QUANTUM

27 June 2024

QUANTUM IOT PROTECT

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

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
27 June 2024	Added how to add IoT assets from third-party discovery engines (external vendors) through APIs. See *"Appendix I - Integrating IoT Assets using Third-Party Discovery Engines through APIs" on page 162*.
24 May 2024	Added how to assign risk level to IoT assets with default credentials in IoT Risk Profile. See *"Default Credentials" on page 61*.
15 March 2024	Updated the procedure to attach a contract to the product in *"Accessing the Quantum IoT Protect Administrator Portal" on page 14*.
14 February 2024	Added how to configure retention period for inactive assets in *"IoT Configuration Profile" on page 61* and *"Assets" on page 35*.
29 January 2024	Added the procedure to onboard Quantum IoT Protect on Quantum Maestro Security Group. See *"Appendix K - Onboarding Quantum IoT Protect on Quantum Maestro Security Group" on page 171*.
05 January 2024	Updated screenshots in *"Appendix C - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory)" on page 89*.
19 December 2023	Added **MikroTik CRS317** to the supported SNMP servers in *"Appendix B - Using SNMP as the IoT Discovery Engine" on page 78*.
01 December 2023	Added **HPE Networking Comware Switch** to the supported SNMP servers in *"Appendix B - Using SNMP as the IoT Discovery Engine" on page 78*.
15 November 2023	Updated the procedure in *"Disabling Quantum IoT Protect" on page 74*: Added a step to remove the IoT policy from SmartConsole.
02 November 2023	Updated the commands in *"Troubleshooting the SNMP- IoT Discovery Integration" on page 86*.
31 October 2023	Updated the procedures in: ▪ *"Appendix B - Using SNMP as the IoT Discovery Engine" on page 78*. ▪ *"Appendix E - Using Unix DHCP - Syslog as the IoT Discovery Engine" on page 115*. ▪ *"Appendix H - Using Infoblox DHCP - Syslog as the IoT Discovery Engine" on page 154*. ▪ *"Appendix G - Using Cisco ISE as the IoT Discovery Engine" on page 143*.

Date	Description
19 October 2023	Added the prerequisite for default Expert mode when you connect to Check Point Security Gateway through SSH: ■ See *"Prerequisites" on page 90* in Appendix C - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory). ■ See *"Prerequisites" on page 130* in Appendix F - Using Unix DHCP as the IoT Discovery Engine.
05 October 2023	Updated the procedures in: ■ *"Appendix C - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory)" on page 89*. ■ *"Appendix F - Using Unix DHCP as the IoT Discovery Engine" on page 129*.
27 September 2023	Updated *"Disabling Quantum IoT Protect" on page 74*.
17 August 2023	■ Updated the prerequisites in *"Integrating SmartConsole with Quantum IoT Protect" on page 18*. ■ Added procedure for *"Disabling Quantum IoT Protect" on page 74*.
24 May 2023	■ Added: • *"IoT Risk Profile" on page 59* in Profiles. • *"Threat Prevention" on page 48* in Zones. ■ Added note to enable Identity Awareness in *"Integrating SmartConsole with Quantum IoT Protect" on page 18*.
20 April 2023	Updated script for SNMP v2c in *"Troubleshooting the SNMP- IoT Discovery Integration" on page 86*.
05 April 2023	Added steps to run discovery on Management Server and Gateways in *"Setting Up SNMP - IoT Discovery Integration" on page 81*.
14 March 2023	Added High level Workflow steps to *"Getting Started" on page 14* and removed High level Workflow section.

Date	Description
27 February 2023	Added these sections: - *"Specific Service Roles" on page 16*. - *"Firmware Scan" on page 54*. Updated these sections: - *"Introduction to Quantum IoT Protect" on page 12*. - *"Profiles" on page 58*. - *"Agents" on page 64*.
25 January 2023	Updated screenshots for bash script in *"Appendix B - Using SNMP as the IoT Discovery Engine" on page 78*.
16 January 2023	Updated location in the bash script in *"Appendix B - Using SNMP as the IoT Discovery Engine" on page 78*.
21 November 2022	First release of this document.

Table of Contents

Introduction to Quantum IoT Protect

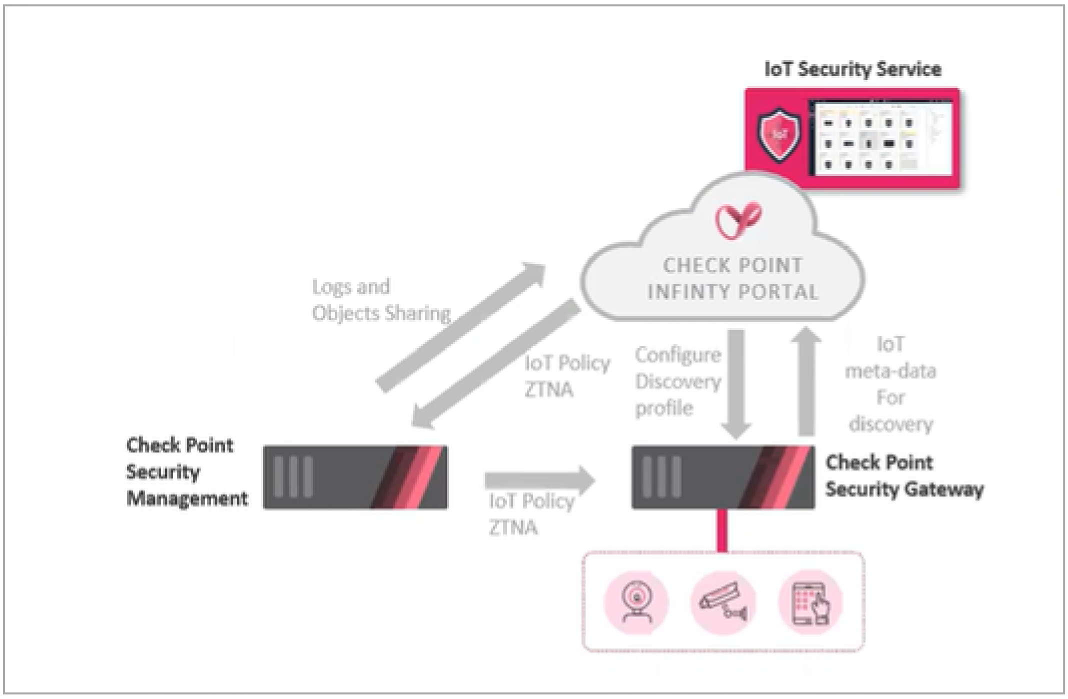
Check Point Quantum IoT Protect secures your network's Internet of Things (IoT) assets from cyber-attacks. Quantum IoT Protect protects only the IoT assets (for example, IP cameras, Smart TVs, Printers and so on) that are discoverable by the Check Point Security Gateway and managed by the Check Point Security Management Server. It connects to the Check Point Security Gateway to discover the IoT assets in your network and uses the Check Point Security Management Server to enforce the security policies for the IoT assets.

Quantum IoT Protect:

- Automatically discovers IoT assets in your network.
- Allows you to enforce security policies on the IoT assets.
- Provides autonomous Zero Trust Network Access (ZTNA) protection.

How it Works

When you integrate Quantum IoT Protect with your Check Point Quantum Security Gateway, it automatically creates the profiles necessary to discover IoT assets connected to the Security Gateway. During the integration, an agent is installed on the Security Gateway to collect and share the assets' meta data with Quantum IoT Protect. IoT policies are generated from the Infinity Portal, sent to the Security Management Server and then enforced on the Security Gateway.


IoT Security Service
CHECK POINT INFINTY PORTAL
Logs and Objects Sharing
IoT Policy ZTNA
Configure Discovery profile
IoT meta-data For discovery
Check Point Security Management
IoT Policy ZTNA
Check Point Security Gateway

Supported Security Gateways and Security Management Servers

Quantum IoT Protect is supported on these Security Gateways and Security Management Servers:

Gateway / Server	Supported Version
Security Gateways	
Security Gateways in the Gateway mode	R81.20 and higher
Cluster of Security Gateways	R81.20 and higher
Quantum Spark Appliances	
Quantum Spark Appliances	R81.10.00 and higher
Cluster of Quantum Spark Appliances	R81.10.00 and higher
Security Management Server	
Security Management Server	R81.20 and higher
Multi-Domain Security Management Server	R81.20 and higher
Scalable Platforms (Maestro and Chassis)	R81.20 and higher

Limitations

Quantum IoT Protect does not support:

- Security Gateways in the Virtual System Extension (VSX) mode
- IPv6 enforcement and discovery

Getting Started

To get started with Quantum IoT Protect:

1. Create an account in the Infinity Portal.
2. Access the Quantum IoT Protect Administrator Portal.
3. License the product.
4. Assign specific service roles to users.
5. Integrate SmartConsole with Quantum IoT Protect.
6. Onboard IoT Assets in Quantum IoT Protect.
7. Manage IoT Assets in Quantum IoT Protect.

Creating an Account in the Infinity Portal

Check Point Infinity Portal is a web-based interface that hosts the Check Point security SaaS services.

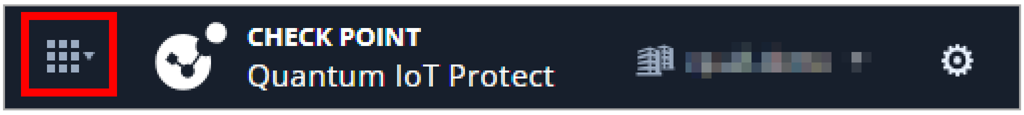
With Infinity Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Infinity Portal account, see the Infinity Portal Administration Guide.

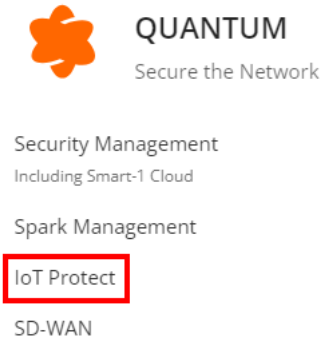
Accessing the Quantum IoT Protect Administrator Portal

To access the Quantum IoT Protect Administrator Portal:

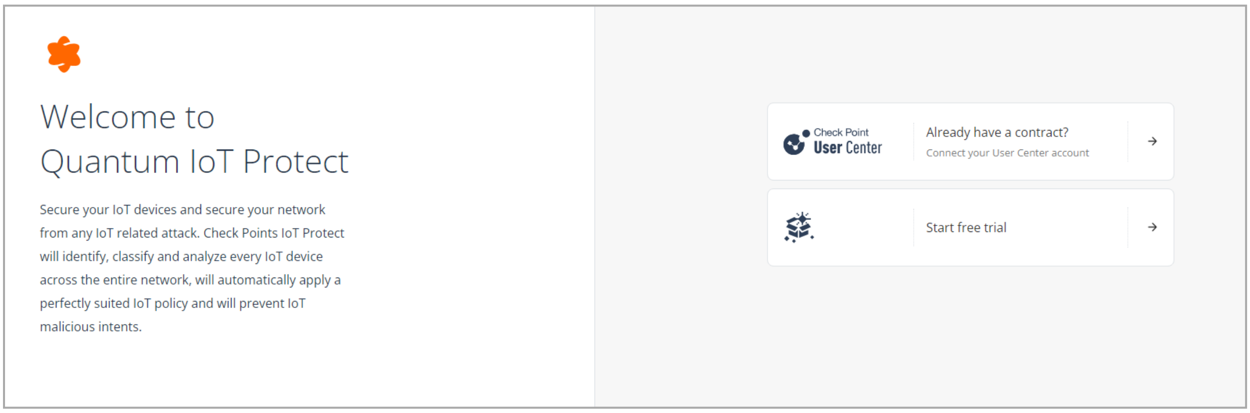
1. Sign in to the *Check Point Infinity Portal*.
2. Click the **Menu** icon in the top left corner.



3. In the **Quantum** section, click **IoT Protect**.



4. If you are accessing the portal for the first time, do one of these:



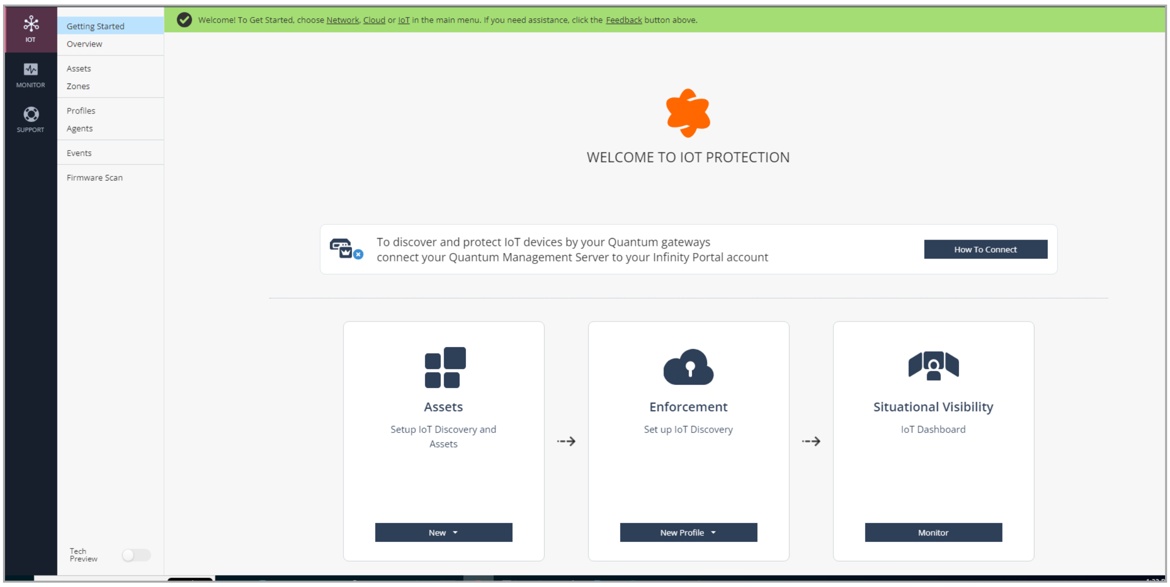
Welcome to
Quantum IoT Protect

Secure your IoT devices and secure your network from any IoT related attack. Check Points IoT Protect will identify, classify and analyze every IoT device across the entire network, will automatically apply a perfectly suited IoT policy and will prevent IoT malicious intents.

- If you already have a Check Point contract, click **Already have a contract** to attach the contract to the product. For more information, see **Associated Accounts** in the *Infinity Portal Administration Guide*.

- If you want to trial the product, click **Start free trial**.

  The IoT Protect **Getting Started** page appears.



Welcome! To Get Started, choose Network, Cloud or IoT in the main menu. If you need assistance, click the Feedback button above.

WELCOME TO IOT PROTECTION

To discover and protect IoT devices by your Quantum gateways connect your Quantum Management Server to your Infinity Portal account

Note - This starts your Quantum IoT Protect trial. To use the service after the trial period, you must purchase a license. For more information, see *"Licensing the Product" below*.

If you have already attached the contract with the product, the IoT Protect **Getting Started** page appears.

Licensing the Product

When you create an account in the Infinity Portal and access the service, you get a free trial version valid for 30 days. After the 30-day trial period, you must purchase a software license to continue to use the product. To purchase a license, you must create a Check Point User Center account. For instructions, see sk22716.

After you create a User Center account, contact your Check Point sales representative to purchase a license.

If you have already licensed the product, you can view your current contract (license) information from the **Infinity Portal** > **Global Settings** > **Contracts** page.

Specific Service Roles

Quantum IoT Protect supports specific service roles in Horizon Policy. For more information, see Specific Service Roles in the *Infinity Portal Administration Guide*.

To access Specific Service Roles:

1. Go to **Global Settings** > **Users** > **New** > **Add User**.
2. Expand **Specific Service Roles** > **Horizon Policy**.

Service Roles	Description
Admin	Can read and modify every administrative setting.
Read-Only	Provides full visibility across your Infinity account.

