INFINITY

16 September 2025

NDR

Deployment Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
16 September 2025	Updated *"Preparing an NDR Sensor" on page 14* to include support for version R82.
25 August 2025	Updated **Supported Sensor Types** in NDR Sensors - *"Overview" on page 11*.
29 July 2025	Product was removed from the Infinity pillar.
18 May 2025	Added *"Setting up SNMP Monitoring on an NDR Sensor" on page 23*
16 March 2025	Updated *"Preparing an NDR Sensor" on page 14*
25 March 2024	Updated *"Registering the Appliance" on page 20*
31 January 2024	The product moved from the Horizon pillar to the Infinity pillar
29 May 2023	Added: ■ *"NDR Security Check-up Report" on page 44* Updated: ■ *"Preparing an NDR Sensor" on page 14* ■ *"SPAN Port Configuration" on page 47* ■ *"Binding with Infinity XDR/XPR" on page 50*
02 January 2023	First release of this document

Table of Contents

Introduction to NDR

Check Point NDR is a comprehensive technology stack for Network Detection and Response. The network sensors can be deployed on premises or in cloud environments.

The Check Point NDR service concept:

- Sensors analyze network traffic, and create logs which are sent to the NDR cloud for storage and analysis.
- Behavioral Analytics AI engines process the logs and create analytical conclusions.
- Human analysts use event visualization tools for more data comprehension.
- Identify data anomalies through correlation with ThreatCloud intelligence and application risk scoring.
- Publish analytical conclusions as threat indicators and tags.
- Input feeds pull threat indicators from third party threat intelligence sources.
- Enforcement points apply the indicators and match them to network traffic, for detect or prevent actions.

This guide focuses on the sensor deployment for the NDR application. You can achieve network visibility in minutes, with easy intuitive deployment, minimal configuration, and no impact on business traffic. No other Check Point products are required for NDR to work.

NDR Registration

Registering a Customer Domain

Note - This product is not part of the Infinity Portal. NDR maintains its own user and access authorizations repository.

NDR tenants are identified as 'domains'. Each domain defines a set of objects with:

- User authorizations for the domain access.
- Sensors that send logs and packet captures to the application.
- Reports, views, and insights.
- Intel indicators (IOCs).

To create a domain, go to *NDR Portal* and click **"Don't have an account? Register here"**. The Company Name you enter becomes the new domain name.

We recommend to subscribe to product news, as this allows Check Point to send you notifications for maintenance alerts and security events. When your domain request is approved, you receive a confirmation email with a link to create your new NDR domain.

Access to NDR Indicator Management Portal

If this is your first domain on the portal, you must add user credentials for your new user account. This process installs a certificate in your browser, and is used to identify and authenticate you to NDR the next time you log in.

You generate the certificate on the portal, download it to your endpoint, and import it into your browser.

1. Enter a password at the prompt. This password is used to encrypt your certificate when stored on disk. Enter the same password two times and remember it for the next step.
2. Click **Download** to download the certificate to your endpoint.

   Note - We recommend **not** to double-click the certificate object after you download it. This causes the operating system's certificate import wizard to launch. Some browsers do not recognize the wizard, and you must reboot the endpoint.
3. In your browser, open **Settings**, go to **Security** > **Management Certificates**, and click **Import**.
4. Browse for the certificate on your disk and select it.

Note - In the browse window you may need to change the file type to "Personal Information Exchange" or to "All files" to see your new downloaded certificate

5. Load the certificate into the Personal certificate store (usually the default).
6. Complete the import procedure.
7. Go to *NDR Portal* and click **Sign In**.
8. At the prompt select your certificate to access the portal.
9. Select the new domain you created from the pull-down menu.

Forcing Chrome Browser Refresh

If you do not receive a prompt for the certificate when you try to sign in, close your browser and then open again to load the certificate into its personal certificate store. Use the History settings in your browser to relaunch all tabs.

1. Close all open Chrome instances.
2. Use the "Windows Key" to search for **PowerShell**. Right click on the PowerShell and select **Run as administrator**.
3. To stop all Chrome-related processes and to activate the certificate, run this command:

```
get -process -name Chrome | stop -process
```

NDR Sensors

Overview

How NDR works:

A network sensor extracts log fields from the network traffic to create a record with these and other fields:

- Source and destination
- IP addresses
- Ports
- Quantity of data transferred
- URLs
- Application categorization
- Risk categorization
- User identity

In return, NDR delivers threat indicators to the sensor.

Supported Sensor Types:

- NDR-Managed: Check Point Security Gateways (Quantum or CloudGuard)
- Non NDR-Managed: Check Point Security Gateways (Quantum, CloudGuard, and Quantum Spark), and Check Point Harmony Endpoint

  In addition, the sensor can deliver threat indicators to third-party devices.

If the sensors are managed by NDR, they are managed from a Management Server hosted by the NDR Indicator Management application. This means that you do not need to install a Management Server, SmartEvent, SmartConsole or provision policy.

A non NDR-Managed sensor sends its logs to a Management Server or Log Server, and Check Point Log Exporter forward the logs to NDR to process. In addition, you must configure the sensor separately to subscribe to NDR Intel feeds.

Check Point Quantum NDR Sensors

You can easily convert any Check Point Quantum Security Gateway appliance into an NDR-Managed NDR Sensor. The appliance's control layer is then slaved to the NDR application, and all control layer communications, with policy, logs, ThreatCloud queries, NTP, DNS, etc. are tunnelled over a mutually-authenticated SSL VPN tunnel to the NDR cloud. Traffic inspection is done through Monitor Mode interfaces attached to switch mirror ports. In addition, inline environment (Bridge Mode) is supported - with fail-open network interfaces.

In NDR mode, the appliance applies Check Point's real-time advanced SNBT threat detection engines on the mirrored network traffic, with:

- IDS/IPS
- Application fingerprinting
- Anti-Virus and Anti-Bot
- Threat Emulation (evasion-resistant sandboxing)

NDR sends analytical conclusions as log records to the NDR back end for more analysis.

Check Point CloudGuard NDR Sensors

You can apply the same NDR mode conversion process you use for Quantum NDR sensors (as described in *"Preparing an NDR Sensor" on page 14* on CloudGuard and Open Server Gaia installations. There are some differences in interface names and license, but the SNBT functionality is the same on these sensors. A major difference is how virtualization specifically impacts the data layer attachment:

- Fail-open interfaces are unavailable - Therefore, the inline environment is not supported, only Monitor Mode.
- CloudGuard for VMware ESX deployments operate similar to physical appliances, through mirroring.
- The NDR application automatically provisions CloudGuard for AWS, with AWS Lambda serverless computing to manage cloud-native traffic mirroring APIs. The CloudGuard Network Security instance is deployed out of band for its Compute capabilities, with no effect on business traffic.
- CloudGuard for GCP operates similarly to AWS, but mirroring is currently manually provisioned.
- As an alternative for all environments, you can deploy a CloudGuard Network Security instance, and convert it into NDR mode. You can provision traffic mirroring on a separate computer or appliance (for example, Check Point CloudGuard Network Security configured with a Mirror and Decrypt policy) on VXLAN.

Log Server Registration

If you have a Check Point Management Server or Log Server that collects logs from Check Point Security Gateways or Check Point Harmony Endpoint, or both, you can export the logs to NDR Indicator Management for NDR visualizations and analysis, as detailed in *"NDR Log Server Registration" on page 30*.

The server is considered non NDR-Managed.

Preparing an NDR Sensor

Overview

This section describes how to convert a Check Point Quantum Security Gateway appliance to an NDR-Managed NDR sensor.

You can use the same process for an NDR sensor installed as a Virtual Machine in a cloud or on an Open Server.

Supported Versions

- R82
- R81.20
- R81.10

Note - Quantum Maestro is supported only in R82 and higher.

Installing Check Point R81.10 and higher

Clean-install Check Point R81.10 or higher on the Quantum (or CloudGuard) Security Gateway and install the latest Jumbo Hotfix Accumulator for the version you installed.

For details, see:

- For R82 - sk181127
- For R81.20 - sk173903
- For R81.10 - sk170416

The Security Gateway is automatically converted to NDR mode when the steps detailed in Registering the Appliance complete successfully.

Important:

- You do not need to install a Check Point Management Server because NDR handles this function. Installing a Standalone server (that runs the Management Server and the Security Gateway) is not supported.
- The First Time Configuration Wizard options: **Enable as part of cluster** and **Enable DAIP (dynamic address)** are not supported.

Determining Configuration Settings

We recommend preparing the appliance in a staging network before deployment to the production environment.

If you use DHCP in the two locations, configure DHCP on the Management interface, and networking parameters will be automatically provisioned.

If you do not use DHCP in the target environment, use two different network interfaces for connectivity from the appliance to the NDR application:

- Target environment: Management interface (`eth0` on virtual instances) with static IP address and default gateway.
- Staging network: select a different connectivity interface that is not used for network monitoring and enable it for DHCP. For example, on an appliance that has on-board interfaces, you can use `eth8`.

This information is required for the target network environment:

1. The Management interface IP address, default gateway IP address (and, if required, IP address and port of a proxy server).
2. Which interface(s) on the appliance are used as Monitor Mode interfaces.

Note - Monitor Mode interfaces are used to connect the appliance to network switch SPAN (mirroring) ports. The default is to set "`eth1`" and "`eth2-01`" as the Monitor Mode interfaces. This default can be altered during appliance registration.
In addition, you can subsequently configure this from the appliance's Gaia Portal you can access from the NDR application.
"`eth1`" refers to the first onboard 1Gbps copper network interface, available on some appliances.
"`eth2-01`" refers to the first interface on the extension card in bay 2, if available on the appliance.

When you install the Security Gateway:

1. Complete the First Time Configuration Wizard, and make sure you can connect to the Internet:
   - Networking configuration on the staging network is complete.
   - You configure a DNS server IP address (if you do not use DHCP) for initial domain name resolution.
2. Enter a value for a SIC activation key.
3. License:

- The appliance starts off after a clean installation with a 14 day evaluation license.
- When you purchase the license, the Quantum appliance automatically pulls it from the User Center.
- You can also install an evaluation license, or for a CloudGuard installation, a BYOL license.

