR integration ...		1	DHCP	N/A		···

Status	Name	Description	Type	Port	On/Off	Actions
✓ Healthy	NDR integration fo...		NDR		●	···

Please contact us at NDREarlyAccessProgram@sophos.com for assistance if you become stuck.

Step 6 Confirm everything is working.

After 24 hours the NDR sensor should be generating regular statistics reports, you can see these in the Threat Analysis Center Detections, Set the ‘Classification Rule’ filter to NDR and apply



Classification Rule: NDR

No detections found within the selected time period.

KNOWN ISSUES:

Currently the NDR query category is showing in Live Discover, but NO queries are currently shown.
Queries should be available in the next few days.

After 1 or more reports or detections have been generated by NDR you can check the version and ID of the NDR sensor with the following Live Discover Query

```
SELECT DISTINCT
  CAST(JSON_EXTRACT(NDR_IOC.raw, '$.ingest_date') AS VARCHAR) DAY,
  CAST(JSON_EXTRACT(NDR_IOC.raw, '$.sensor') AS VARCHAR) Sensor,
  CAST(JSON_EXTRACT(NDR_IOC.raw, '$.sensor_id') AS VARCHAR) Sensor_ID,
  CAST(JSON_EXTRACT(NDR_IOC.raw, '$.sensor_version') AS VARCHAR) Sensor_Version
FROM mdr_ioc_all AS NDR_IOC
WHERE NDR_IOC.ioc_worker_id = 'worker_ndr'
ORDER BY DAY DESC
```