Integrating SmartConsole with Quantum IoT Protect

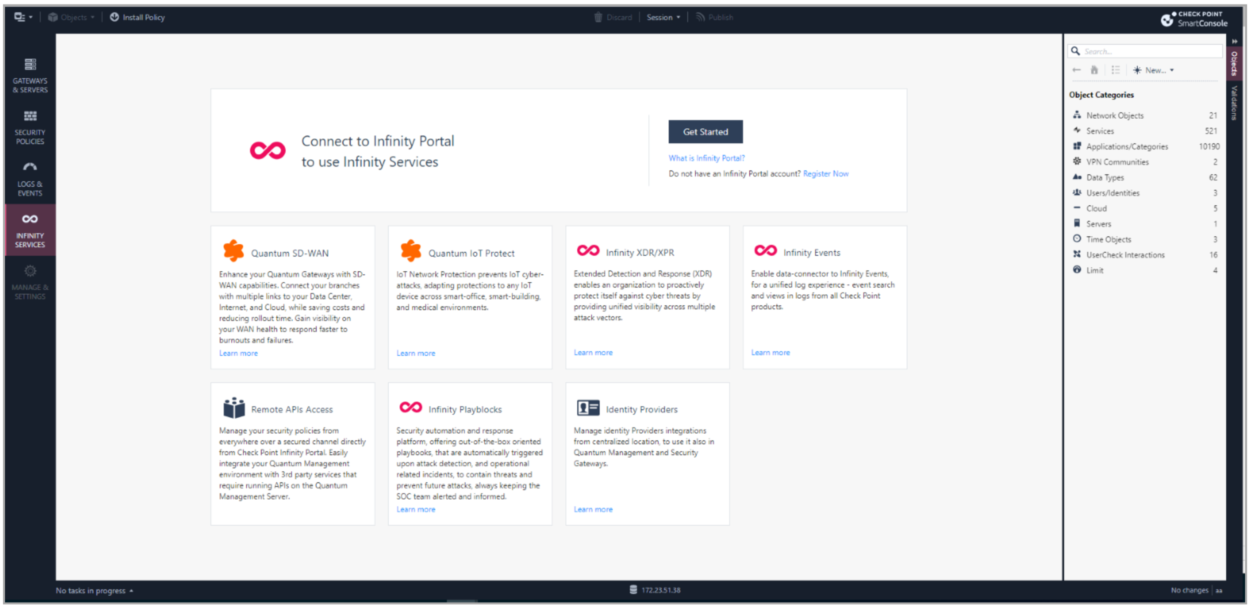
Prerequisites

- To install IoT policies on a Centrally Managed Quantum Spark Appliance, you must enable the Identity Awareness (IDA) Software Blade in the Security Gateway object. To enable IDA, follow the instructions in sk180475.
- If your Check Point Management Server is protected by a third-party firewall:
  - Add these domains as trusted on the firewall:
    - *.checkpoint.com
    - *.amazontrust.com
    - http://s.ss2.us/r.crl
  - Allow access to the services listed in sk179105.

Procedure

To integrate SmartConsole with Quantum IoT Protect:

1. In the SmartConsole, navigate to the **Infinity Services** menu, and click **Get Started**.



Connect to Infinity Portal to use Infinity Services

Do not have an Infinity Portal account? Register Now

Quantum SD-WAN: Enhance your Quantum Gateways with SD-WAN capabilities. Connect your branches with multiple links to your Data Center, Internet, and Cloud, while saving costs and reducing rollout time. Gain visibility on your WAN health to respond faster to burnouts and failures.

Quantum IoT Protect: IoT Network Protection prevents IoT cyber-attacks, adapting protections to any IoT device across smart-office, smart-building, and medical environments.

Infinity XDR/XPR: Extended Detection and Response (XDR) enables an organization to proactively protect itself against cyber threats by providing unified visibility across multiple attack vectors.

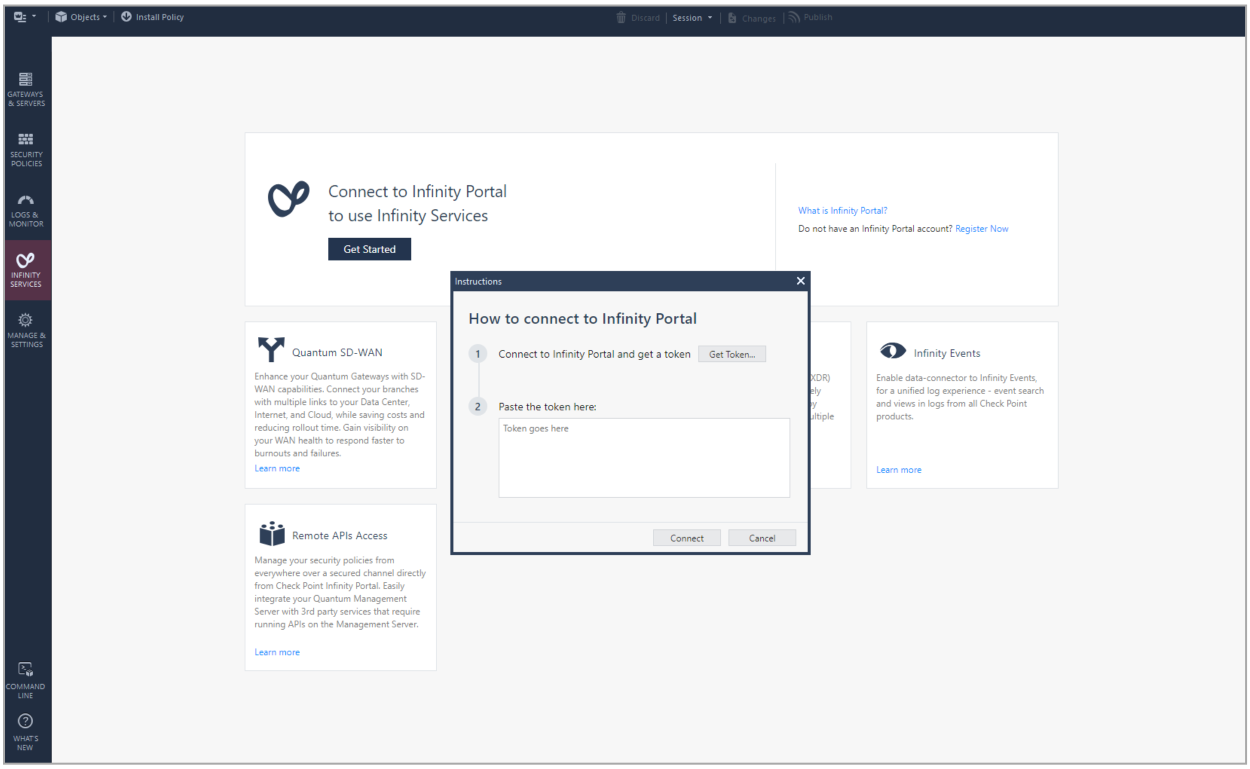
Infinity Events: Enable data-connector to Infinity Events, for a unified log experience - event search and views in logs from all Check Point products.

Remote APIs Access: Manage your security policies from everywhere over a secured channel directly from Check Point Infinity Portal. Easily integrate your Quantum Management environment with 3rd party services that require running APIs on the Quantum Management Server.

Infinity Playblocks: Security automation and response platform, offering out-of-the-box oriented playbooks, that are automatically triggered upon attack detection, and operational related incidents, to contain threats and prevent future attacks, always keeping the SOC team alerted and informed.

Identity Providers: Manage identity Providers integrations from centralized location, to use it also in Quantum Management and Security Gateways.

2. In the **Instructions** window, click **Get Token**.



Connect to Infinity Portal
to use Infinity Services

What is Infinity Portal?

Do not have an Infinity Portal account? Register Now

Instructions

How to connect to Infinity Portal

1 Connect to Infinity Portal and get a token

2 Paste the token here:

Token goes here

Quantum SD-WAN

Enhance your Quantum Gateways with SD-WAN capabilities. Connect your branches with multiple links to your Data Center, Internet, and Cloud, while saving costs and reducing rollout time. Gain visibility on your WAN health to respond faster to burnouts and failures.

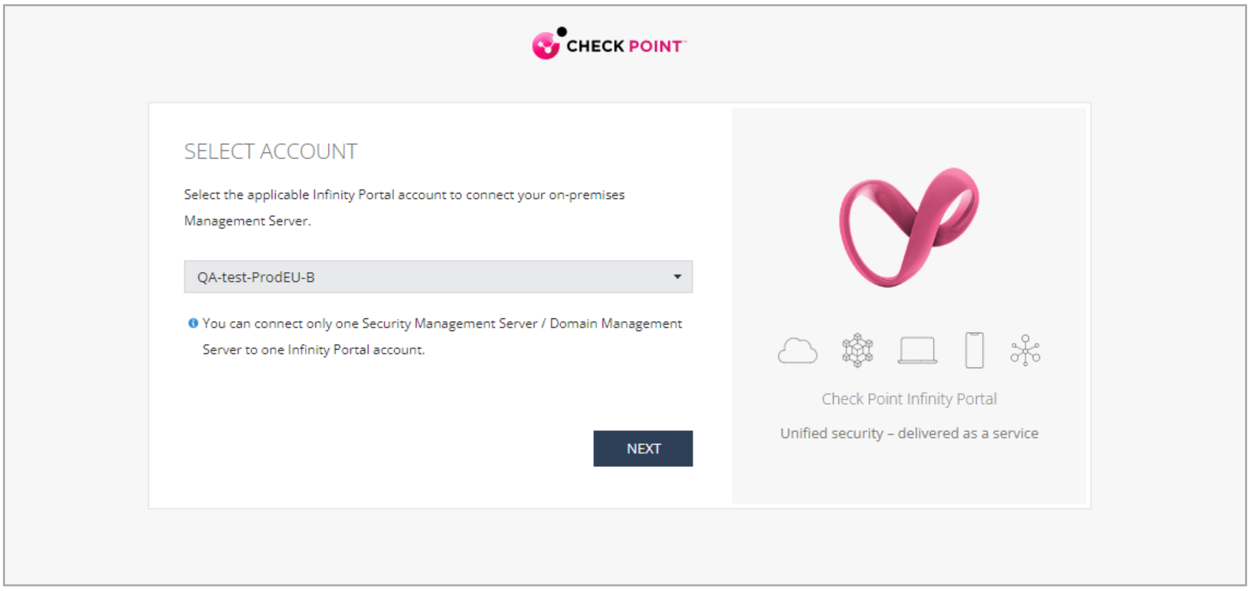
Infinity Events

Enable data-connector to Infinity Events, for a unified log experience - event search and views in logs from all Check Point products.

Remote APIs Access

Manage your security policies from everywhere over a secured channel directly from Check Point Infinity Portal. Easily integrate your Quantum Management Server with 3rd party services that require running APIs on the Management Server.

3. Select the registered account and click **Next**.


CHECK POINT
NEXT
Check Point Infinity Portal
Unified security – delivered as a service

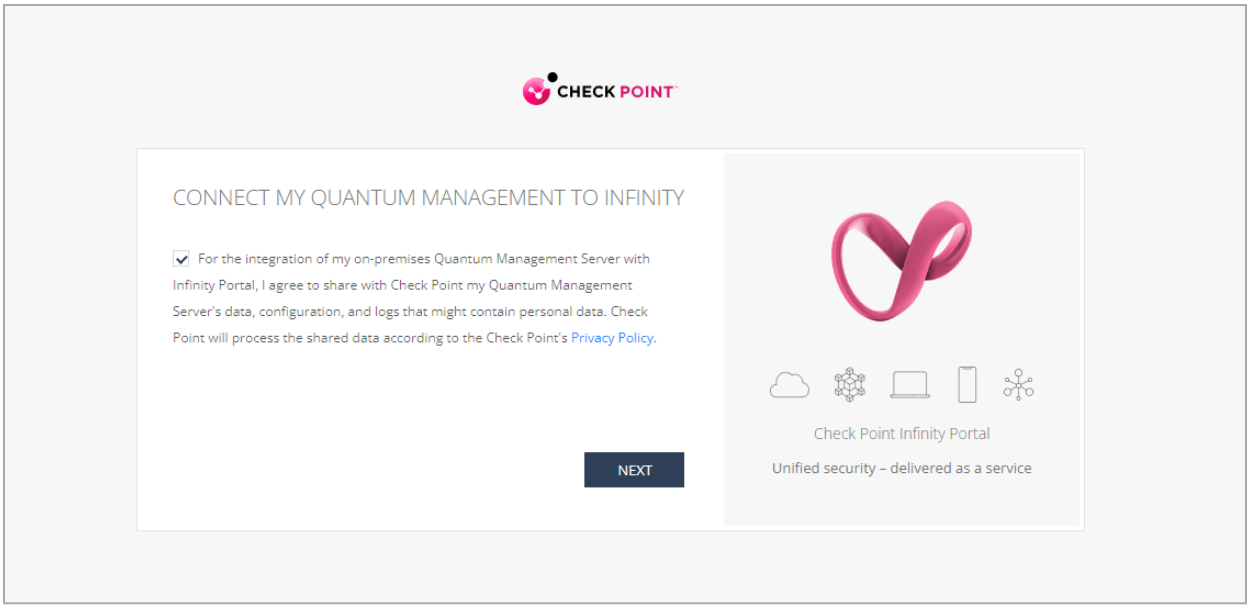
SELECT ACCOUNT

Select the applicable Infinity Portal account to connect your on-premises Management Server.

QA-test-ProdEU-B

You can connect only one Security Management Server / Domain Management Server to one Infinity Portal account.

4. Accept the terms of service and click **Next**.

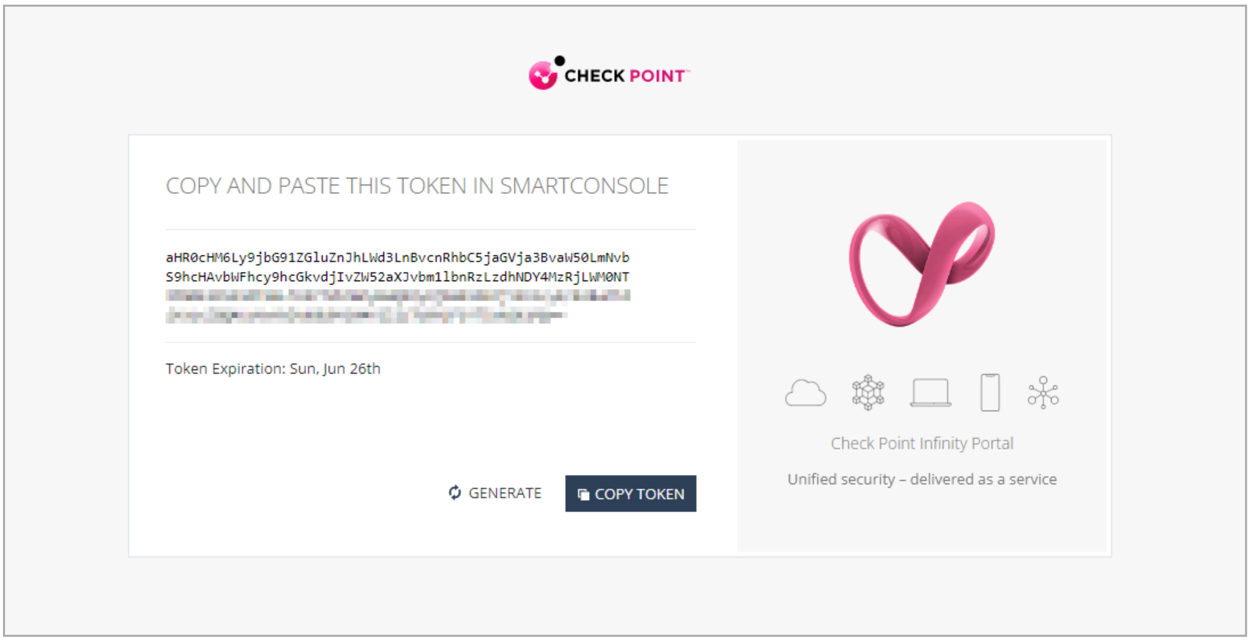


CONNECT MY QUANTUM MANAGEMENT TO INFINITY

☑ For the integration of my on-premises Quantum Management Server with Infinity Portal, I agree to share with Check Point my Quantum Management Server's data, configuration, and logs that might contain personal data. Check Point will process the shared data according to the Check Point's Privacy Policy.