4. Configure the Management interface IP address and default gateway as required for the target network environment. Keep this interface disconnected while in the staging network.
5. If the target environment requires proxy configuration, this must be the last configuration step, as after defining the proxy, the appliance loses its Internet connectivity while in the staging network.

The appliance should remain connected to the portal for about 15 minutes after you complete the registration sequence for engine updates to complete the download.

Note - When the registration process successfully completes, you cannot connect to the appliance remotely with SSH or Gaia Portal. This is because the NDR sensor's control plane is tunnelled above SSL VPN to the NDR portal, and you can manage it only from the NDR application. In addition, the admin password is automatically randomized.
For post-registration maintenance, see *"Accessing the Sensor's Gaia Portal" on page 21*.

NDR Sensors for VMware ESX

Installation on VMware ESX follows the same process as for a physical appliance, with these further qualifications:

- Allocate a minimum of 100GB disk space for the sensor VM.
- Allocate a minimum of 2GB RAM for each processing core, with a minimum total of 8GB RAM.

Refer to VMware networking documentation for instructions on how to configure port mirroring on VMware virtual switches. Capture port groups must have Promiscuous Mode set to Accept if you use VMware VSS or VDS virtual switches.

Accessing the NDR Portal

Create these access rule authorizations on your network for allowing access out to the NDR application:

- If there is a firewall present, it must allow TCP port 443 connectivity from the appliance's Management interface to IP address 35.156.213.136, in addition to 18.196.115.85 (for *NDR Portal*), and 35.157.19.226 (for `feeds.now.checkpoint.com`).
- The NDR sensor authenticates to the NDR Indicator Management application portal with mutually authenticated TLS. Therefore, if you use HTTPS Inspection on the outbound path, you must request an exception for the NDR appliance's management traffic.
- Create an HTTPS Inspection exception for user access to *NDR Portal*.

Network Interfaces for Traffic Inspection

Monitor Mode

In most cases, you deploy the NDR sensor appliance passively, connected to one or more customer network switch's mirroring (SPAN) ports. It is necessary to identify which interfaces on the appliance are used for this function and make sure that they match your networking connections (fiber or copper) and speeds.

Note - The effective bandwidth for a monitor-mode port is usually less than the port specification. This is because the switch mirrors bi-directional traffic on a one appliance interface. For example, a 1Gbps interface on the appliance can only manage a maximum of 0.5 Gbps full-duplex traffic. More than that can overwhelm the link and cause packet loss on the switch.

Inline Bridge Mode

In some cases, customers find challenges with provisioning SPAN ports. An alternative connectivity option is an inline bridge (bump in the wire). This is an easy-to-provision configuration, however it does not provide the East/West visibility that monitor mode can. Its primary advantages are the ability to deliver on-box prevention, inline HTTPS Inspection, and Threat Extraction. Inline bridge deployment with NDR sensors is supported only with a Check Point Quantum Security Gateway fitted with a fail-open network interface.

You must install a fail-open NIC in the appliance's bay 1. A two-port fiber fail-open NIC is automatically provisioned with a single two-interface bridge. A four-port copper fail-open NIC provides two bridges. Connect the odd-numbered interfaces on the card (`eth1-01`, and if available, `eth1-03`) to the internal networking appliance and the even-numbered interfaces to the external appliance. You can toggle the bypass mode from the NDR application portal's Sensors tab through **Actions** > **BYPASS**.

Note - A common mistake is to connect the fail-open interface to a switch mirror (SPAN) port instead of using it as a bridge. This can cause high CPU consumption and sensor instability.
One more problematic configuration is management-over-bridge: the appliance's Management interface is connected to an internal network, and the management traffic to the NDR Portal is passed back through the appliance's bridge. This configuration is supported but can cause the appliance to disconnect from NDR each time the fail-open NIC bypass mode is toggled. Check Point recommends to connect the Management to a network segment on the external side of the NDR sensor.

Packet Duplication because of Overlapping Traffic

When processing traffic from multiple interfaces, it is important to prevent the appliance from seeing the same packet twice from multiple interfaces, as this can cause sensor instability. This scenario can occur if multiple interfaces see network segments that pass packets between them without intervening NAT.

In contrast, a correct deployment is to mirror a DMZ, and an internal network segment. One more scenario is when the appliance is a bridge between the firewall and the ISP router and monitors a SPAN port off a core switch. While each packet might be seen twice by the appliance, egress hide-NAT on the firewall means that the two packets' source IP addresses and ports are different.

Combined Inline/Monitor Mode

The best practice configuration combines inline (for prevention) and monitor-mode (for East-West) attachments. Because of the packet duplication limitation, the inline attachment must be external to the NAT. The real internal source IP addresses are seen on the monitor-mode interfaces and therefore can support Identity Awareness. You can also use multiple sensors to address this limitation.

Some network switches support a SPAN with ACL configuration, whereby you provide the switch with a set of rules for network traffic that should be mirrored from ingress ports to egress port. This can be used to exempt mirroring of traffic that would be already visible to the NDR appliance from other interfaces. For example, if the NDR appliance is deployed inline in the NAT for inspecting North/South traffic, configure switch mirroring, so it does not include traffic between internal and external addresses.

Lights Out Management(LOM)

In some rare situations, a NDR sensor may lose its cloud connection and you can no longer access it from the NDR application. In these cases, you can use a LOM module to remotely reboot the appliance or provide access to the console interface. You configure the LOM from the Gaia Clish, so you must do this before you register the appliance. See sk92652 for more details.

Configuring the Sensor on the NDR Indicator Management Application Portal

After you complete all the preparations, configure the sensor.

1. Log in to *NDR Portal*.
2. Access the customer domain.
3. If there are no sensors in the domain, you are directed to the **Sensors** tab.
4. From the left menu, select **Management** > **Sensors** > click **New** (top middle).
5. For a Quantum Security Gateway appliance, select **Physical** and enter the appliance's MAC address in colon-separated six-tuple notation (for example: 00:1C:7F:12:34:56).

   You can find the MAC address on a pull-out label on the appliance's front panel.

   The MAC address is the same as the appliance's Management interface's MAC address.

   Note - For a Security Gateway deployed as a Virtual Machine in a cloud or Open Server, select **Virtual**. A virtual MAC is generated automatically to identify the sensor.
6. Enter a description/name for the sensor.
7. Enter the sensor's location as a Latitude, Longitude pair.

   For example, Check Point HQ is located at 32.07, 34.79609.

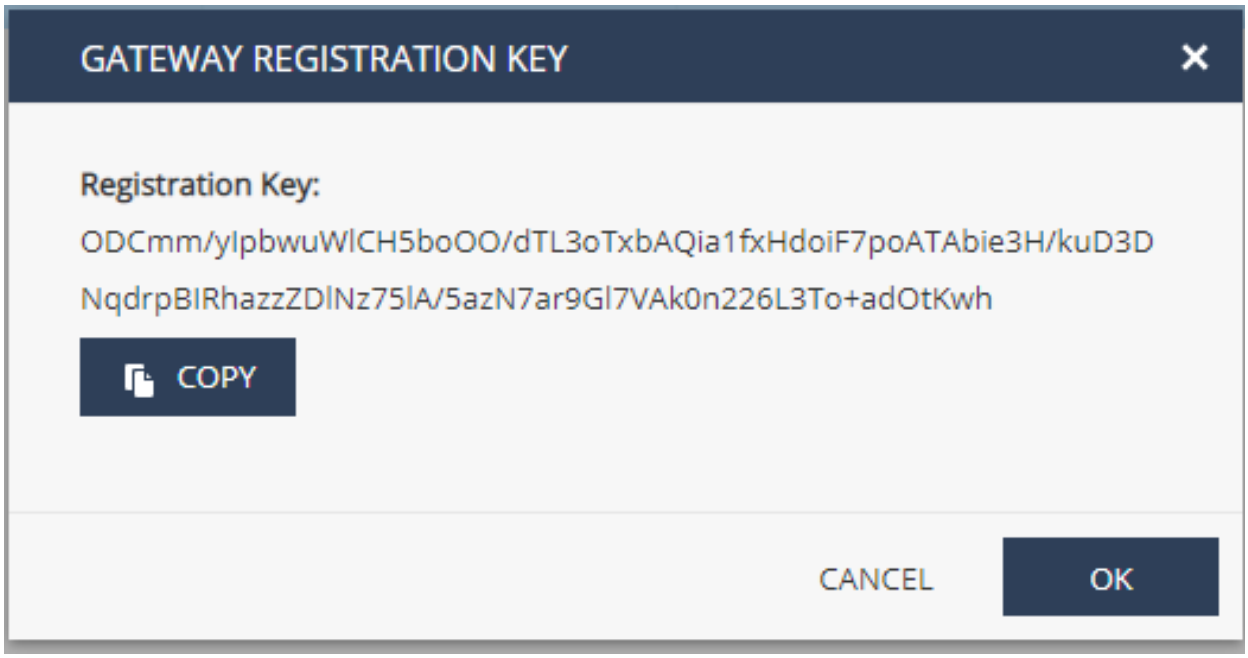
   This location is used for representation on the Cyber Threat Map.
8. Select the time zone for the sensor.
9. Click **ADD** in the lower right corner of the new sensor form.

   At this time the sensor entry is displayed in the Sensors table with these icons:

   - **State** - The icon "+" shows that the sensor entry was "Created".
   - Connected indicator (lightbulb) - Gray. It turns green when the sensor establishes the TLS tunnel to the NDR Indicator Management portal.
   - **xNDR-Managed** - The NDR application manages this Security Gateway.