NEXT
Check Point Infinity Portal
Unified security – delivered as a service

5. Click **Copy Token**.



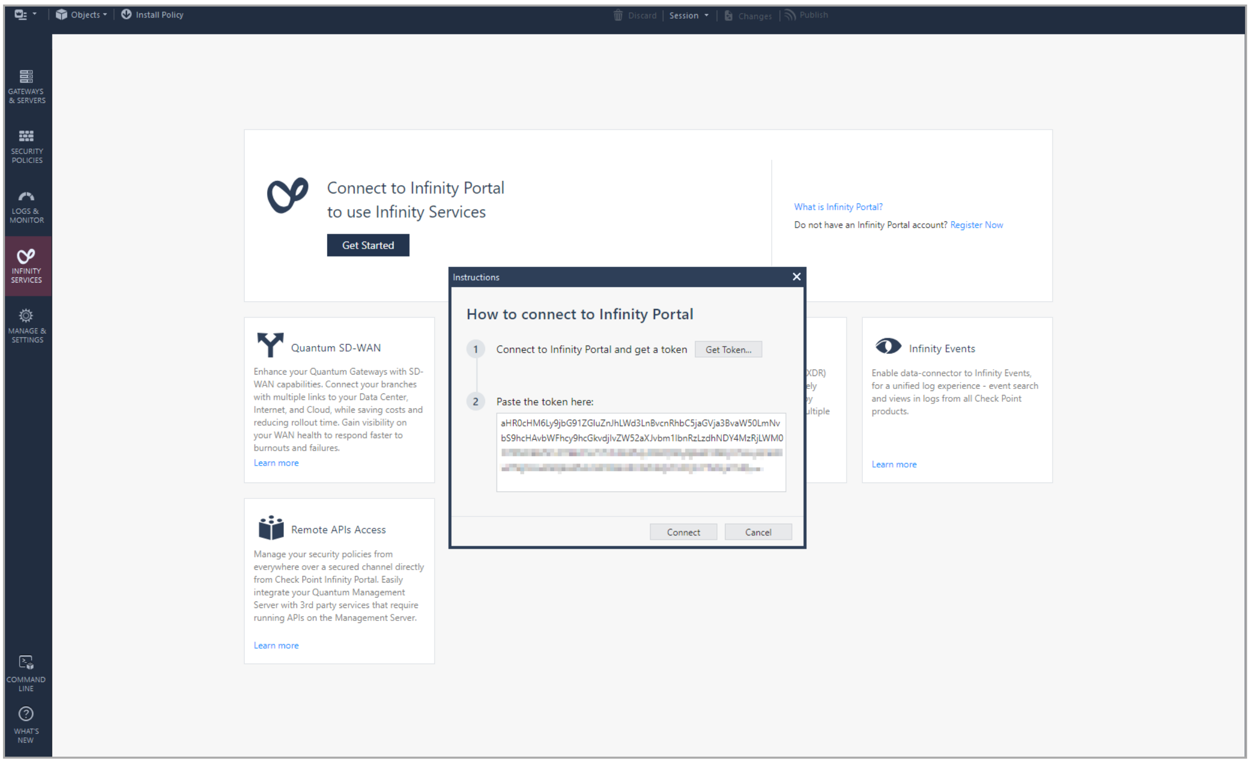
COPY AND PASTE THIS TOKEN IN SMARTCONSOLE

```
aHR0cHM6Ly9jbG91ZGluZnJhLWd3LnBvcnRhbC5jaGVja3BvaW50LmNvb
S9hcHAvbWFhcy9hcGkvdjIvZW52aXJvbm1lbnRzLzdhNDY4MzRjLWM0NT
```
[redacted]

Token Expiration: Sun, Jun 26th

GENERATE
COPY TOKEN
Check Point Infinity Portal
Unified security – delivered as a service

6. In the **Instructions** window, paste the token and click **Connect**.



Connect to Infinity Portal to use Infinity Services

Do not have an Infinity Portal account? Register Now

How to connect to Infinity Portal

1 Connect to Infinity Portal and get a token

2 Paste the token here:

aHR0cHM6Ly9jbG91ZGluZnJhLWd3LnBvcnRhbC5jaGVja3BvaW50LmNv
bS9hcHAvbWFhcy9hcGkvdjIvZW52aXJvbm1lbnRzLzdhNDY4MzRjLWM0
[redacted]

Quantum SD-WAN

Enhance your Quantum Gateways with SD-WAN capabilities. Connect your branches with multiple links to your Data Center, Internet, and Cloud, while saving costs and reducing rollout time. Gain visibility on your WAN health to respond faster to burnouts and failures.

Infinity Events

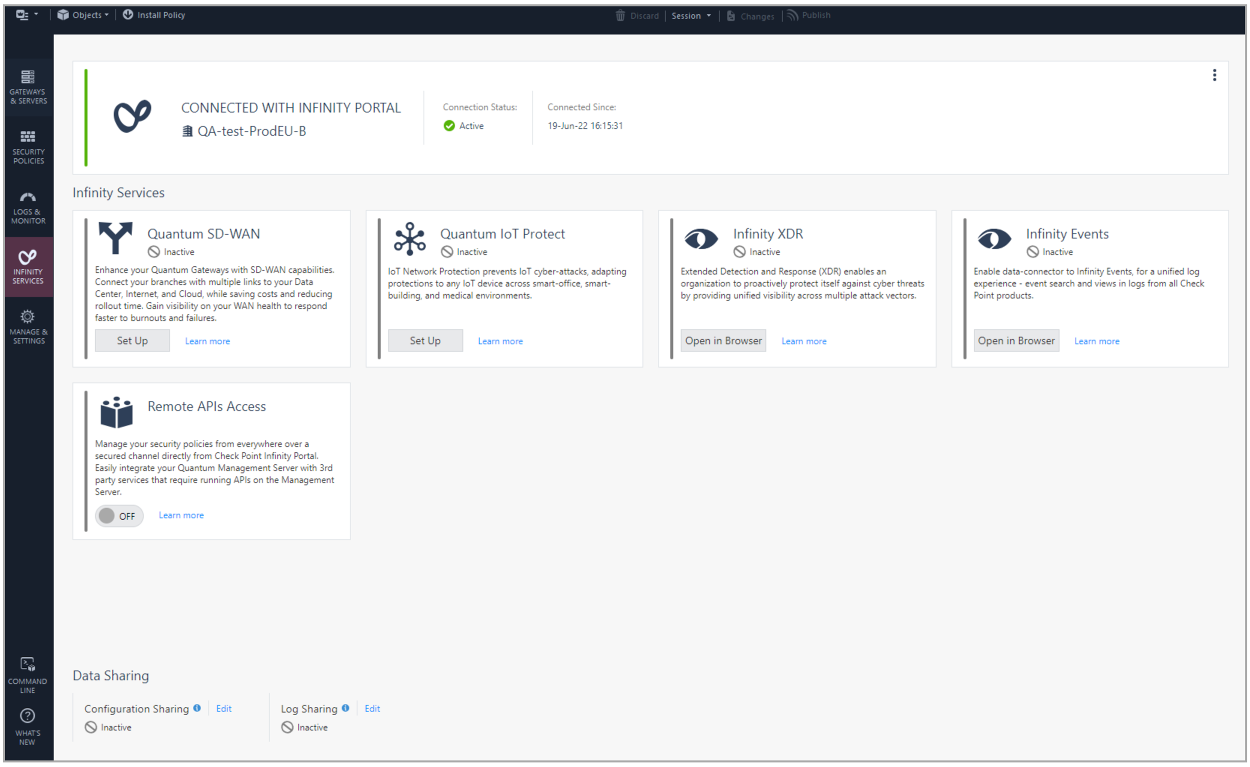
Enable data-connector to Infinity Events, for a unified log experience - event search and views in logs from all Check Point products.

Remote APIs Access

Manage your security policies from everywhere over a secured channel directly from Check Point Infinity Portal. Easily integrate your Quantum Management Server with 3rd party services that require running APIs on the Management Server.

When the SmartConsole connects to the Infinity Portal, the **Connectivity Status** changes to **Active**.

7. Navigate to **Infinity Services** and in the **Quantum IoT Protect** widget, click **Set Up**.



CONNECTED WITH INFINITY PORTAL
QA-test-ProdEU-B

Connection Status: Active

Connected Since: 19-Jun-22 16:15:31

Infinity Services

Quantum SD-WAN
Inactive

Enhance your Quantum Gateways with SD-WAN capabilities. Connect your branches with multiple links to your Data Center, Internet, and Cloud, while saving costs and reducing rollout time. Gain visibility on your WAN health to respond faster to burnouts and failures.

Quantum IoT Protect
Inactive

IoT Network Protection prevents IoT cyber-attacks, adapting protections to any IoT device across smart-office, smart-building, and medical environments.

Infinity XDR
Inactive

Extended Detection and Response (XDR) enables an organization to proactively protect itself against cyber threats by providing unified visibility across multiple attack vectors.

Infinity Events
Inactive

Enable data-connector to Infinity Events, for a unified log experience - event search and views in logs from all Check Point products.

Remote APIs Access

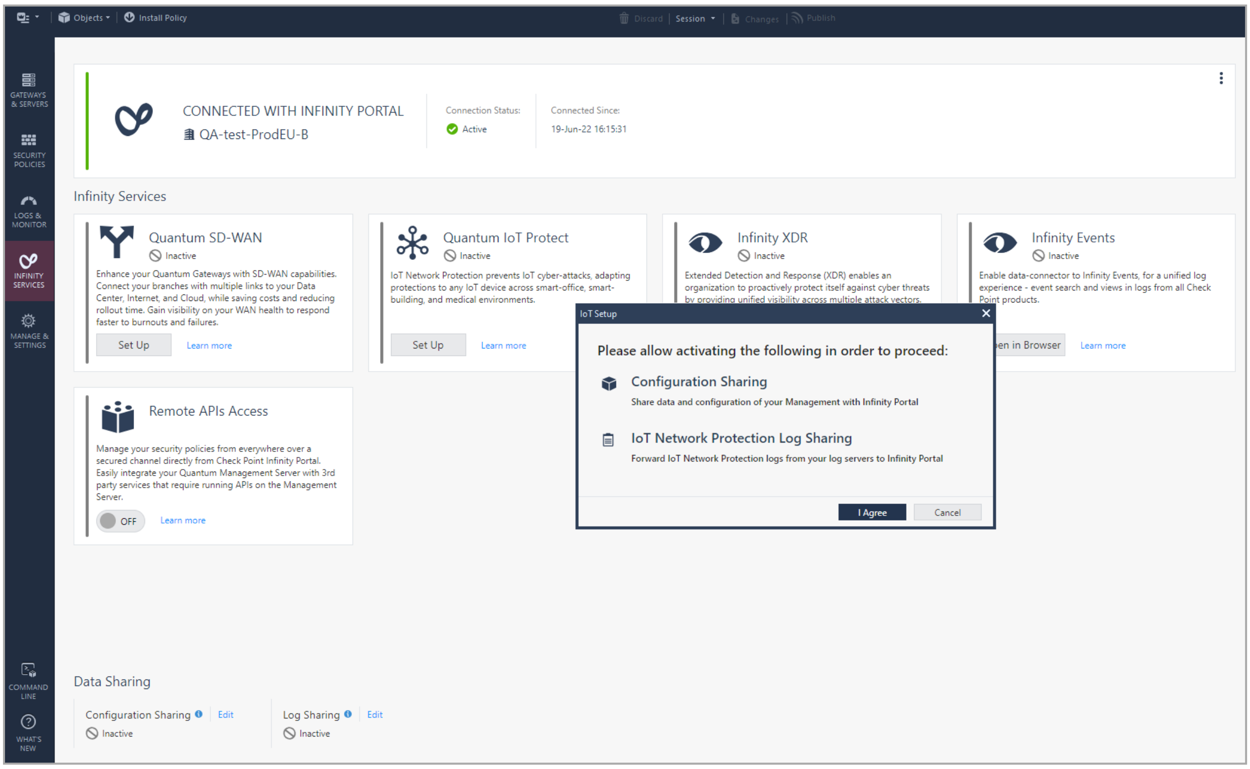
Manage your security policies from everywhere over a secured channel directly from Check Point Infinity Portal. Easily integrate your Quantum Management Server with 3rd party services that require running APIs on the Management Server.

Data Sharing

Configuration Sharing: Inactive

Log Sharing: Inactive

8. To activate configuration sharing and log sharing, in the **IoT Setup** window, click **I Agree**.



CONNECTED WITH INFINITY PORTAL
QA-test-ProdEU-B

Connection Status: Active

Connected Since: 19-Jun-22 16:15:31

Infinity Services

Quantum SD-WAN
Inactive
Enhance your Quantum Gateways with SD-WAN capabilities. Connect your branches with multiple links to your Data Center, Internet, and Cloud, while saving costs and reducing rollout time. Gain visibility on your WAN health to respond faster to burnouts and failures.

Quantum IoT Protect
Inactive
IoT Network Protection prevents IoT cyber-attacks, adapting protections to any IoT device across smart-office, smart-building, and medical environments.

Infinity XDR
Inactive
Extended Detection and Response (XDR) enables an organization to proactively protect itself against cyber threats by providing unified visibility across multiple attack vectors.

Infinity Events
Inactive
Enable data-connector to Infinity Events, for a unified log experience - event search and views in logs from all Check Point products.

Remote APIs Access
Manage your security policies from everywhere over a secured channel directly from Check Point Infinity Portal. Easily integrate your Quantum Management Server with 3rd party services that require running APIs on the Management Server.

IoT Setup

Please allow activating the following in order to proceed:

Configuration Sharing
Share data and configuration of your Management with Infinity Portal

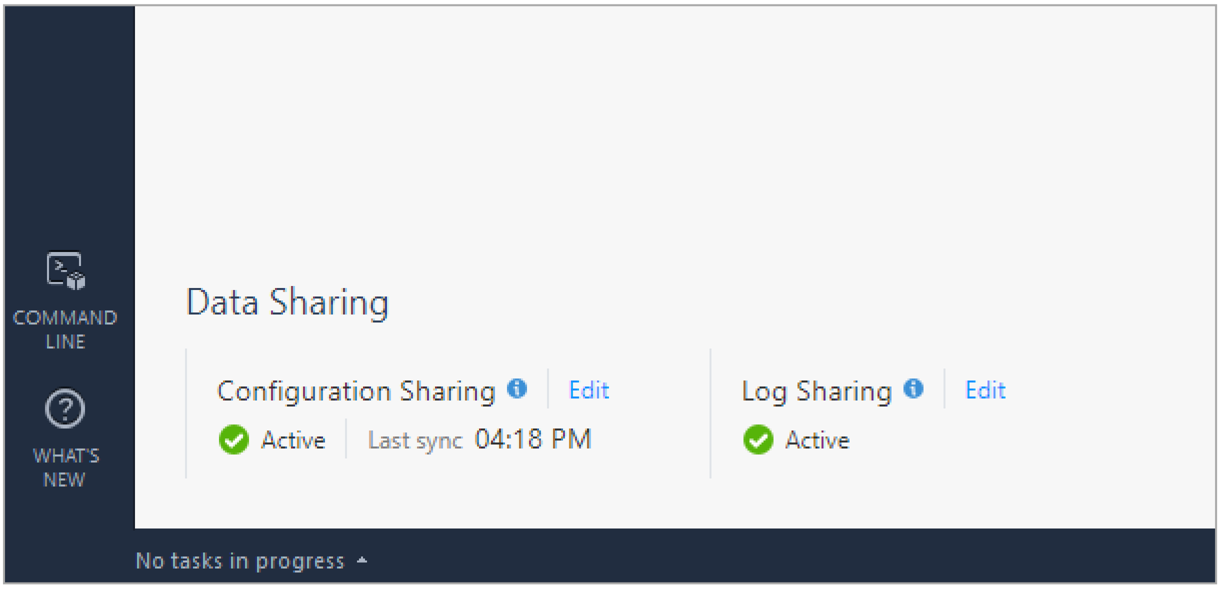
IoT Network Protection Log Sharing
Forward IoT Network Protection logs from your log servers to Infinity Portal

Data Sharing

Configuration Sharing
Inactive

Log Sharing
Inactive

When the SmartConsole integrates with Quantum IoT Protect, in the **Data Sharing** section, **Configuration Sharing** and **Log Sharing** status changes to **Active**.



Data Sharing

Configuration Sharing
Active Last sync 04:18 PM

Log Sharing
Active

No tasks in progress

Onboarding IoT Assets in Quantum IoT Protect

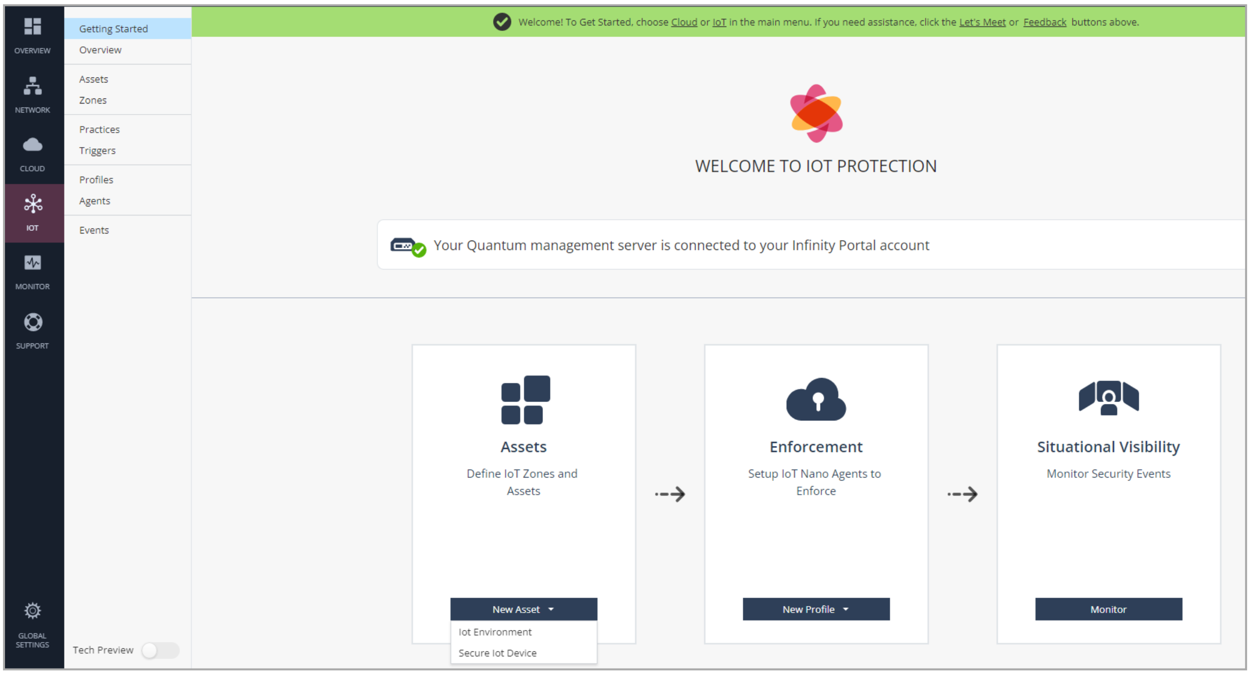
Notes -

- The documentation only covers the published features. To view the future enhancements, enable **Tech Preview** at the bottom of the page.
- Quantum IoT Protect is supported with Multi-Domain Server with single domain only. To onboard, see *"Appendix A - Onboarding Quantum IoT Protect on a Multi-Domain Management Server with Single Domain" on page 76*.
- To onboard Quantum IoT Protect on Quantum Maestro Security Group, see *"Appendix K - Onboarding Quantum IoT Protect on Quantum Maestro Security Group" on page 171*.

To onboard your IoT assets:

1. Log in to the *Check Point Infinity Portal*.
2. Under **Quantum**, go to **IoT Protect** > **IoT** > **Getting Started**.
3. In the **Assets** widget, click **New Asset** > **IoT Environment**.

   The **IoT Environment** wizard appears.

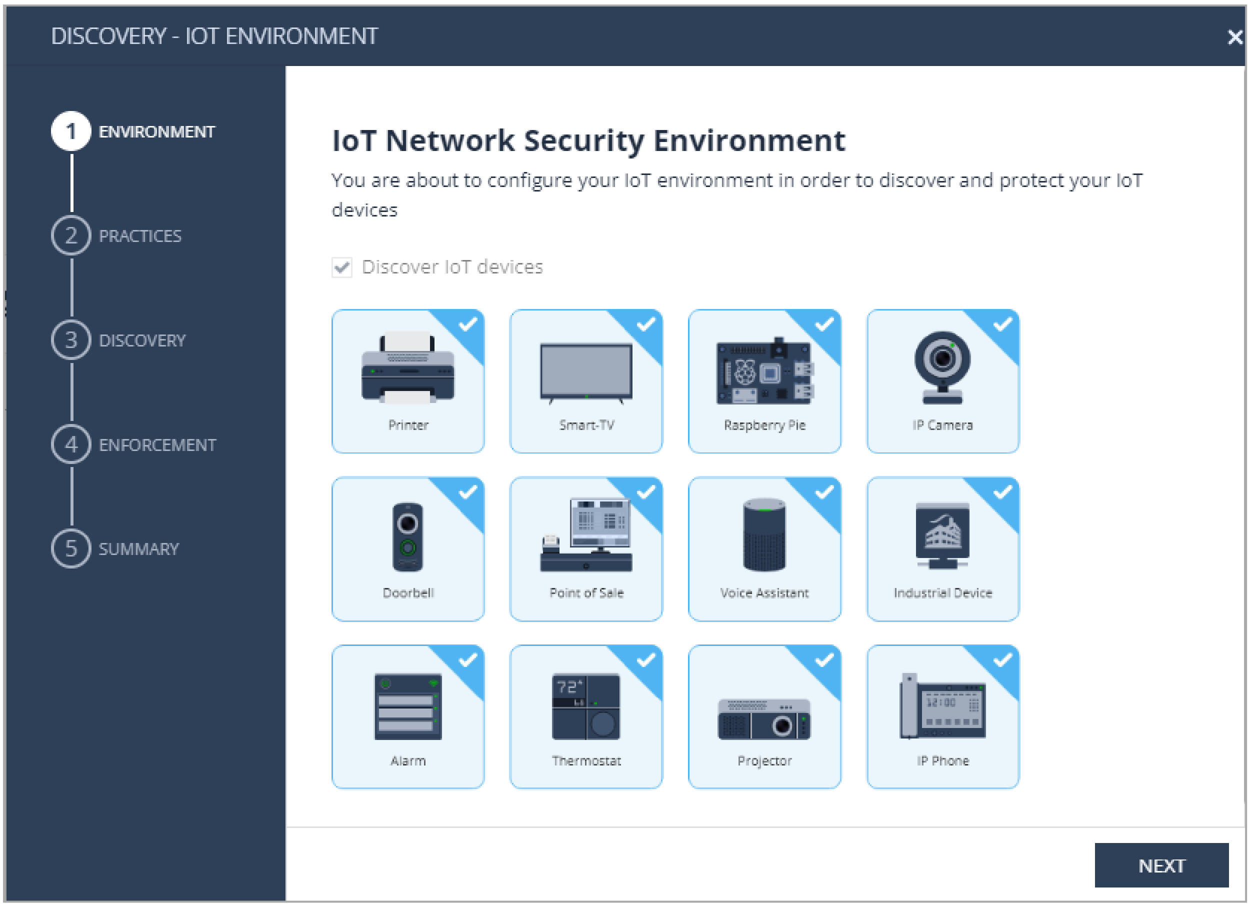


Welcome! To Get Started, choose Cloud or IoT in the main menu. If you need assistance, click the Let's Meet or Feedback buttons above.

WELCOME TO IOT PROTECTION

Your Quantum management server is connected to your Infinity Portal account

4. In the **Environment** screen, click **Next**.



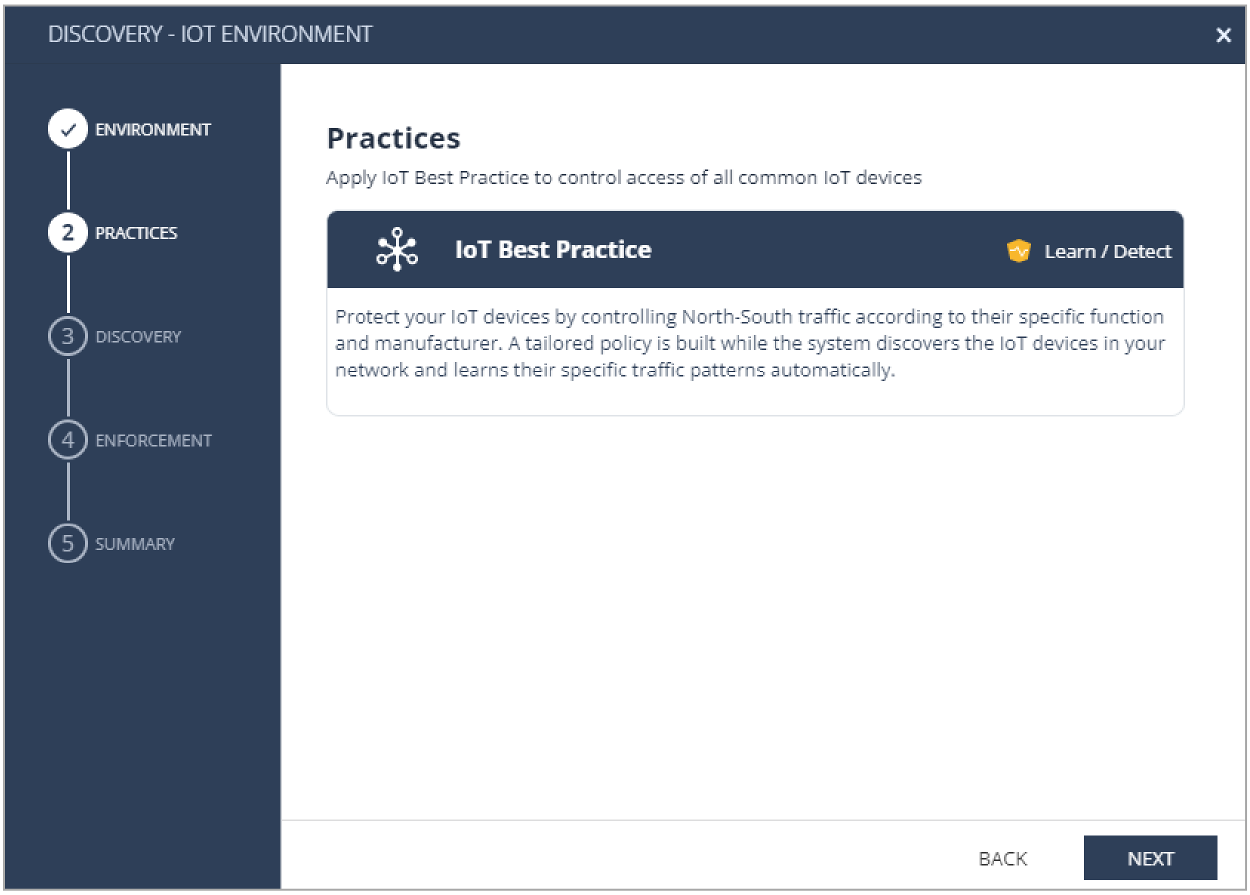
DISCOVERY - IOT ENVIRONMENT

IoT Network Security Environment

You are about to configure your IoT environment in order to discover and protect your IoT devices

☑ Discover IoT devices

5. In the **Practices** screen, click **Next**.



DISCOVERY - IOT ENVIRONMENT

Practices

Apply IoT Best Practice to control access of all common IoT devices

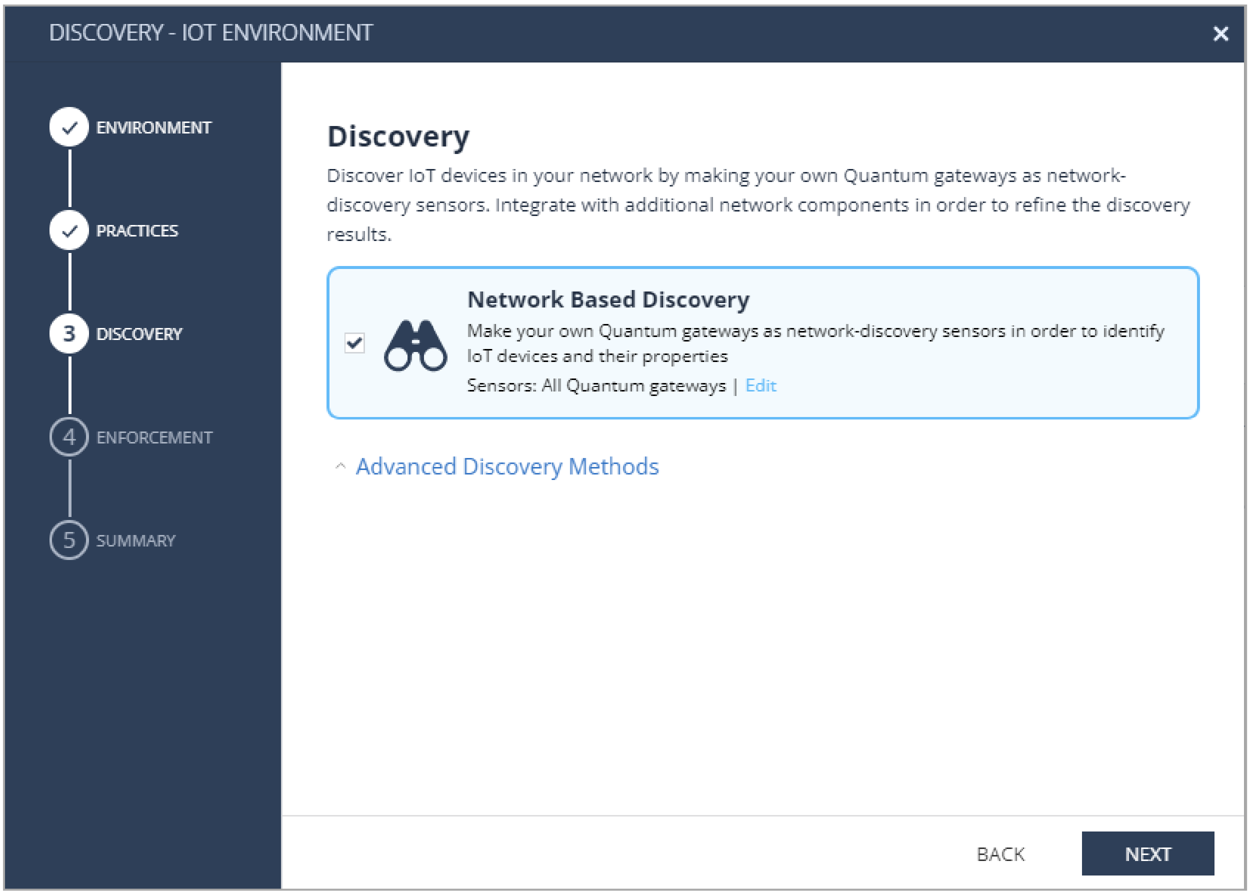
IoT Best Practice

Learn / Detect

Protect your IoT devices by controlling North-South traffic according to their specific function and manufacturer. A tailored policy is built while the system discovers the IoT devices in your network and learns their specific traffic patterns automatically.

6. In the **Discovery** screen:
   - Select **Network Based Discovery** and click **Edit**.

     Or
   - Click **Next** to apply network security on all gateways (default).



DISCOVERY - IOT ENVIRONMENT

Discovery

Discover IoT devices in your network by making your own Quantum gateways as network-discovery sensors. Integrate with additional network components in order to refine the discovery results.

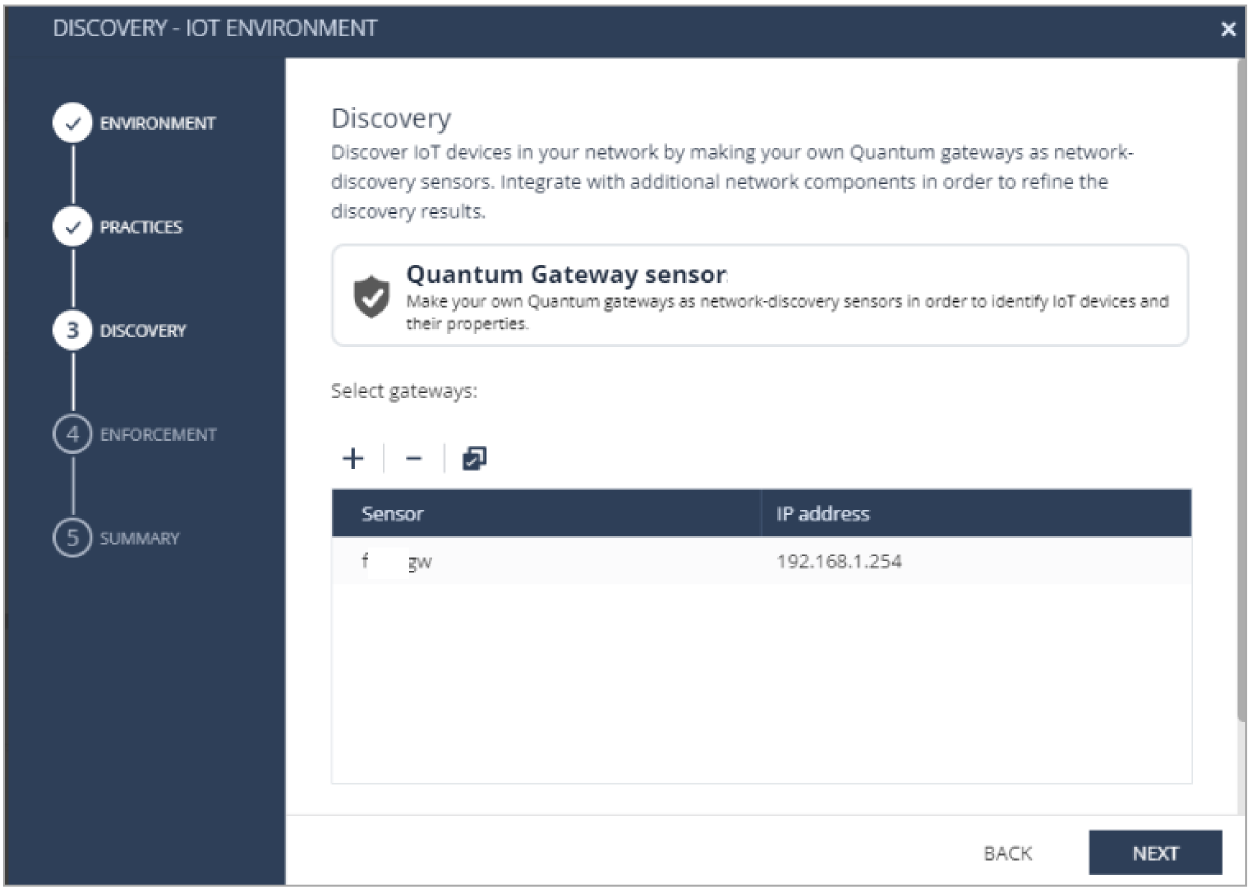
☑ Network Based Discovery

Make your own Quantum gateways as network-discovery sensors in order to identify IoT devices and their properties

Sensors: All Quantum gateways | Edit

7. Click **+**. From the security gateways listed, select the gateway that is connected to the IoT assets in your network.