10. Select the sensor entry (highlighted in blue) and select **Generate Registration Key** from the **Actions** menu.

    A new window opens with the registration key, for example:



11. Copy the registration key for use on the appliance.

Registering the Appliance

1. If the sensor requires an HTTPS proxy server to access the Internet:
   a. Configure the proxy server in Gaia OS in the Gaia Portal or with Clish.
   b. Run this command in Expert mode:

   ```
   export HTTPS_PROXY=http://<proxy ip/name>:<proxy port>
   ```

   For example:

   ```
   # export HTTPS_PROXY=http://local.proxy:8080
   ```

2. On the command line on the appliance, in the **Expert mode**, run this command with the "`<registration key>`" obtained from the NDR Indicator Management application portal in step 10 in the above procedure:

   ```
   curl_cli -f -s -S --cacert $CPDIR/conf/ca-bundle.crt
   https://portal.now.checkpoint.com/static/install.sh | bash
   /dev/stdin --token <registration key> --monitor eth1 --monitor
   eth2-01
   ```

Note - Configure at minimum one interface in monitor-mode. In the example above, the two interfaces `eth1` and `eth2-01` are set as monitor interfaces.

3. The appliance reboots automatically and connects to NDR with the registration key.
4. On the NDR Indicator Management application portal, the connected lightbulb turns green. The State icon then starts to rotate, which indicates policy installation. Finally, the State icon appears as a check mark - which means it is **Activated**.

Accessing the Sensor's Gaia Portal

When an NDR-Managed sensor is activated and connected, it can be monitored and controlled only from the NDR Indicator Management application portal.

A user on the domain where the sensor is registered can see the sensor's resource consumption status (CPU, memory, disk).

Go to the **MANAGEMENT** > **System Monitor** tab.

For a user with a Domain Administrator role:

Go to **MANAGEMENT** > **Sensors** tab's Actions menu: **OPEN GAIA PORTAL**.

When you select the sensor and click this option it opens the appliance's WebUI in a new browser tab. The administrator can change interface mappings, see appliance status, and install Jumbo Hotfix Accumulators.

Plans

Each NDR sensor is related to a **plan** that controls its behavior. An Initial-Plan is automatically created for each domain and connected with all new sensors. You can change this plan, create more plans, and associate different sensors with the applicable one.

In contrast to standard Check Point Security Gateways that implement access control and threat prevention, NDR focuses only on the latter. The NDR does not manage an access policy - all traffic is allowed if it is not detected as malicious. This simplifies security management very much, allowing for plug-and-play operation. The plan is, therefore, quite simple, defining these attributes:

- Threat Prevention – always enabled. It includes the IPS, Anti-Virus, and Anti-Bot blades.
- Extended Visibility – enabled by default. It includes the Application Control and URL Filtering blades.
- Prevent Mode – disabled by default (default is Detect Mode). Enabling Prevent Mode causes the sensor to block network traffic forwarded through the sensor's inline bridges if it is matched by one or more of the Threat Prevention blades with Medium or High confidence.

Note - An inline sensor blocks network traffic that match threat indicators with **Prevent**action, also when it is connected to a Detect Mode plan.

- Threat Extraction – disabled by default, only active for inline traffic.
- Threat Emulation – enabled by default. NDR uploads files extracted from the network to the cloud for static and dynamic analysis (sandboxing).
- Packet Capture – disabled by default, packet captures are created and attached to log records for packets matching a threat prevention detection.
- Identity Awareness and HTTPS Inspection – disabled by default and not editable. These settings show the status of the related services, which NDR cloud team provisions on request.

Example:

Setting up SNMP Monitoring on an NDR Sensor

This section describes how to set up SNMP monitoring on an NDR Sensor.

Step 1: Enable SNMP Monitoring in the NDR System

SNMP Monitoring must be enabled in the NDR system. To enable this feature, submit a request to the NDR Team: ndr@checkpoint.com.

Step 2: Configure Gaia SNMP

To enable and configure SNMP, follow the procedure used for any Check Point Gaia device (see the R81.20 Gaia Administration Guide for instructions).

Step 3: Configure a Static Route

To enable communication between the NDR Sensor and the NMS Server, create a static route.

1. To create a static route using Gaia portal or CLI, run this command:

   ```
   set static-route <nms_server_ip>/32 nexthop gateway address
   <gateway_ip> on
   ```

2. To apply the new static route, restart the Sensor's connection to the NDR Cloud with this command:

   ```
   vg cloud_disconnect
   ```

Step 4: Configure a Dynamic Object to allow SNMP traffic

The NDR Sensor uses an "SNMPSource" Dynamic Object for communication with the NMS server.

To create the "SNMPSource" Dynamic Object, run this command:

```
dynamic_objects -n SNMPSource -r <nms_server_ip> <nms_server_ip> -a
```

Note - The "`-r`" option accepts a range of IP addresses, so it is necessary to specify the IP address twice in the command.

Moving From Detect to Prevent

Overview

NDR blocks undesirable network traffic that bypassed other cyber defenses (presents as false negatives). The default operation mode is Detect, as most sensors are deployed passively with Monitor Mode interfaces. Prevent Mode on these sensors creates Prevent logs, but the traffic is not blocked as the sensor only inspects a mirror of the real network traffic.

This section details how to enable prevention based on NDR.

Prevention with Inline NDR Sensors

A physical NDR-Managed sensor deployed with inline interfaces prevents traffic flow through its bridged fail-open NICs.

To activate the inline sensor prevention:

1. Configure exceptions with action Prevent for protections that must apply even when in Detect Mode.
2. Edit the sensor's plan and enable Prevent Mode to set the default threat protection action to Prevent.
3. Set the action attribute for applicable threat indicators to Prevent.

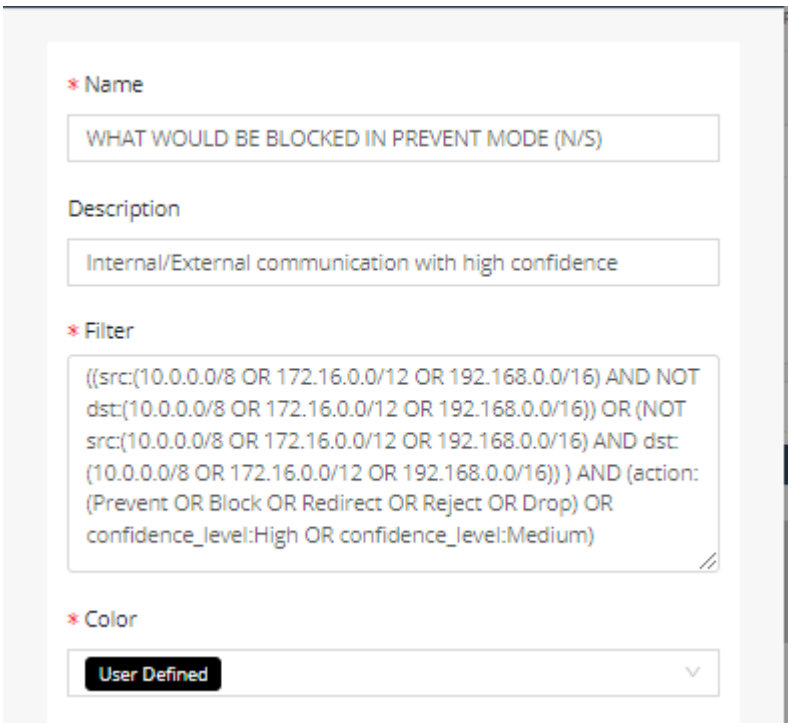
Note - Prevention is not applied in these situations:

- Bypass Mode – When the sensor is in Bypass On, network traffic through the sensor's fail-open NICs is not processed and cannot be detected or prevented.
- Monitor Mode interfaces – An inline appliance can have multiple Monitor Mode interfaces. Direct prevention is not supported for traffic received on these interfaces.

Determining what to block in Prevent Mode

To determine what to block, we recommend that you first review the traffic that is inspected in the default Detect Mode. Create exceptions to include any false positives that can influence business traffic.

For example, create a DOMAIN or PERSONAL view that matches such traffic:



Note that the IP ranges in this example are the primary default internal ranges. Your network may have different internal IP ranges. You must configure these internal ranges in the **MANAGEMENT** > **Settings** tab, specifying the ranges in CIDR format. In addition, this example assumes that the NDR sensor's inline bridge forwards traffic between the internal network and the Internet (North/South) and ignores East/West traffic. Your network may have a different configuration.

In some cases, for example, when under active attack, you may prefer to switch to Prevent Mode immediately and create the exceptions only after users complain that their traffic is blocked.

Exceptions

Use the **MANAGEMENT** > **Exceptions** tab to manage Threat Prevention exceptions. You can apply the exceptions on specific sensors or globally on all domain sensors. Create Threat Prevention rules to configure exceptions, and install a Threat Prevention policy on the sensors for every modification.

The exception attributes are similar to the ones found in SmartConsole application:

- Scope – Expressed as Sources or Destinations in CIDR notation. For an individual IP address, use /32.
- Protections or Blades – Select blade names from the pull-down menu or enter a protection name.
- Services – Select from the menu or enter the service name.

- Action – Changes the behavior of the selected protections or blades for the defined scope and services:
  - Prevent – Used in Detect Mode or to enable Prevent on Low confidence protections.
  - Detect – Used in Prevent Mode to cause the sensor to log but not block the specified traffic.
  - Inactive – Turns off the selected protections or blades.
- Track – Set to **None** when the action is Inactive.

Threat Prevention using Threat Indicators

For threat indicators managed on the INTEL tab you can select DETECT or PREVENT for the action. An NDR appliance uses Prevent to block network traffic with matching that are forwarded on its inline bridges. This block applies regardless if the plan is set to Detect or Prevent.

The indicators must be related to a data set that has **Apply on NDR Sensors** enabled (default). In addition, the indicators must be **Enabled** and not expired.

Threat indicators are the primary NDR response mechanism because they can be published to non-NDR-Managed Check Point Security Gateways and to 3rd party firewalls. This let you use NDR in a passive mode of operation and prevent threats indirectly.

You can manually create threat indicators from the NDR application user interface, load them from a file, or configure automated input feeds to pull them from external sources. In addition, NDR Behavioral Analytic AI engines automatically publish threat indicators to block detected high-risk traffic.