   Click **Next**.



Discovery

Discover IoT devices in your network by making your own Quantum gateways as network-discovery sensors. Integrate with additional network components in order to refine the discovery results.

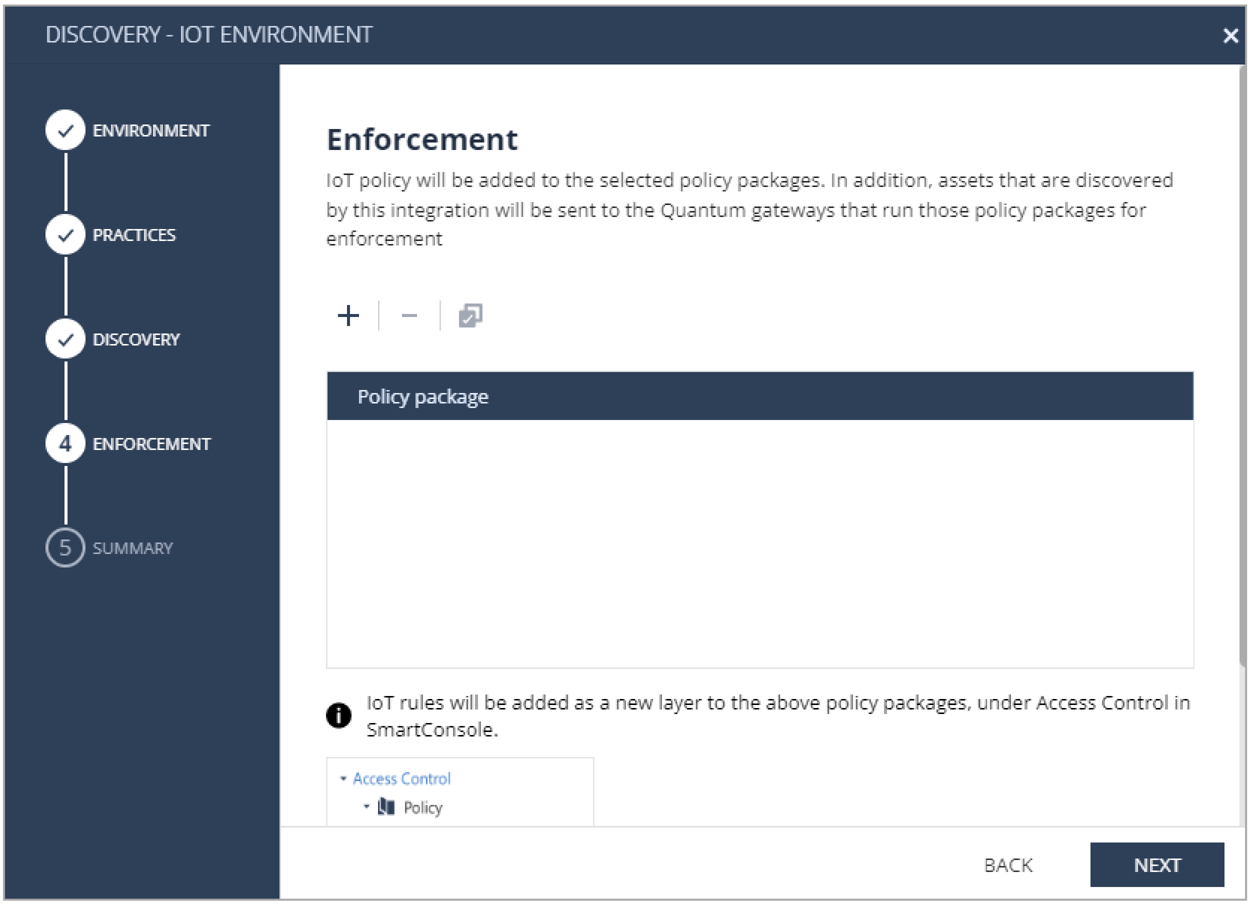
Quantum Gateway sensor

Make your own Quantum gateways as network-discovery sensors in order to identify IoT devices and their properties.

Select gateways:

Sensor	IP address
f gw	192.168.1.254

8. In the **Enforcement** screen, click **+** to add a **Policy package**.



DISCOVERY - IOT ENVIRONMENT

Enforcement

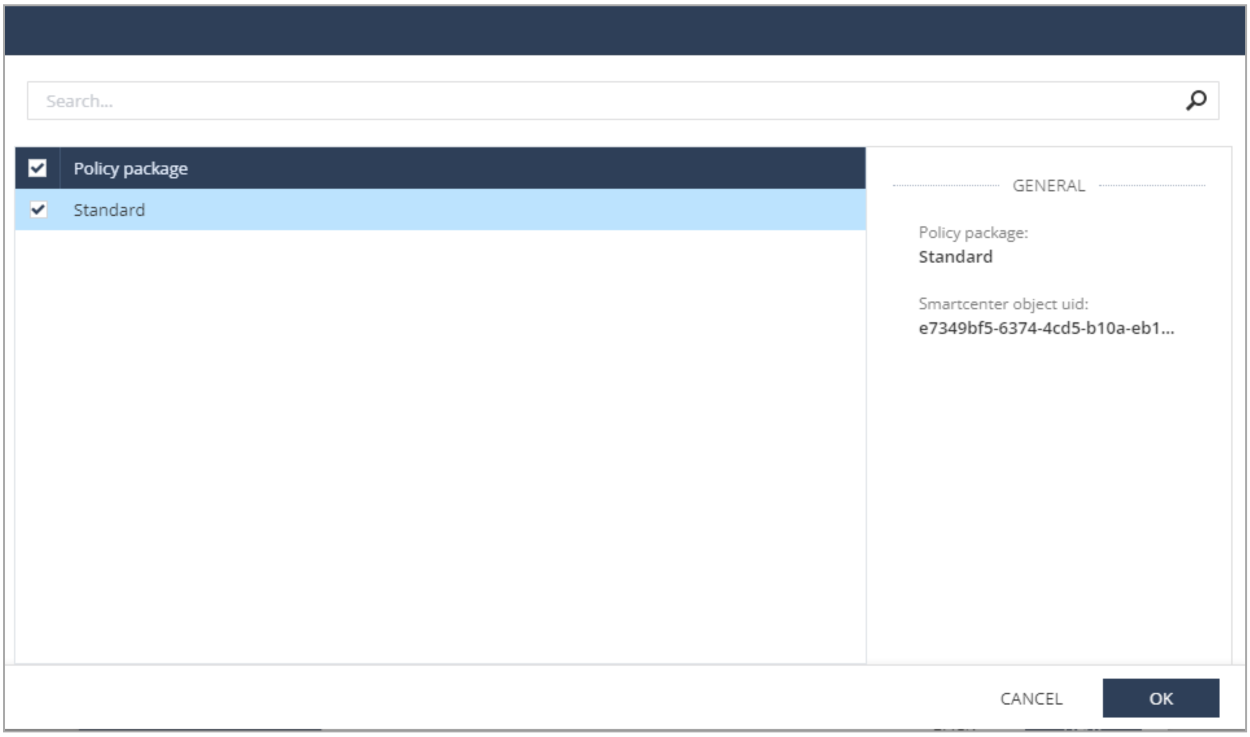
IoT policy will be added to the selected policy packages. In addition, assets that are discovered by this integration will be sent to the Quantum gateways that run those policy packages for enforcement

Policy package

IoT rules will be added as a new layer to the above policy packages, under Access Control in SmartConsole.

9. Select **Standard** and click **OK**.

   The policy package is added.



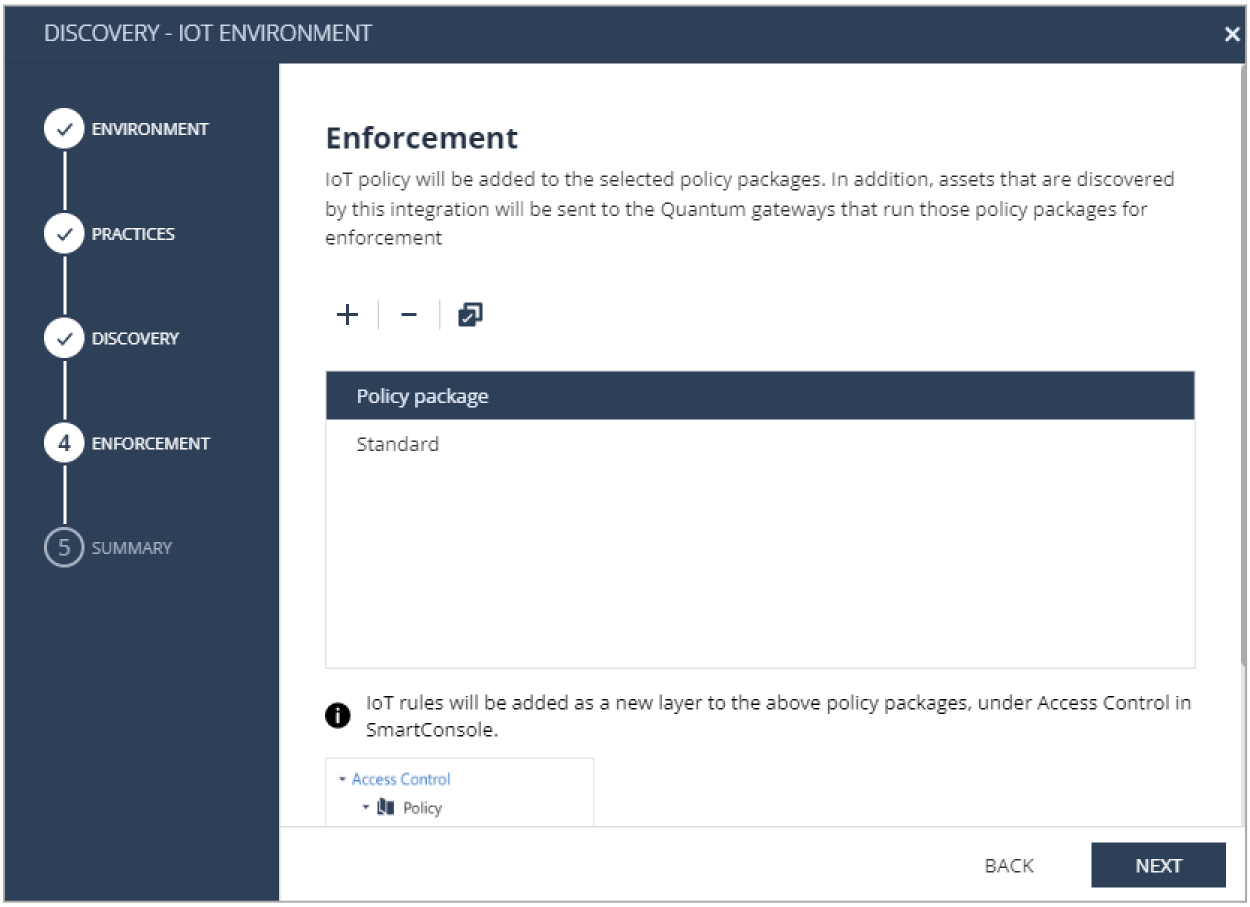
☑	Policy package
☑	Standard

GENERAL

Policy package: Standard

Smartcenter object uid: e7349bf5-6374-4cd5-b10a-eb1...

10. Click **Next**.



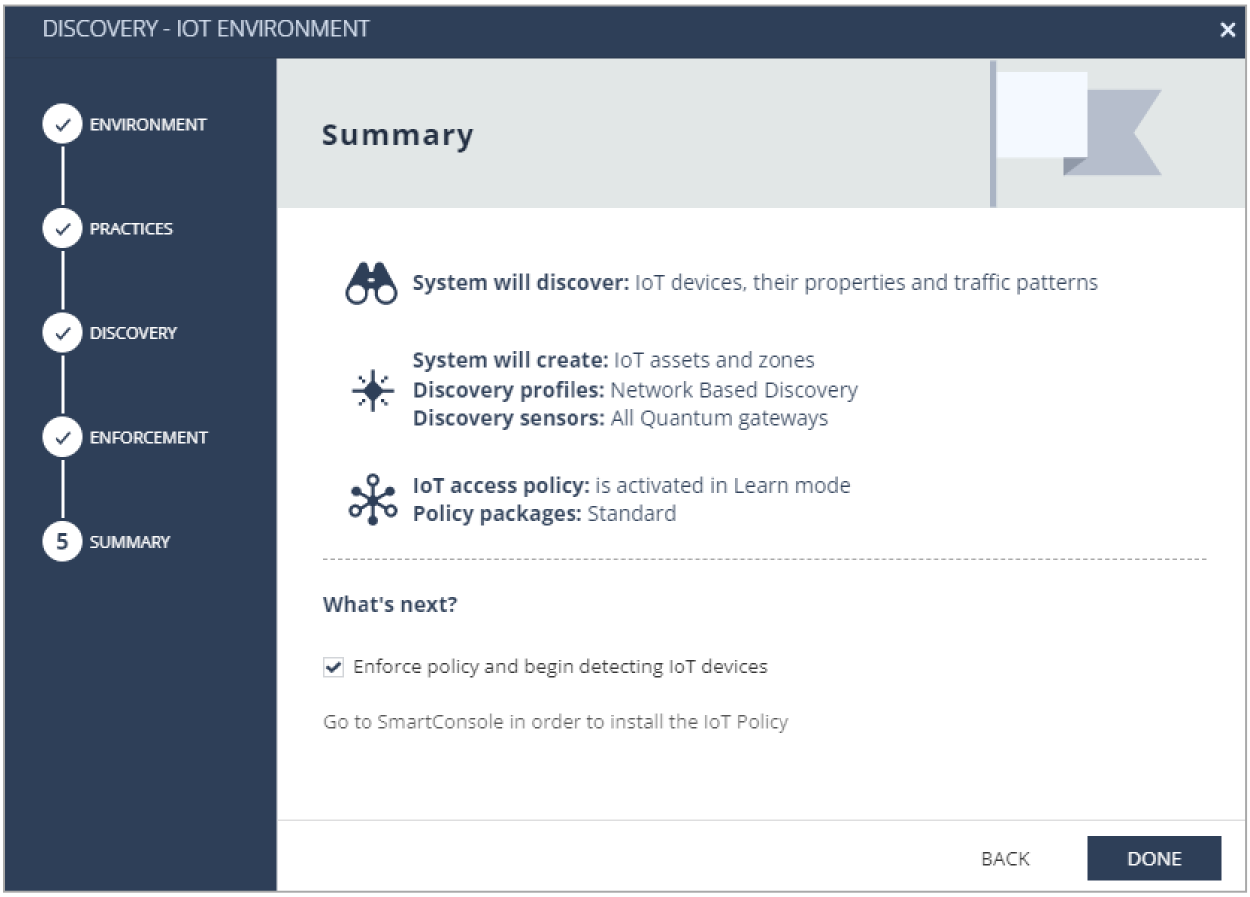
Enforcement

IoT policy will be added to the selected policy packages. In addition, assets that are discovered by this integration will be sent to the Quantum gateways that run those policy packages for enforcement

Policy package
Standard

IoT rules will be added as a new layer to the above policy packages, under Access Control in SmartConsole.