The default action for new manually-created indicators is DETECT. You can set the action to PREVENT during the initial entry or edit the indicators. You can edit individually or in bulk. For editing in bulk – select the indicators that you want to switch to PREVENT, select Bulk Edit, and set Action to **Prevent**. You can select the indicators and click **PREVENT**.

The default action is determined by the corresponding input feed's policy for automatically-created threat indicators. This policy applies only when the indicator value is first created. You can change the Action on existing indicators, and this new Action continues even if the input feed source refreshes the indicator.

For example, you can switch the Behavioral input feed action to Prevent for Medium and High confidence indicators. This input feed is created by default for all domains and represent the NDR Behavioral Analytic engines.

For more information on threat indicators, refer to the *NDR Indicator Management User Guide*.

Configuring Check Point Security Gateways to Pull NDR Indicators

You can easily configure your Check Point firewalls to pull feeds of threat indicators from NDR for blocking. It prevents threats automatically, with no need to policy push.

You can associate each indicator with one or more data sets, either manually or through the input feed policy. A data set is published on two output feed URLs: Prevent and Detect. Each of these feeds includes the indicators related to the data set that have the corresponding action (Prevent or Detect). This separation is useful because Check Point Security Gateways associate action with an individual feed configured on the Security Gateway.

The URL for each output feed is displayed on the portal and you can copy it to the clipboard with the **COPY URL** button. The **COPY FULL COMMAND** option runs the applicable "`ioc_feeds`" command on a Security Gateway to pull the output feed.

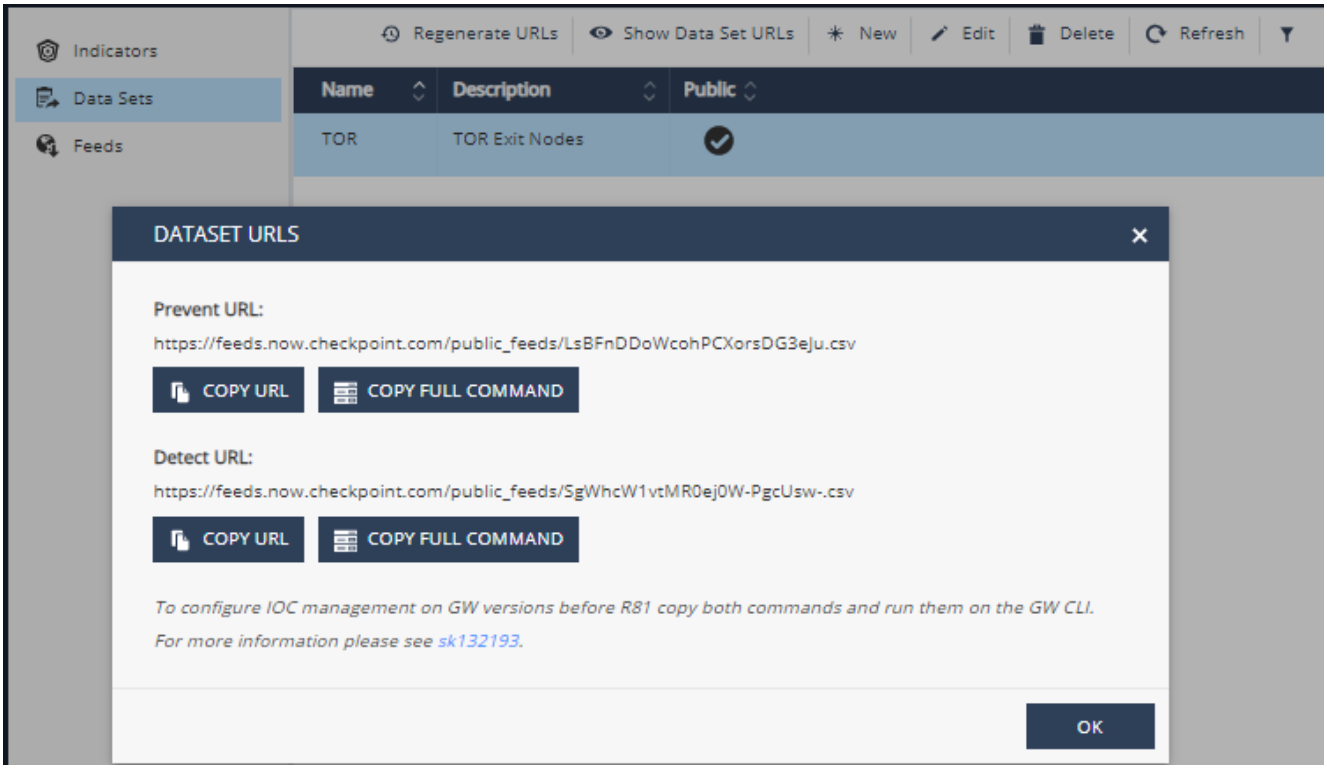
To enable a feed on the Check Point Security Gateway:

1. Select the desired data set (for example, Behavioral or TOR Exit Nodes).
2. Click **Show Data Set URLs**.
3. Click **COPY FULL COMMAND** for the set of indicators (DETECT or PREVENT).

   This puts the complete Security Gateway "`ioc_feeds`" command to the clipboard buffer.
4. Connect to the command line on the Security Gateway command line.
5. Log in to the Expert mode.
6. Paste and run the command.

Starting from R81.10 and higher, you can use the COPY URL option and configure the feeds from your SmartConsole. Go to **Security Policies** > **Threat Prevention** > **Indicators**.

For more information on how to enable this functionality on your Security Gateway, refer to sk132193.


Indicators
Data Sets
Feeds
Regenerate URLs
Show Data Set URLs
New
Edit
Delete
Refresh
Name
Description
Public
TOR
TOR Exit Nodes
DATASET URLS
Prevent URL:
https://feeds.now.checkpoint.com/public_feeds/LsBFnDDoWcohPCXorsDG3eJu.csv
COPY URL
COPY FULL COMMAND
Detect URL:
https://feeds.now.checkpoint.com/public_feeds/SgWhcW1vtMR0ej0W-PgcUsw-.csv
COPY URL
COPY FULL COMMAND
To configure IOC management on GW versions before R81 copy both commands and run them on the GW CLI.
For more information please see sk132193.
OK

NDR Log Server Registration

Overview

If you have a Check Point Log Server, you can use the Check Point Log Exporter (sk122323) to send your logs to the NDR Indicator Management application in addition to or instead of using dedicated NDR Sensors. The NDR application receives the Log Exporter configuration, downloads it to the Log Server, and executes it with one command.

Prerequisites

- The Log Server must run version R80.30 or higher.
- If you have a firewall, it must allow the appliance's Management interface to connect through TCP port 443 to these IP addresses: 35.156.213.136, 3.120.103.74, and 18.196.115.85 (for *NDR Portal*).
- The Log Server uses TLS to authenticate to the NDR application portal. Therefore, if you use HTTPS Inspection on the outbound path, you must create an exception for the log export traffic from the Log Server.
- You must create an HTTPS Inspection exception to access the *NDR Portal*.
- You must enable Extended Logging for the Application Control and URL Filtering blades on your Check Point Security Gateways. Other recommended blades include IPS, Anti-Bot, Anti-Virus, and Threat Emulation.

Configuring the Sensors in the NDR Application Portal

To configure the NDR sensors:

1. Log in to the *NDR Portal*.
2. Go to the **Customer Domain**.

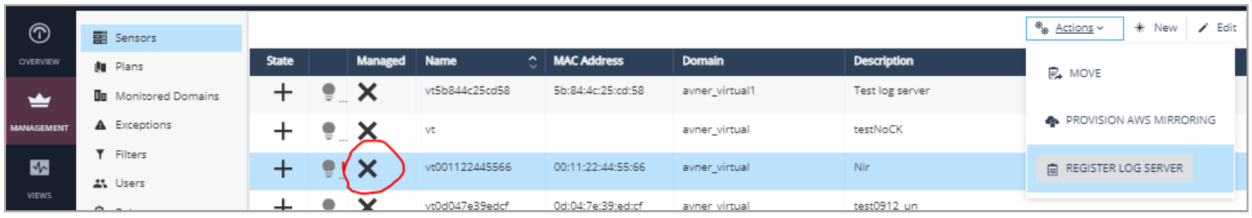
   If there are no sensors on the domain, it opens the **Sensors** tab.
3. From the left-hand menu, select **Management** > **Sensors** > click **New** (top middle).
4. To create an unmanaged sensor, clear the **NDR Managed** checkbox. Do not enter a MAC address.
5. Enter a description/name for the sensor. Select the correct time zone.

6. If the Log Server is a Multi-Domain Log Server, enable **Multi-Domain Log Server (MDS)** and enter the applicable Domain Log Server name and IP address.

   For each Domain Management Server on a Multi-Domain Security Management Server that is to be exported to NDR, you must assign an individual NDR sensor.