11. In the **Summary** screen, review the summary and click **Done**.



DISCOVERY - IOT ENVIRONMENT

Summary

System will discover: IoT devices, their properties and traffic patterns

System will create: IoT assets and zones
Discovery profiles: Network Based Discovery
Discovery sensors: All Quantum gateways

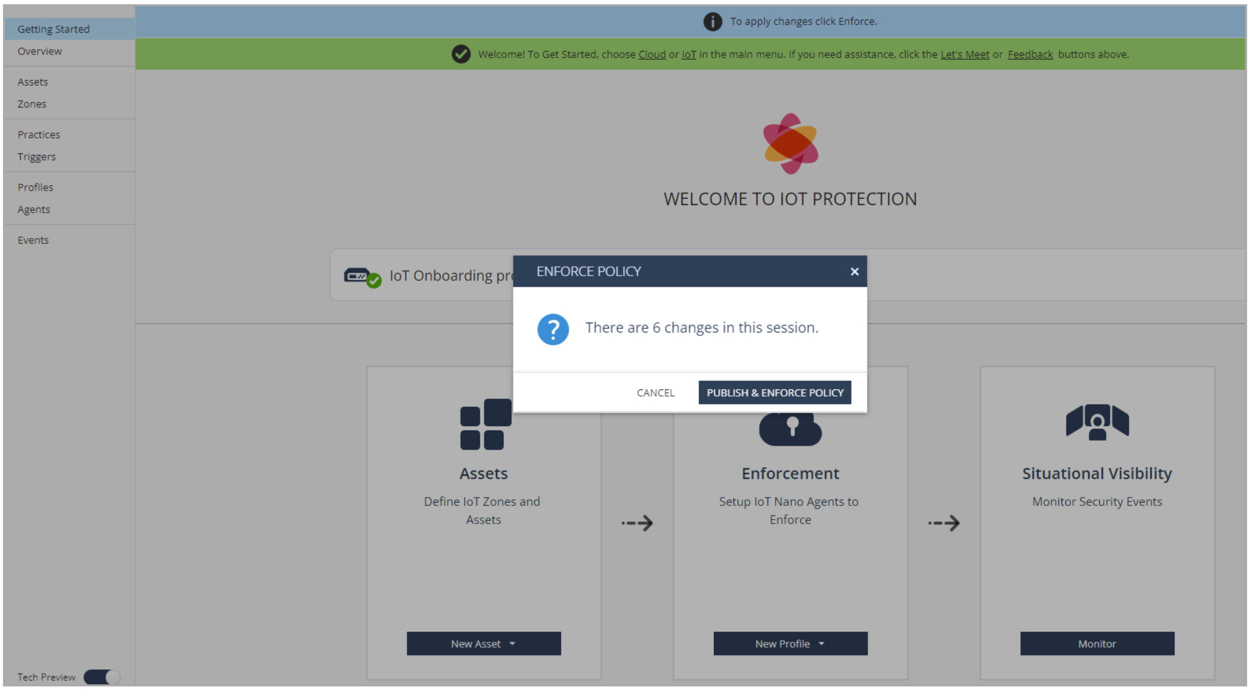
IoT access policy: is activated in Learn mode
Policy packages: Standard

What's next?

☑ Enforce policy and begin detecting IoT devices

Go to SmartConsole in order to install the IoT Policy

12. Click **Publish & Enforce Policy**.



To apply changes click Enforce.

Welcome! To Get Started, choose Cloud or IoT in the main menu. If you need assistance, click the Let's Meet or Feedback buttons above.

WELCOME TO IOT PROTECTION

ENFORCE POLICY

There are 6 changes in this session.

13. Go to Smart Console and click **Install Policy** for the policy package(s) selected in steps 8 and 9.

14. Go to **IOT** > **Overview**.

Verify if the **Overview** page shows the discovered IoT assets. For more information, see *"Overview" on page 32*.

Managing IoT Assets in Quantum IoT Protect

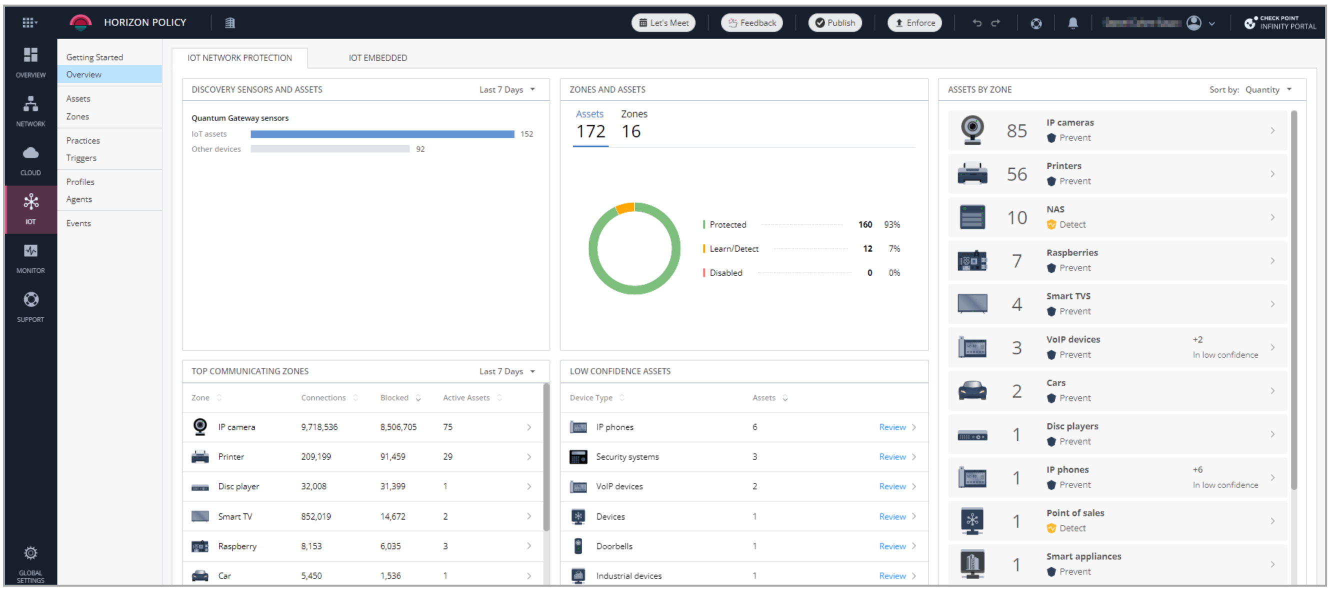
This chapter describes how to manage the onboarded IoT assets in Quantum IoT Protect application.

Note - The documentation only covers the published features.
To view the future enhancements, enable **Tech Preview** at the bottom of the page.

Overview

The **Overview** page shows an overview of network protection statistics for the onboarded IoT assets.

To access the **Overview** page, click **IoT** > **Overview**.



DISCOVERY SENSORS AND ASSETS — Last 7 Days

Quantum Gateway sensors

IoT assets	152
Other devices	92

ZONES AND ASSETS

Assets 172 Zones 16

Protected	160	93%
Learn/Detect	12	7%
Disabled	0	0%

ASSETS BY ZONE — Sort by: Quantity

85	IP cameras	Prevent	
56	Printers	Prevent	
10	NAS	Detect	
7	Raspberries	Prevent	
4	Smart TVS	Prevent	
3	VoIP devices	Prevent	+2 In low confidence
2	Cars	Prevent	
1	Disc players	Prevent	
1	IP phones	Prevent	+6 In low confidence
1	Point of sales	Detect	
1	Smart appliances	Prevent	

TOP COMMUNICATING ZONES — Last 7 Days

Zone	Connections	Blocked	Active Assets
IP camera	9,718,536	8,506,705	75
Printer	209,199	91,459	29
Disc player	32,008	31,399	1
Smart TV	852,019	14,672	2
Raspberry	8,153	6,035	3
Car	5,450	1,536	1

LOW CONFIDENCE ASSETS

Device Type	Assets	
IP phones	6	Review
Security systems	3	Review
VoIP devices	2	Review
Devices	1	Review
Doorbells	1	Review
Industrial devices	1	Review

Discovery Sensors and Assets

Shows the number of **IoT assets** and **Other devices** (not IoT assets) discovered by different sensors. For example, Quantum gateway sensor, integrations used to discover the IoT assets (such as SNMP, MS-DHCP and so on).

You can view this information for the last 7 days, 14 days or 30 days.

Note - If the current discovery mechanism does not discover all the IoT assets in your network, you can use any one of these supported services on the Check Point Management Server to improve the discovery accuracy.

- *"Appendix B - Using SNMP as the IoT Discovery Engine" on page 78*.
- *"Appendix C - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory)" on page 89*.
- *"Appendix D - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Splunk)" on page 106*.
- *"Appendix E - Using Unix DHCP - Syslog as the IoT Discovery Engine" on page 115*.
- *"Appendix F - Using Unix DHCP as the IoT Discovery Engine" on page 129*.
- *"Appendix G - Using Cisco ISE as the IoT Discovery Engine" on page 143*.
- *"Appendix H - Using Infoblox DHCP - Syslog as the IoT Discovery Engine" on page 154*.
- *"Appendix I - Integrating IoT Assets using Third-Party Discovery Engines through APIs" on page 162*

Zones and Assets

Shows the number of IoT assets, zones and the operating mode (Protected, Learn/Detect, and Disabled) of IoT assets.

Operating Mode	Description
Protected	Assets/Zones secured by Quantum IoT Protect.
Learn/Detect	Assets/Zones in Learn/Detect mode.
Disabled	Assets/Zones not handled by Quantum IoT Protect.

For more information on zones, see *"Zones" on page 43*.

For more information on operating modes, see *"Access Control" on page 45*.

Assets By Zone

Shows the zones and number of IoT assets in each zone. You can sort the zones by:

- Quantity (default)
- Name
- Mode

Click **>** to view zone information. See *"Zones" on page 43*.

Top Communicating Zones

Shows the assets' communication statistics for each zone.

You can view this information for the last 7 days, 14 days or 30 days.

Item	Description
Zone	Zone name.
Connections	The number of asset connections discovered in the zone.
Blocked	The number of assets whose traffic is blocked in the zone.
Active Assets	The number of assets with active traffic in the zone.

Low Confidence Assets

Shows the list of assets for which the system has low confidence on their function. The system does not enforce the zone's best practices for these assets.

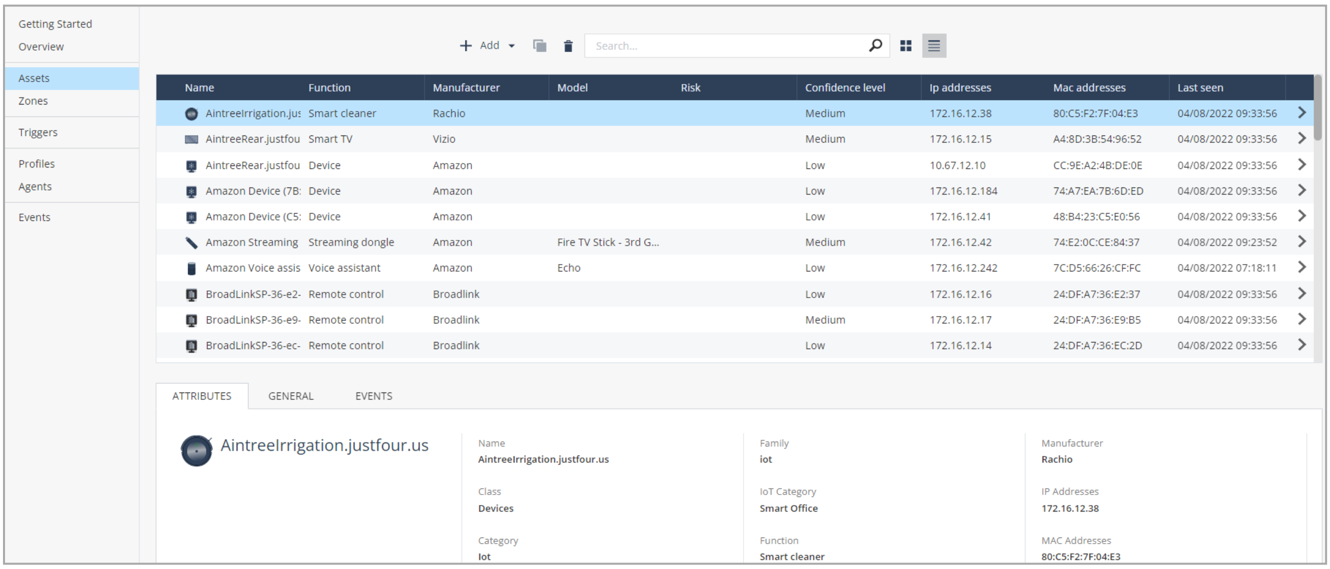
To view more information about each asset, click **Review**.

Assets

The **Assets** page shows the IoT assets information.

Note - An asset that does not communicate with Quantum IoT Protect for a specific time period is considered as an inactive asset. To set this value, go to **Asset Configuration** > **inactiveAssetRetention** in *"IoT Configuration Profile" on page 61*. After this period, Quantum IoT Protect automatically deletes the inactive asset from the system.

To access the **Assets** page, go to **IoT** > **Assets**.

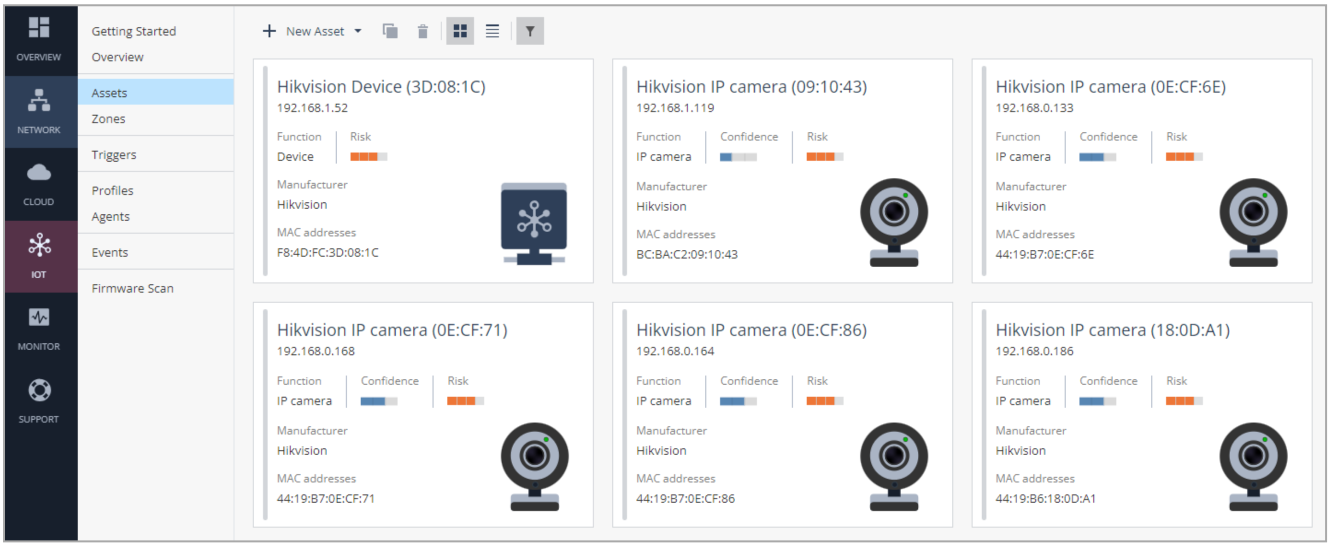


Name	Function	Manufacturer	Model	Risk	Confidence level	Ip addresses	Mac addresses	Last seen
AintreeIrrigation.jus	Smart cleaner	Rachio			Medium	172.16.12.38	80:C5:F2:7F:04:E3	04/08/2022 09:33:56
AintreeRear.justfou	Smart TV	Vizio			Medium	172.16.12.15	A4:8D:3B:54:96:52	04/08/2022 09:33:56
AintreeRear.justfou	Device	Amazon			Low	10.67.12.10	CC:9E:A2:4B:DE:0E	04/08/2022 09:33:56
Amazon Device (7B:	Device	Amazon			Low	172.16.12.184	74:A7:EA:7B:6D:ED	04/08/2022 09:33:56
Amazon Device (C5:	Device	Amazon			Low	172.16.12.41	48:B4:23:C5:E0:56	04/08/2022 09:33:56
Amazon Streaming	Streaming dongle	Amazon	Fire TV Stick - 3rd G...		Medium	172.16.12.42	74:E2:0C:CE:84:37	04/08/2022 09:23:52
Amazon Voice assis	Voice assistant	Amazon	Echo		Low	172.16.12.242	7C:D5:66:26:CF:FC	04/08/2022 07:18:11
BroadLinkSP-36-e2-	Remote control	Broadlink			Low	172.16.12.16	24:DF:A7:36:E2:37	04/08/2022 09:33:56
BroadLinkSP-36-e9-	Remote control	Broadlink			Medium	172.16.12.17	24:DF:A7:36:E9:B5	04/08/2022 09:33:56
BroadLinkSP-36-ec-	Remote control	Broadlink			Low	172.16.12.14	24:DF:A7:36:EC:2D	04/08/2022 09:33:56

AintreeIrrigation.justfour.us

Name	Family	Manufacturer
AintreeIrrigation.justfour.us	iot	Rachio
Class	**IoT Category**	**IP Addresses**
Devices	Smart Office	172.16.12.38
Category	**Function**	**MAC Addresses**
Iot	Smart cleaner	80:C5:F2:7F:04:E3

The default is the table view. To switch to card view, click ▦.