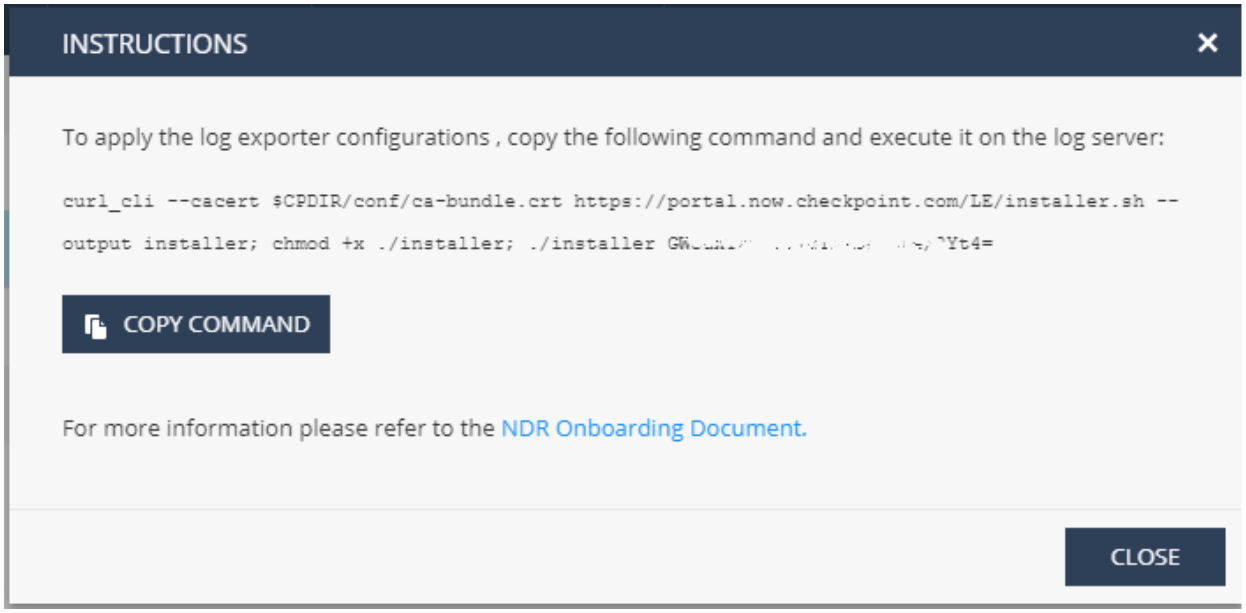
7. Click **ADD** in the lower right corner of the new sensor form.

8. Click on the new sensor entry you created and select **REGISTER LOG EXPORTER** from the **Actions** menu.



9. In the confirmation window, click **CONTINUE**.

10. Click **COPY COMMAND** to copy the personalized script to your clipboard:



Registering the Log Server

To register the Log Server:

1. Connect to the command line on the Log Server.
2. Log in to the Expert mode.
3. Paste the personalized script and click **Enter**.
4. The script executes and a "good day" message appears.

If an error message appears, contact *Check Point Support*.

5. When logs start to move to the NDR, the light bulb icon next to the sensor turns green:

Working with Amazon Web Services (AWS)

Overview

NDR automatically deploys a Check Point CloudGuard Network Security instance in Monitor Mode into your AWS VPC through an AWS CloudFormation stack. The stack registers Lambdas (serverless compute instances) that use cloud-native APIs to provision cloud vendor traffic mirroring, to selectively mirror network traffic for analysis and threat detection. The sensors do not require any configuration and do not affect the traffic flow.

Terminology

- VPC
- Region and Availability Zone (AZ)
- EC2
- Traffic Mirroring
- Elastic Network Interfaces (ENI)
- Elastic Load Balancing (ELB/NLB)
- Lambda
- CloudFormation
- CloudWatch
- Identity and Access Management (IAM)

If you are new to AWS, see Getting Started with AWS.

Scoping and Costs

Your AWS estate is allocated to accounts, regions, and VPCs. The Check Point NDR solution monitors network traffic between, into, and out of EC2 compute instances. Each EC2 instance is defined in one VPC and AZ and communicates with one or more ENIs.

NDR uses cloud-native AWS Traffic Mirroring to receive network traffic for inspection. A CloudGuard Network Security (CG NS) instance functions as an NDR sensor through the CloudFormation stack. An AWS Network Load Balancer (NLB) is used in addition in front of the CG NS. Traffic mirroring is configured for a specific VPC and AZ to the NLB when mirroring sessions are created from all ENIs that match a mirroring policy. The NLB routes the mirrored traffic to the NDR sensor.

Traffic Mirroring on a per-mirrored ENI basis costs approximately $11/month for each ENI. (Pricing varies across different AWS regions.)

Required Resources for the AWS Account

Step 1: Preparing your AWS account

1. Make sure you know which VPCs and AZs you mirror, and that you have sufficient IAM permissions to provision the NDR components. Missing permissions cause a failure in the environment, and error messages appear on the AWS Console.
2. Use the region selector in the navigation bar to select the AWS region where you want to deploy the NDR instance on AWS.
3. You must have an SSH key pair in your preferred region.
4. If necessary, request a service limit increase for the AWS resources that you plan to use. By default this guide uses:
    - c5.xlarge for the NDR instances
5. The NDR Indicator Management instance is deployed into an existing VPC with existing workloads. You must create two subnets for use by NDR. These subnets must be in the same Availability Zone in the region:
    - 1 internal subnet for the NDR Indicator Management instance's interface to receive traffic mirroring.
    - 1 external subnet with Internet access for the instance to send logs to the NDR Indicator Management portal.
6. The external subnet must present a route out to the Internet. If it is placed behind a network Security Gateway, the NDR instance can be allocated a local AWS IP address. Otherwise you must configure an Elastic IP (EIP) for the NDR instance for direct outbound access.

Step 2: Subscribing to CloudGuard Network Security in AWS Marketplace

To deploy a Check Point NDR Sensor, you must first subscribe your AWS account to Check Point CloudGuard Network Security:

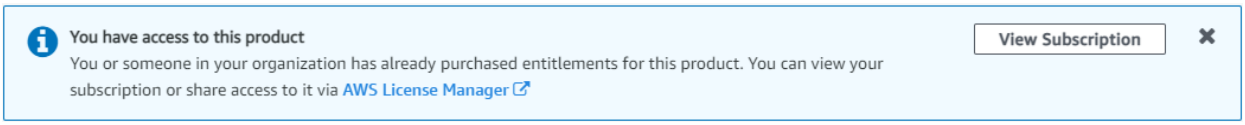
1. Log in to AWS Marketplace.

   Note - You must have AWS-marketplace "Subscribe IAM" permission.

2. Select the BYOL licensing option for the Check Point CloudGuard Network Security:

   See CloudGuard Network Security with Threat Prevention & SandBlast BYOL.

3. If the account is already subscribed, a message appears at the top of this AWS Marketplace page that the AWS account is already entitled:

4. If you are not subscribed, select **Continue** to subscribe.

5. Click **Accept Terms** to accept the AWS Marketplace license agreement.

Launch in AWS

After you complete all the preparations, you can continue to deploy the sensor.

1. Log in to the NDR portal and go to the Customer Domain.

   If there are no sensors on the domain, it opens on the **Sensors** tab.

2. From the left-hand menu, select **Management** > **Sensors** > Click **New** (top middle), then select **Virtual** and enter a name and a description for the sensor.

3. Select the correct time zone and click **ADD** in the lower right corner.

4. Select the new sensor entry and click **Actions** > **LAUNCH IN AWS**.

5. A registration key is created for the new virtual sensor and launches an AWS CloudFormation template in a new browser tab. You are redirected to log in to your AWS account.

Note - The NDR application portal does not receive or store customers AWS credentials.

NDR CloudFormation Template

1. **AWS General Configuration**

   Enter these parameters before you create the stack:

a. **Stack Name**: Automatically generated based on the sensor name. You can change this name to identify the sensors AZ.

   If you relaunch the stack due to an error, for example, missing IAM permissions, we recommend that you change this name to prevent resource collision in case the previous stack did not complete the automated clean up operations.

b. **VPC** where you want to deploy the NDR instance.

c. **Availability zone** - A NDR instance must be deployed in each monitored AZ to prevent AWS inter-AZ network traffic mirroring costs.

d. **AZ External subnet** - This subnet must have access to the Internet (directly or routed through other networks).

   In particular, the network must be able to pass TCP port 443 traffic to these IP addresses: 3.64.14.68 and 35.156.213.136. If there is an outbound proxy, it must exempt HTTPS traffic inspection to these addresses.

e. **AZ Internal subnet** - The mirrored traffic is delivered to an NDR instance's VXLAN endpoint on this subnet. It can be the same as the AZ External subnet.

Note - Make sure the selected subnets are compatible with the selected availability zone.

2. **NDR Sensor Configuration**

Enter these parameters before you create the stack:

a. **EC2 Instance type** - AWS instance size used for the NDR sensor instance.

   The default is **c5.xlarge**. A sensor that is too large has greater AWS costs. An undersized sensor provides reduced visibility because of uninspected connections and may in extreme cases become unstable and disconnect from the NDR Indicator Management back end.

   The primary sizing consideration is the volume of traffic mirrored to the sensor for inspection. See Appendix A for guidelines on how to estimate traffic volumes in AWS, with AWS CloudWatch.

   For a rough guide on how to select the instance type:

AWS instance type	c5.large	c5.xlarge	c5.2xlarge	c5.4xlarge	c5.9xlarge
# vCores	2	4	8	16	32
Max total traffic/sec	~0.5 Gbps	~1 Gbps	~2 Gbps	~4 Gbps	~8 Gbps

b. **EC2 key name** - AWS security key pair for SSH access to the NDR Indicator Management instance. Usually, this key is not used, but you must enter a key pair for the instance deployment. There is no default.

c. **Allocate EIP** - By default, this attribute is set to **No** as in most customer VPCs the NDR Indicator Management EC2 instance created on the AZ External subnet receives an internal AWS IP address and a default gateway for outbound connectivity. Set this to **Yes** if you must allocate the AWS Elastic IP on the instance for direct Internet access.

Procedure for Resizing an NDR Sensor on AWS

For an activated sensor (in v state), in case it is undersized or too large and it is necessary to change instance Type, follow these steps to relaunch it with the new size:

a. On AWS, remove the stack. This will clean up all resources consumed by the NDR Indicator Management solution.

b. On the Infinity NDR application portal - on the **MANAGEMENT** > **Sensors** tab

   i. Select the sensor entry (it shows as "Disconnected" - grey lightbulb icon)

   ii. Click on **Actions** > **X DEACTIVATE**

   iii. Click on **Actions** > **LAUNCH IN AWS**

c. Fill in the CloudFormation Template with the new parameters.

Note - We recommend that you make sure that the used stack is deleted before you launch the new one, or to manually change the stack name to prevent named collisions on deployed AWS resources.