Hikvision Device (3D:08:1C)
192.168.1.52
Function: Device | Risk
Manufacturer: Hikvision
MAC addresses: F8:4D:FC:3D:08:1C

Hikvision IP camera (09:10:43)
192.168.1.119
Function: IP camera | Confidence | Risk
Manufacturer: Hikvision
MAC addresses: BC:BA:C2:09:10:43

Hikvision IP camera (0E:CF:6E)
192.168.0.133
Function: IP camera | Confidence | Risk
Manufacturer: Hikvision
MAC addresses: 44:19:B7:0E:CF:6E

Hikvision IP camera (0E:CF:71)
192.168.0.168
Function: IP camera | Confidence | Risk
Manufacturer: Hikvision
MAC addresses: 44:19:B7:0E:CF:71

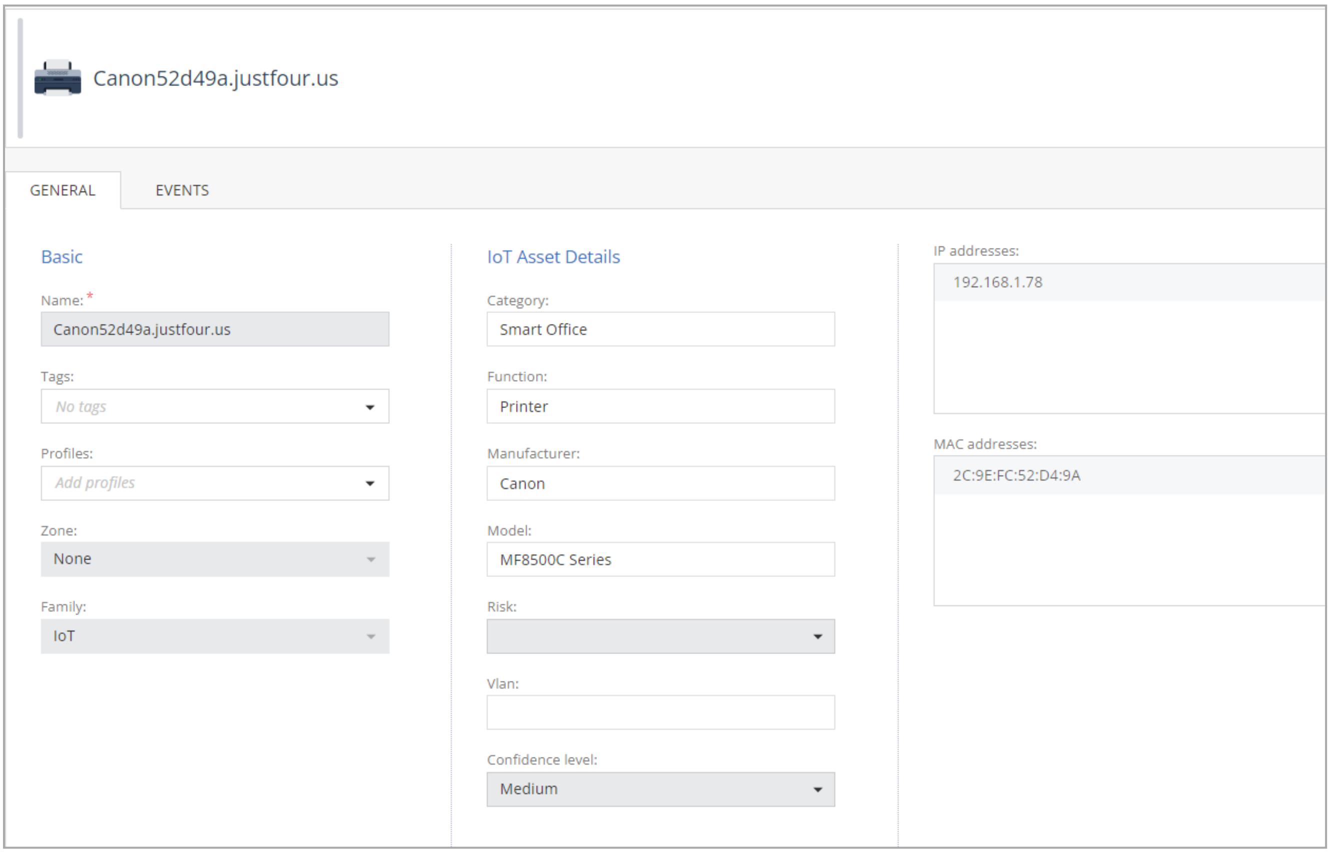
Hikvision IP camera (0E:CF:86)
192.168.0.164
Function: IP camera | Confidence | Risk
Manufacturer: Hikvision
MAC addresses: 44:19:B7:0E:CF:86

Hikvision IP camera (18:0D:A1)
192.168.0.186
Function: IP camera | Confidence | Risk
Manufacturer: Hikvision
MAC addresses: 44:19:B6:18:0D:A1

Item	Description
Name	The name of the IoT asset. If Quantum IoT Protect cannot retrieve the name of the asset, it creates a name in the format: <Manufacturer> <Function> <Model> <Suffix of the asset MAC address>. For example, Yamaha AV receiver RX-V681 (DC:EB:A7).
Function	Function of the asset. For example, Printer.
Manufacturer	Manufacturer of the asset. For example, Amazon.
Model	Model number of the asset.
Risk	Risk level of the asset: ■ High ■ Low ■ Medium ■ None ■ Unknown
Confidence level	Confidence level for the asset functionality: ■ High ■ Low ■ Medium ■ Unknown
IP address	IP address of the asset.
Mac address	MAC address of the asset.
Last seen	The date and time when the asset information was last synchronized with Quantum IoT Protect. The synchronization happens every six hours.
>	View detailed information about the asset in these tabs: ■ *"General " on the next page* ■ *"Events" on page 38* ■ *"Attributes" on page 40* ■ *"Practices" on page 41*
🗑	Delete an asset.

General

Shows the generic information about the selected IoT asset.



Canon52d49a.justfour.us

Basic

Name: * Canon52d49a.justfour.us

Tags: No tags

Profiles: Add profiles

Zone: None

Family: IoT

IoT Asset Details

Category: Smart Office

Function: Printer

Manufacturer: Canon

Model: MF8500C Series

Risk:

Vlan:

Confidence level: Medium

IP addresses: 192.168.1.78

MAC addresses: 2C:9E:FC:52:D4:9A

Item	Description
Basic	
Name	Name of the asset.
Tags	Not applicable.
Profiles	Not applicable.
Zone	Asset zone.
Family	Family in which the asset belongs. ▪ IoT ▪ Generic
IoT Asset Details	
Category	Category of the asset.
Function	Function of the asset.

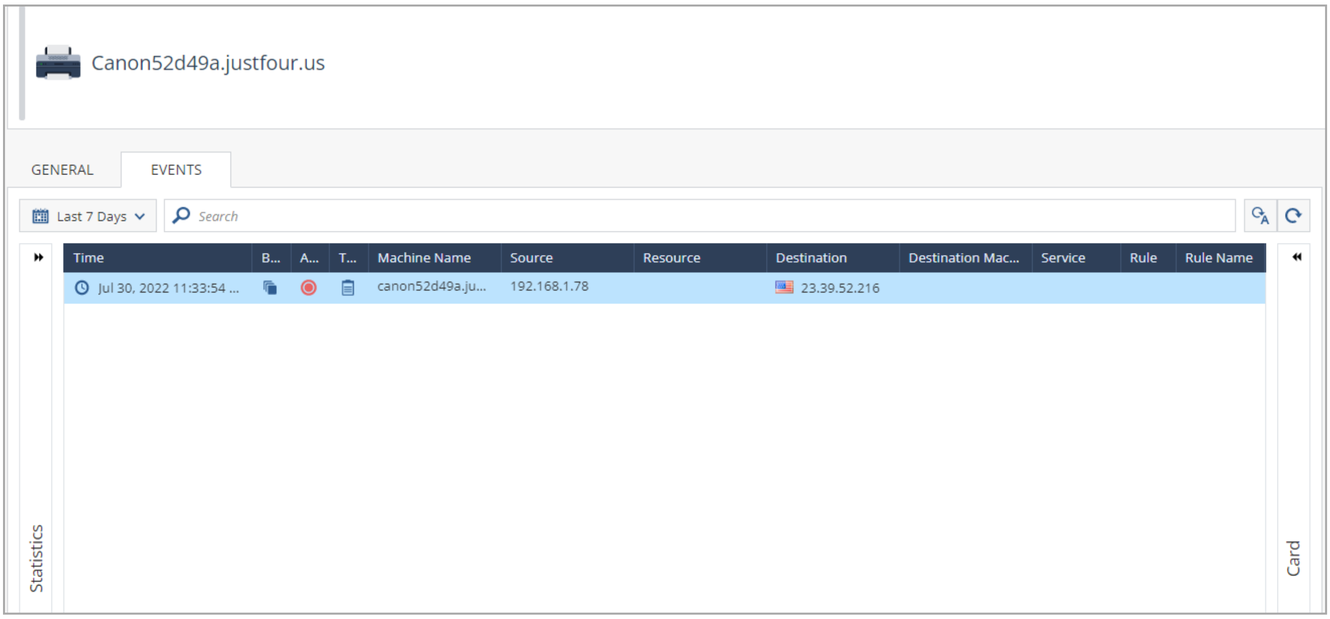
Item	Description
Manufacturer	Manufacturer of the asset.
Model	Model number of the asset.
Risk	Risk level of the asset: ■ High ■ Low ■ Medium ■ None ■ Unknown
VLAN	VLAN of the asset.
Confidence level	Confidence level for the asset functionality: ■ High ■ Low ■ Medium ■ Unknown
IP addresses	IP address of the asset.
MAC addresses	MAC address of the asset.

Events

Shows the events logged for the selected asset.

To view the event statistics, click ⏩ in the **Statistics** bar on the left.

For card view, click ⏪ in the **Card** bar on the right.



Canon52d49a.justfour.us

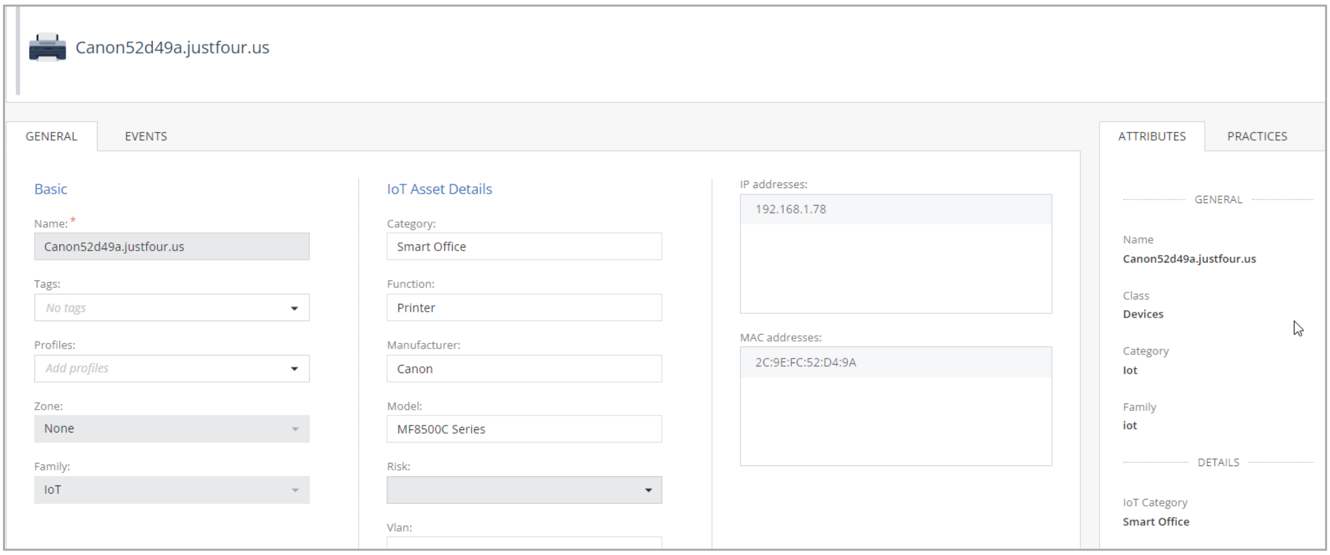
Time	B...	A...	T...	Machine Name	Source	Resource	Destination	Destination Mac...	Service	Rule	Rule Name
Jul 30, 2022 11:33:54 ...		●		canon52d49a.ju...	192.168.1.78		23.39.52.216				

Event Parameter	Description
Time	Time of the event.
Blade	Software blade which triggered the logs: ■ Firewall ■ IoT ■ IoT URL Filtering ■ Application Control IoT
Action	Action enforced on the event: ■ Drop - Block. ■ Accept - Allow.
Type	■ Connection - Event generated in an individual connection. ■ Session - Event generated in a session.
Machine Name	Name of the asset.
Source	IP address of the IoT asset.
Resource	Resource accessed by the asset.
Destination	IP address of the destination.
Destination Machine Name	Name of the destination asset.
Service	Service that generated the event.

Event Parameter	Description
Rule	Rule number from the relevant policy package and Rulebase (Examples - 7.1, 11.5).
Rule Name	Name of the rule (Examples - Internet IoT all, IoT DNS to internal).

Attributes

Shows the attributes of the selected asset.



Canon52d49a.justfour.us

Basic

Name: * Canon52d49a.justfour.us

Tags: No tags

Profiles: Add profiles

Zone: None

Family: IoT

IoT Asset Details

Category: Smart Office

Function: Printer

Manufacturer: Canon

Model: MF8500C Series

Risk:

Vlan:

IP addresses: 192.168.1.78

MAC addresses: 2C:9E:FC:52:D4:9A

GENERAL

Name
Canon52d49a.justfour.us

Class
Devices

Category
Iot

Family
iot

DETAILS

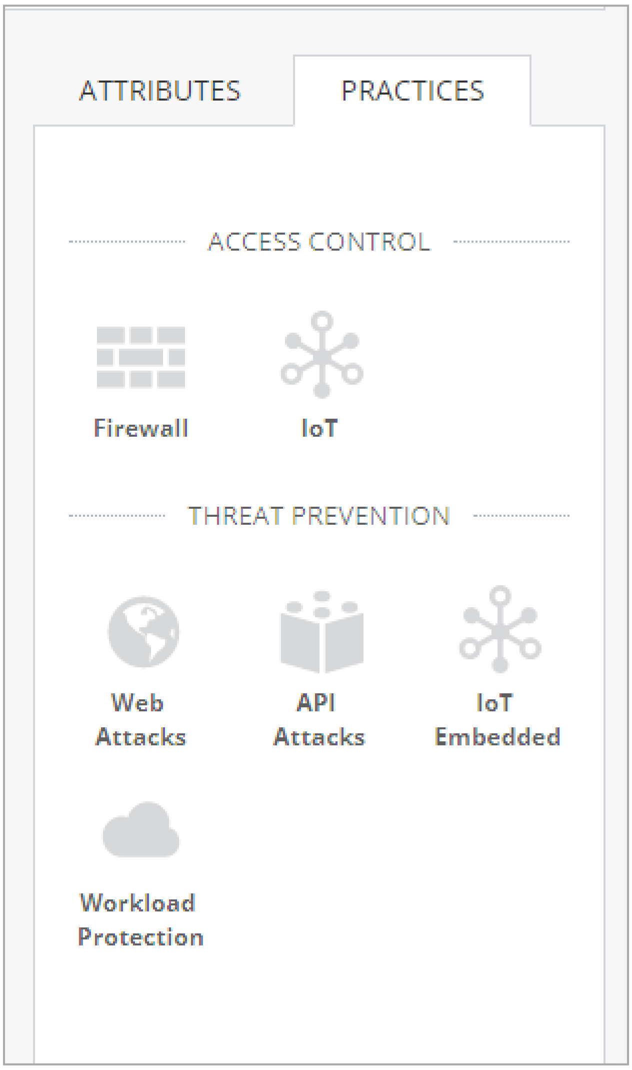
IoT Category
Smart Office

Item	Description
General	
Name	Name of the asset.
Class	▪ Device ▪ Agent
Category	Category of the asset.
Family	Family in which the asset belongs.
Details	
IoT Category	Category of the asset.
Function	Function of the asset.
Manufacturer	Manufacturer of the asset.