3. **CG NDR Configuration - Advanced**

These parameters all have applicable default values, and it is not necessary to change them. They provide advanced NDR Sensor configuration.

a. **Expiration period** - Time after which the stack is automatically deleted. This releases all AWS resources allocated for this stack. Default is **No expiration**.

b. **Include EC2 Instances with the following tags (default all)** - Use to constrain the set of mirrored EC2 instances with a comma-separated list of Key=Value AWS tags.

c. **Exclude EC2 Instances with the following tags (default none)** - Use to further limit the set of mirrored EC2 instances.

d. **Monitor all ENIs** - For multi-homed EC2 instances, if you set this parameter to **No**, it monitors only the primary ENI.

e. **VXLAN ID** - VTEP number for mirroring sessions. Usually set to the default value of **1**.

f. **VPC scan interval** - Default is 10 minutes.

g. **Version** - Do not change.

h. **Registration key** - Do not change.

4. **Confirmation and Stack Creation**

   Examine the acknowledgment and click **Create stack**.

   The CloudFormation Template (CFT) spins up the NDR Indicator Management instance in your selected VPC and AZ, and runs two lambda functions that provision AWS traffic mirroring.

   It typically takes up to 20 minutes before you start seeing logs on the NDR application portal. The sensor's icon on the portal changes to a green light-bulb icon with a **v** status. You can track the CFT progress in the AWS Console, including any applicable error messages.

5. **AWS Resources Provisioned by the CFT**

   a. A security group is created for each ENI:

      - Internal ENI - Allow incoming vxlan (udp 4789), reject outbound.
      - External ENI - Allow incoming ssh/https (tcp 22/443), allow outbound.

   b. AWS Traffic Mirroring sources and sessions for each mirrored ENI.

   c. AWS Network Load Balancer (NLB), defined as the mirroring target, routes mirrored traffic to the NDR sensor instance on the defined VXLAN on the AZ Internal subnet.

   d. Two lambda functions automatically configure AWS traffic mirroring. An EC2 instance creation event on the VPC triggers its examination against the mirroring policy (include and exclude lists). In addition, the VPC is scanned on the defined scan interval, and any deleted EC2 instances result in clean up of the corresponding mirroring sources and sessions. EventBridge rules control these invocations.

   e. Elastic IP if enabled in the CFT.

   Note - If you remove the stack from the AWS Console - it removes all related resources in your VPC, including the NDR Indicator Management CloudGuard Network Security instance, the lambda functions, and the traffic mirroring sessions.

Mirroring More VPCs

The **LAUNCH IN AWS** CFT provisions traffic mirroring for a specified VPC and AZ, and mirrors the traffic to a Load Balancer and NDR Sensor.

There is an alternative **PROVISION AWS MIRRORING** CFT that does not create those two instances. Instead, it accepts the mirroring target as a parameter. It allows one deployed NDR sensor to mirror traffic from multiple VPCs. As long as the sensor and the mirrored traffic are defined in the same Availability Zone, there are no additional AWS costs related to inter-VPC or even inter-account traffic mirroring.

Note - We recommend that you do not mirror across AZ boundaries even though there is no technical limitation. AWS costs grow significantly if traffic is mirrored between different AZs.

To provision mirroring on a different VPC:

1. From the left-hand menu, select **Management** > **Sensors** > Click **New** (top middle), then clear **Managed** and enter a description/name for the sensor.
2. Select the correct time zone and click **ADD** in the lower right corner.
3. Select the new sensor entry and click **Actions** > **PROVISION AWS MIRRORING**.

   This step launches an AWS CloudFormation template in a new browser tab. It first redirects you to log in to the customer's AWS account. Enter your AWS account number and access credentials to log in to your AWS Console.
4. The CFT parameters are equivalent to those of LAUNCH IN AWS, with these exceptions:
   - As no sensor is deployed, the CFT omits these parameters: AZ External Subnet, AZ Internal Subnet, the entire CG NDR Configuration section, Version, Registration key
   - A Traffic Mirror Target parameter is added. Enter a NDR Indicator Management Load Balancers mirror target ID (for example 'tmt-xxxxxx').
5. Check the acknowledgment and click **Create stack**.

Traffic Mirroring Include/Exclude Lists

The NDR Indicator Management Cloud Formation template, which is deployed per sensor from the NDR portal, handles the traffic mirroring include and exclude lists. To include or exclude instances for traffic mirroring, enter comma-separated key-value pairs in the CFT, for example:

- MYTAG=DOMIRROR,MYOTHERTAG=INSTANCE.
- CKP_TYPE = Sensor

Apply these tags to each instance to include or exclude them from traffic mirroring.

To update your traffic mirroring include/exclude tags after initial CFT deployment, issue a CFT Stack update to revise the tags or to apply a different tag scan interval.

1. Find the CloudFormation Stack used to deploy your sensor, select the **Change Sets** tab, and click **Create Change Set**.
2. Select **Use the current template** and click **Next**.
3. Change the Include or Exclude tags as applicable, or change the VPC Scan interval, or both. Click **Next**.
4. Do not make any changes in the stack options and click **Next**.
5. At the review screen, examine all parameters, then acknowledge the stack capabilities and click **Create Change Set**.
6. Give the change set a name and click **Create Change Set** to make the changes to the applicable NDR sensors.

Sensor Deactivation on Stack Deletion

If you want to remove the Cloudformation Stack which deployed your NDR Sensor, and relaunch in AWS from the NDR application portal, you must first deactivate the sensor on the portal. This is because the NDR back end does not know if the sensor is deactivated, only that it is disconnected.

To deactivate the sensor:

1. On the **MANAGEMENT** > **Sensors** tab, select the applicable sensor.
2. From the **Actions** menu select **X DEACTIVATE**.

Users and Access Control

Domains

The **domain** is the basic object collection on NDR Indicator Management. All objects are connected to a domain. This includes sensors, logs, packet captures, indicators, views, insights, reports, etc.

Authorizations

Each domain defines a set of user authorizations that you can view and edit in **MANAGEMENT** > **Users**. A user's authorization on the domain defines a Role for the user's access to the domain.

Users

The first time a user authorizes to a domain, it creates a user object with the user's email address. The user is independent of any domain. The user's email address is used both for the user's unique identity and to communicate with the user, for example, for reports and notifications.

The user receives an email with a link. Clicking on the link provisions the user object and generates a certificate with the user's email address as the CN. This certificate is downloaded to the user's endpoint and installed with a user-defined security level.

When the user logs in with his certificate, the NDR application verifies the user's certificate, retrieves the user's domain authorizations, and matches them to the requested domain and service. Not approved requests are rejected. Authorized and unauthorized requests are audited and you can see them on the **MANAGEMENT** > **System Events** tab.

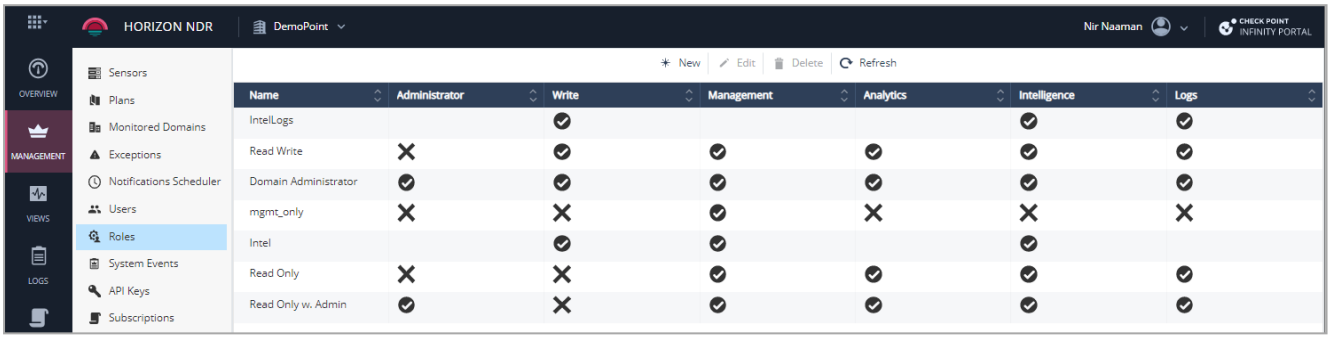
Note - Deleting a user record from **MANAGEMENT** > **Users** does not revoke the user's certificate – only the user's authorizations to the domain. If a user is left with no authorizations to any domain, the user account is eventually deleted by automated clean up services, and the user certificate revoked.

Note - A user with Write authorizations can invoke the **MANAGEMENT** > **Users** > **Actions** > **REISSUE CREDENTIALS** for a user. This sends an email with a reissue link to the target user's email address. If the user receives the email and clicks the link, a new certificate is generated for the user to download.

Roles

A Role defines a set of permissions to use NDR Indicator Management services. The **MANAGEMENT** > **Roles** tab shows the currently supported permissions:

- **Administrator** – User authorizations, monitored domains, and input feed management.
- **Write** – Modify objects on the domain.
- **Management** – Access the **MANAGEMENT** tab and its services.
- **Analytics** – Access the **VIEWS** and **INSIGHTS** tabs and their services.
- **Intelligence** – Access the **INTEL** tab and its services.
- **Logs** – Can see logs on the domain.



By default, each domain includes the **Read Only**, **Read Write**, and **Domain Administrator** roles. You can configure additional roles as needed.

For example, the Read Only role can access all tabs but cannot manage user authorizations or change any objects. The Intel role shows only the MANAGEMENT and INTEL tabs and can therefore only view and change indicators, not logs.

Monitored Domains

The monitored domain can be accessed by all approved users. The Domain Administrator can create a new domain from the **MANAGEMENT** > **Monitored Domains** tab. This creates a monitored subdomain for all the users approved to the monitored domain can access. The new domain is added to the domain drop-down menu.

The monitored domain defines the permissions that users approved to the monitoring domain receive on the monitored domain's objects. Effective permissions are the intersection (the minimum) of the user's permissions on the two domains.

For example, suppose domain X monitors domain Y with the Read Only role. if a user is approved as a Domain Administrator on X, he now has permissions to access Y's objects and services as a Read Only Domain Administrator. If the user is approved to X and Y, access to Y's objects and services is controlled through the more specific role assignment, which means the approval on the Y domain.

When the monitoring relationship is created in the context of the creation of a subdomain, the Domain Administrator role is used for the relationship.

Establishing a Monitoring Relationship between two Domains

You can create the monitoring relationship between any two domains even if the two domains were originally created independently. To do this:

1. Log in with a user that has Domain Administrator authorizations.
2. Click *** New** on the **MANAGEMENT** > **Monitored Domains** tab.
3. Specify a **Monitoring Domain Name**. It must match the monitoring domain's name fully.
4. Provide an **Email**, **First Name**, and **Last Name** for the contact person at the monitoring domain.
5. Select a **Role** for the monitoring relationship – this restricts the actions the monitoring domain's users can do on the current domain.
6. Click **SAVE**.
7. The request shows up on the monitoring domain. A Domain Administrator for that domain must click **Approve** on the request before it takes effect.

For example, to allow the Check Point Managed Detection and Response (MDR) service to monitor your domain, enter **Check_Point_MDR** as the Monitoring Domain Name. When the MDR team approves the monitoring request, the MDR service starts automatically with NDR APIs to pull insights and logs from NDR to MDR, and to supply threat indicators to enforcement points for prevention.

A Domain Administrator on either the monitoring or monitored domain can delete the relationship.

NDR Security Check-up Report

Overview

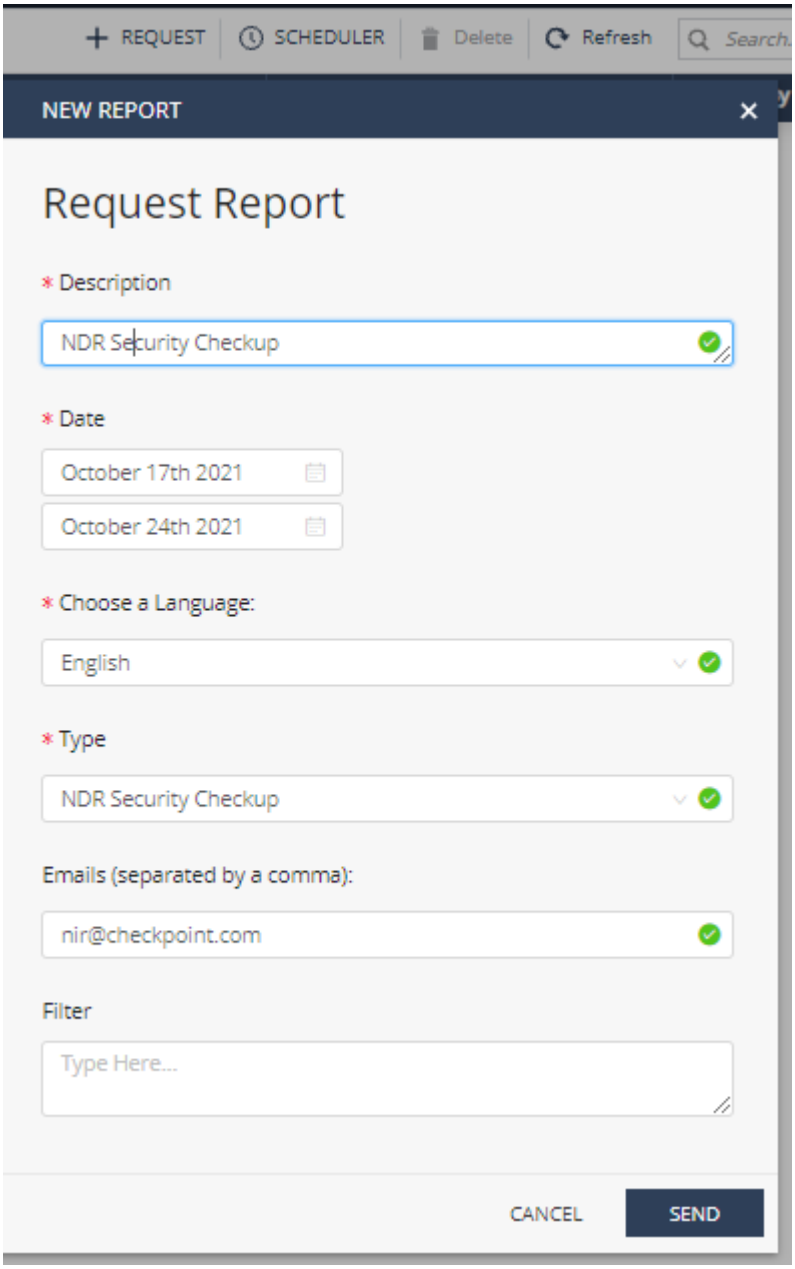
The NDR Web application lets users easily create a Security Check-up report and other more specialized reports.

When it is necessary, you can approve more users to see this information on the application.

After the NDR sensor completes activation, it starts to send logs generated by the different Check Point software blades. By default, these include Threat Prevention (Anti-Bot, Anti-Virus, IPS, Threat Emulation) and Access blades (Firewall, Application Control, URL Filtering). These logs stay on the customer's domain even after the sensor is deactivated.

Generating an NDR Report

1. Browse to the **Reports** tab.
2. Click **+ REQUEST** to submit a new report request.
3. Enter a **Description** for the report.
4. The **Date** range defaults to the last 7 days - this is typically sufficient for a Security Check-up.
5. Keep the **Language** setting as English - currently the only supported language.
6. Select the report **Type**: **NDR Security Checkup** or **Security Checkup - Advanced** (see below).
7. Enter your email address to send the report to.
8. Optionally enter a **Filter**. This is typically used to not include uninteresting data, or to focus on a specific part of the network.
9. Click **SEND** to send the report request.
10. After some minutes, you receive the report in your mailbox, and it is displayed in the Reports tab on the portal.



NDR Report Types for Security Check-up

- **Security Checkup - Advanced** -Includes the findings of a variety of security threats: malware infections, usage of high risk web applications, intrusion attempts, loss of sensitive data, etc.
- **NDR Security Checkup** - Customized and scoped report for NDR, that includes the findings of a security estimate conducted in your network leveraging AI insights and threat analytics.

Generating a Threat Topology Report

One of the advanced analytical tools on the NDR portal is the Threat Topology visualization. Threat Topology let you map network interactions and prioritize different event types.

To export a Threat Topology visualization for presentation out of the portal:

On **ANALYTICS** > **Threat Topology**, click **Export HTML** (bottom right)

This generates a report in HTML archive format, that you can send to the customer. Opening the report object provides an offline interactive experience that is equivalent to the one on the NDR application.

SPAN Port Configuration

HP/Aruba Switches

See: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=25100

1. Create the session and assign the local mirroring port (where your IDS is connected):

   ```
   mirror session-# port exit-port-# [name name-str]
   ```

   "`session-#`" is a value from 1 to 4.

   Example:

   ```
   mirror 1 port 11
   ```

2. Assign the monitored ports, vlans or mac addresses to any of the created local port mirroring sessions:

   - ```
     interface {port | trunk | mesh} monitor all {in | out | both} mirror {session-# | name-str} [{session-# | name-str}] [{session-# | name-str}] | [{session-# | name-str}] [no-tag-added]
     ```

     Example:

     ```
     interface 28 monitor all both mirror 1
     ```

     OR

   - ```
     vlan vid-# monitor all {in | out | both} mirror {session-# | name-str} [{session-# | name-str}] [{session-# | name-str}] [{session-# | name-str}]
     ```

     Example:

     ```
     vlan 32 monitor all both mirror 1
     ```

Cisco Switches

See: https://www.cisco.com/c/en/us/td/docs/switches/metro/me3600x_3800x/software/release/15-3_2_S/configuration/guide/3800x3600xscg/swSPAN.pdf

1. Enter the switch configuration mode:

   ```
   configure terminal
   ```

2. Create the monitoring session"

   ```
   monitor session {session_number} type local
   ```

   Example:

   ```
   monitor session 1 type local
   ```

3. Designate the source port with 'both' for ingress and egress"

   ```
   source interface interface_type {list(,) or give range(-) of interfaces} both
   ```

   Example:

   ```
   source interface gigabitethernet 2/1 both
   ```

4. Designate the destination port"

   ```
   destination interface interface_type {list(,) or give range(-) of interfaces} both
   ```

   Example:

   ```
   destination interface gigabitethernet 2/4
   ```

5. Enable the SPAN session"

   ```
   no shutdown
   ```

Complete Example:

```
Switch# configure terminal

Switch(config)# monitor session 1 type local

Switch(config-mon-local)# source interface gigabitethernet 2/1

Switch(config-mon-local)# destination interface gigabitethernet 2/4

Switch(config-mon-local)# no shutdown
```

Juniper Switches

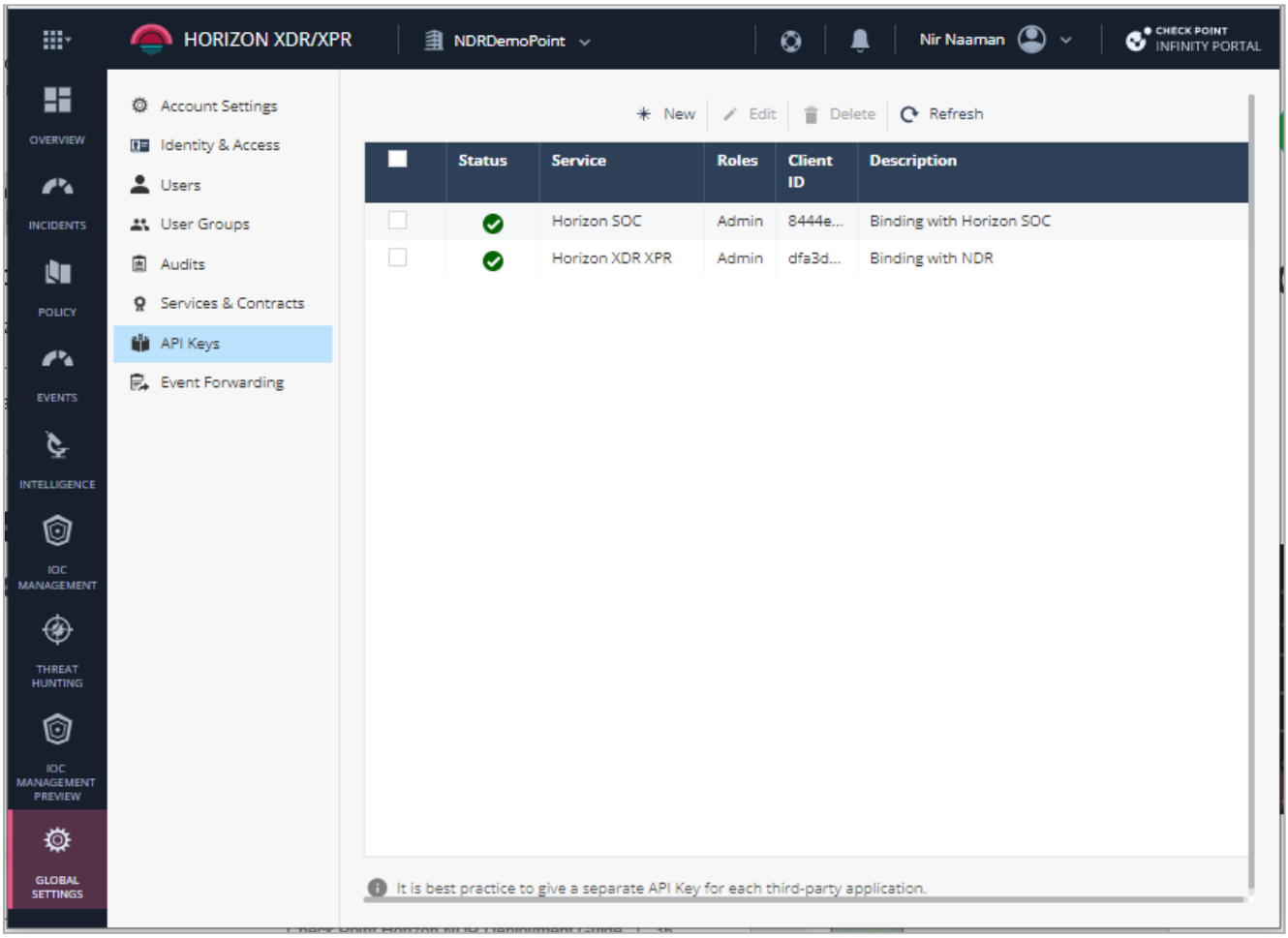
See: https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/port-mirroring-and-analyzers-configuring.html

Binding with Infinity XDR/XPR

Note: Infinity XDR/XPR is served from a different portal from NDR. It is published on the Infinity Portal: portal.checkpoint.com.

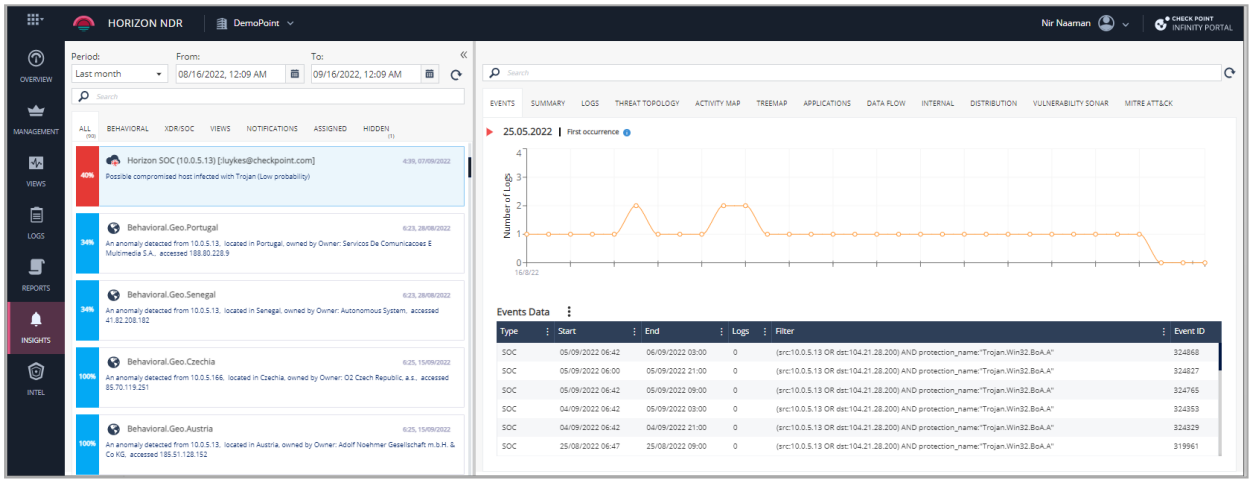
Creating a Infinity XDR/XPR API Key

1. Log in to the Infinity Portal and select Infinity XDR/XPR as the application.
2. On **GLOBAL SETTINGS** > **API Keys**, click *** New**, select **Infinity XDR/XPR** as the Service. Optionally: Enter a Description (for example. Binding with NDR Indicator Management).
3. Click **CREATE**.
4. Infinity XDR/XPR outputs two values: a Client ID, and an Access Key. Copy these values, as you cannot retrieve the Access Key after you close the window.

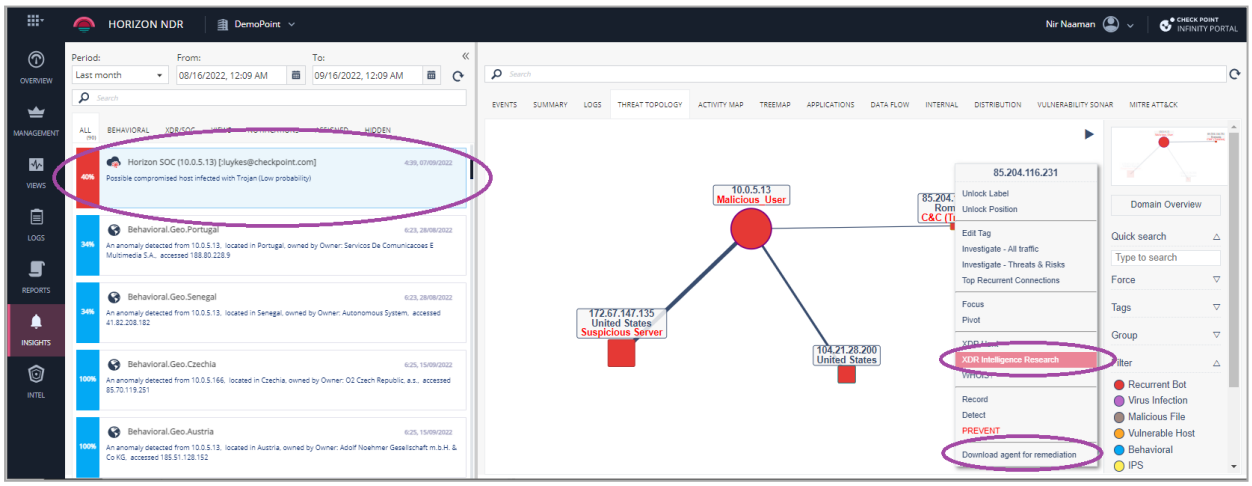


Importing the Infinity XDR/XPR API Key into NDR Indicator Management

1. Log in to the NDR Indicator Management application portal and open the customer domain.
2. On the **MANAGEMENT** > **API Keys** tab, click *** New**, select **Infinity XDR/XPR** as Type, and enter the Client ID and Access Key that you copied from the Infinity XDR/XPR.
3. NDR pulls the Infinity XDR/XPR's outputs automatically and adds to NDR's native Behavioral Analytics AI engines. This let you visualize incidents in context with NDR's advanced threat visualization capabilities.



4. In addition, NDR let you pivot back to Infinity XDR/XPR for ThreatCloud and Open Source investigation.



NDR Limitations

- NDR only supports sensors that can run Check Point version R81.10 or R81.20.
- Quantum Spark appliances (Gaia Embedded) are not supported.
- Cluster mode is not supported for dedicated NDR sensors.
- AWS traffic mirroring does not support some non-Nitro EC2 instance types. For more AWS limitations, review the Traffic Mirroring limitations article from the AWS site.

Glossary

A

AI
Artificial Intelligence

AWS
Amazon® Web Services. Public cloud platform that offers global compute, storage, database, application and other cloud services.

AZ
Availability Zone

B

BYOL
Bring Your Own License

C

C&C
Command and Control

CDC
Cyber Defense Center

CF
Cloud Formation

CFT
CloudFormation template

CG
CloudGuard

CGN
CloudGuard NDR

CGNDR
CloudGuard Network Detection and Response

CGNS
CloudGuard NDR Sensor

CHKP
Check Point

CIDR
Classless Inter-Domain Routing

CPG
Check Point Graph

CPU
Central Processing Unit

CSV
Comma Separated Value

E

EC2
Elastic Compute Cloud

EDR
Endpoint Detection and Response

ENI
Elastic Network Interface

F

FONIC
Fail-Open Network Interface Card

G

GW
Gateway

H

HD
Hard Drive

HTML
HyperText Markup Language

I

ID
Identifier

IDS
Intrusion Detections System

IoC
Indicator of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IRT
Incident Response Team

IT
Information Technology

L

L2
Layer 2

M

MAC ID
Media Access Control Identifier

MDR
Managed Detection and Response

N

NDR
Network Detection and Response

NIC
Network Interface Card

R

RAM
Random Access Memory

S

SaaS
Security as a Service

SGW
Security Gateway

SOC
Security Operations Center

SSL
Security Socket Layer

STIX
Structured Threat Information eXpression™

SUM
Summary

T

TAXII
Trusted Automated eXchange of Indicator Information™

TI
Threat Indicator

TIP
Threat Intelligence Platform

U

UI
User Interface

URL
Uniform Resource Locator

V

vCore
Virtual Core

VPC
Virtual Private Cloud