Item	Description
IP addresses	IP address of the asset.
MAC addresses	MAC address of the asset.
Confidence level	Confidence level for the asset functionality: ■ High ■ Low ■ Medium ■ Unknown

Practices

Shows the different **Access Control** and **Threat Prevention** practices applied on the asset.



Inactive Assets

An asset that does not communicate with Quantum IoT Protect for a specific time period is considered as an inactive asset. To set this value, go to **Asset Configuration** > **inactiveAssetRetention** in *"IoT Configuration Profile" on page 61*.

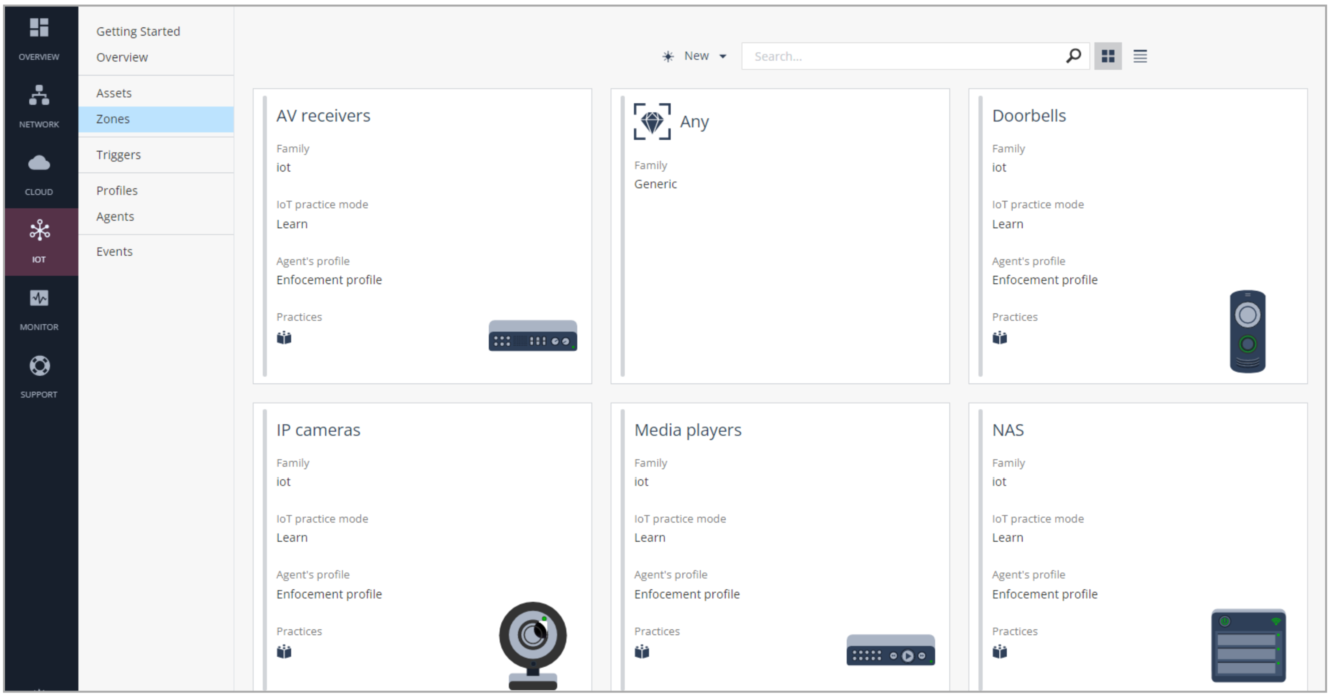
After this period, Quantum IoT Protect automatically deletes the inactive asset from the system.

Zones

A zone is a group of IoT assets categorized by their function. Quantum IoT Protect automatically adds the onboarded assets to the relevant zones.

To access the **Zones** page, go to **IoT** > **Zones**.

For example, IP cameras are added to the **IP cameras** zone.



AV receivers
Family
iot
IoT practice mode
Learn
Agent's profile
Enfocement profile
Practices

Any
Family
Generic

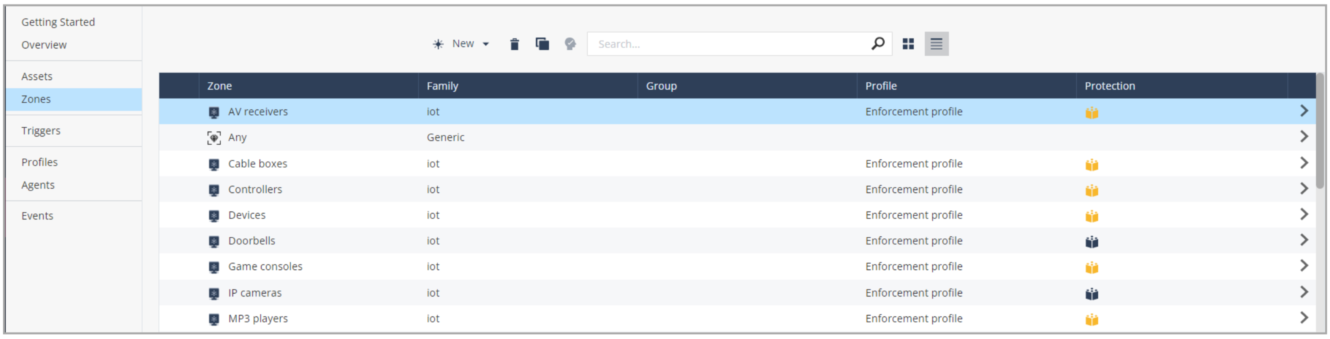
Doorbells
Family
iot
IoT practice mode
Learn
Agent's profile
Enfocement profile
Practices

IP cameras
Family
iot
IoT practice mode
Learn
Agent's profile
Enfocement profile
Practices

Media players
Family
iot
IoT practice mode
Learn
Agent's profile
Enfocement profile
Practices

NAS
Family
iot
IoT practice mode
Learn
Agent's profile
Enfocement profile
Practices

Note - The default is the card view. To switch to table view, click ☰.



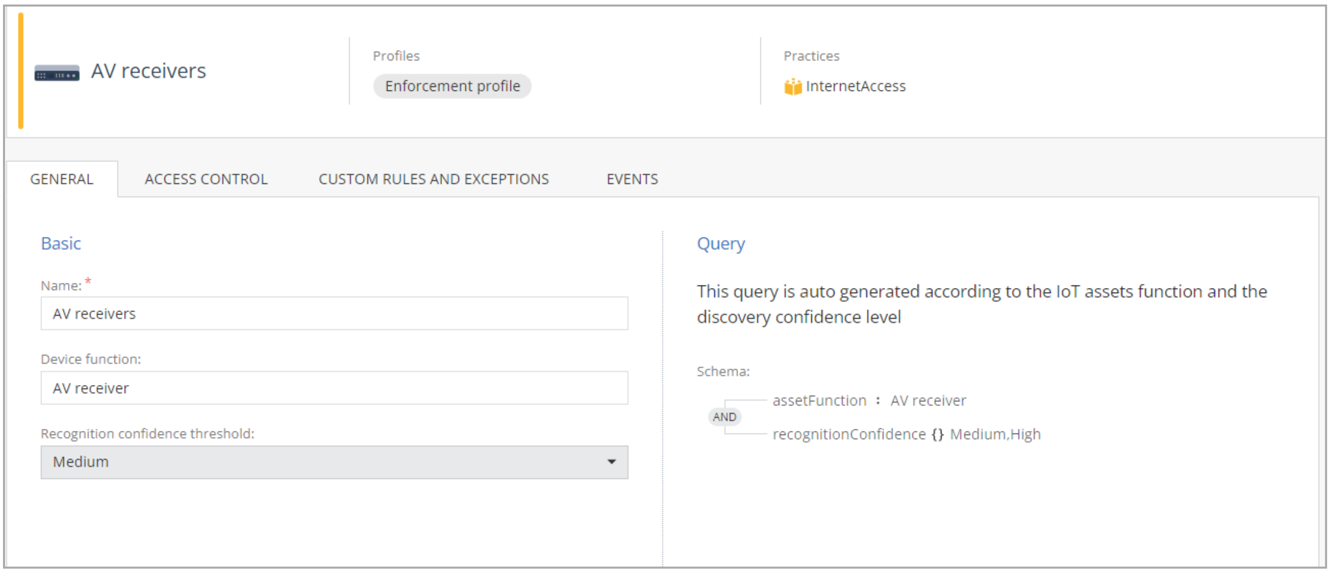
Zone	Family	Group	Profile	Protection
AV receivers	iot		Enforcement profile	
Any	Generic			
Cable boxes	iot		Enforcement profile	
Controllers	iot		Enforcement profile	
Devices	iot		Enforcement profile	
Doorbells	iot		Enforcement profile	
Game consoles	iot		Enforcement profile	
IP cameras	iot		Enforcement profile	
MP3 players	iot		Enforcement profile	

Item	Description
✳ New ▾	Create a new zone.
🗑	Delete a zone.

Item	Description
⧉	Create a clone of the selected zone.
Card view	
Family	Family in which the assets in the zone belong. ■ IoT ■ Generic
IoT practice mode	Practice mode of the zone.
Agent's profile	Profile of the agent.
Practices	Sub-practice mode of the zone: ■ Yellow - **Learn/Detect** mode. ■ Grey - **Prevent** mode.
Table view	
Zone	Name of the zone.
Family	Family in which the assets in the zone belong. ■ IoT ■ Generic
Profile	Profile of the agent.
Protection	Sub-practice mode of the zone ■ Yellow - **Learn/Detect** mode. ■ Grey - **Prevent** mode.
>	Click to view detailed information about the zone in these tabs: ■ *"General" below* ■ *"Access Control" on the next page* ■ *"Threat Prevention" on page 48* ■ *"Custom Rules and Exceptions" on page 49* ■ *"Events" on page 51* ■ *"Practices" on page 53*

General

Shows the basic information about the zone and the query run to add the asset to the zone.



Basic

Name: *
AV receivers

Device function:
AV receiver

Recognition confidence threshold:
Medium

Query

This query is auto generated according to the IoT assets function and the discovery confidence level

Schema:

AND
assetFunction : AV receiver
recognitionConfidence {} Medium,High

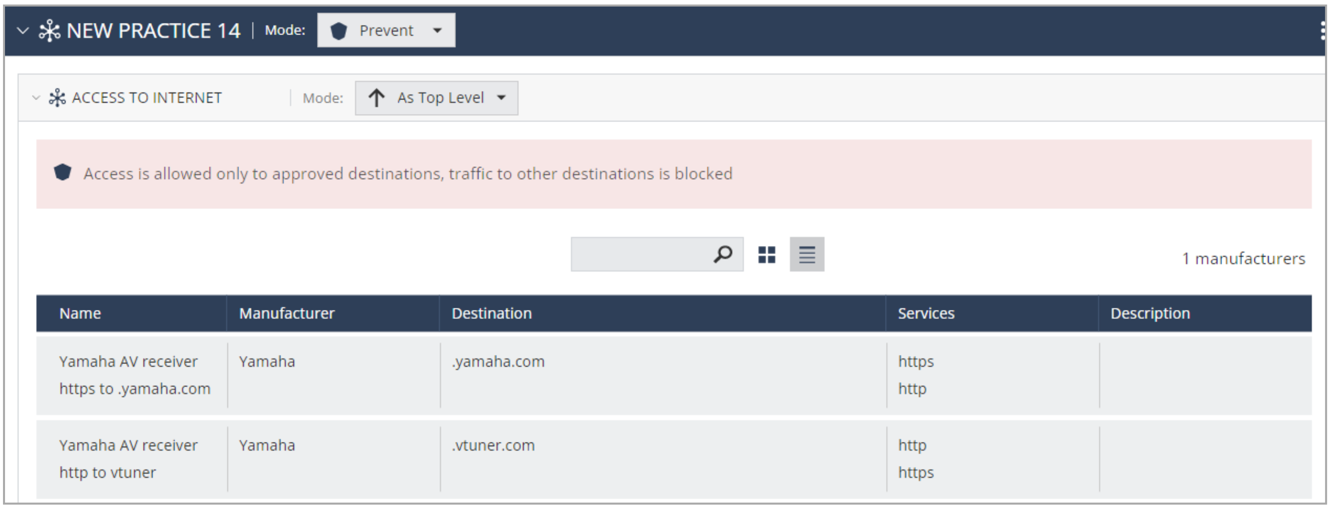
Item	Description
Basic	■ **Name** - Name of the zone. ■ **Device function** - Function of the asset. ■ **Recognition confidence threshold** - The minimum confidence level required to add an asset to the zone.
Query	Query that the system runs to categorize a discovered IoT asset to a zone. By default, the asset discovery confidence level (**recoginitionConfidence** parameter) is set to **Medium** and **High**. To update the query, change the required field value(s) under the **Basic** section.

Access Control

You can define the access control mode for the zone that is applied to all the assets in the zone.

The mode for a zone is set through practice and sub-practice(s). A sub-practice inherits the mode from its parent practice by default.

In this example, **New Practice 14** is the parent practice and **Access to Internet** is the sub-practice.



Access is allowed only to approved destinations, traffic to other destinations is blocked

1 manufacturers

Name	Manufacturer	Destination	Services	Description
Yamaha AV receiver https to .yamaha.com	Yamaha	.yamaha.com	https http	
Yamaha AV receiver http to vtuner	Yamaha	.vtuner.com	http https	

To define the access control mode:

1. In the **New Practice** > **Mode**, select a mode:

   Note - The default mode is **Learn / Detect**.

   - **Prevent** - Allows access only to the domains in the approved destinations list. Access to all other domains is blocked. For more information, see *"Approved Destinations" below*.
   - **Disabled** - Does not monitor and secure the asset.
   - **Learn / Detect** - Monitors the traffic without blocking it.This is the recommended mode for the initial three to six months after you provision the asset. This helps in analyzing the traffic and setting up policies. Once the policies are configured, the mode should be switched to **Prevent**.

2. Select a **Mode** for the sub-practice(s):

   Note - The default mode is **Learn / Detect**.

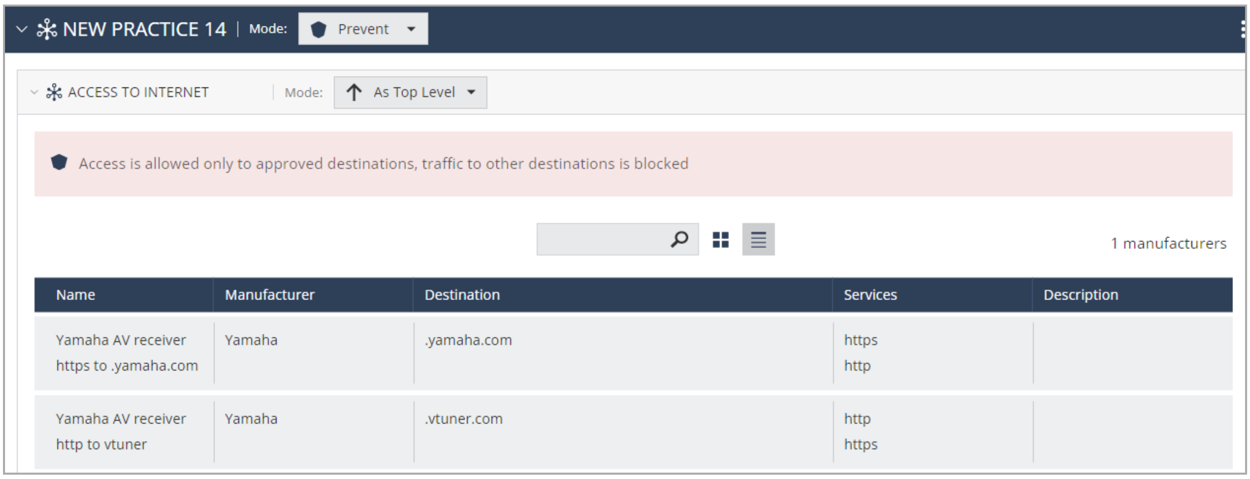
   - **As Top Level** - Applies the same access mode as its parent practice.
   - **Disabled** - Does not monitor and secure the asset.
   - **Learn / Detect** - Monitors the asset traffic but does not block it even if it violates the policy.
   - **Prevent** - Allows access only to the domains in the approved destinations list. Access to all other domains is blocked.

Approved Destinations

Check Point maintains a list of approved destinations for every zone. The access to the approved destinations depends on the mode you set.

To view the approved destinations for a zone:

- In card view, on the zone card, hover the cursor over the **approved destinations** text.
- In table view, see the **Destination** column.



NEW PRACTICE 14 | Mode: Prevent

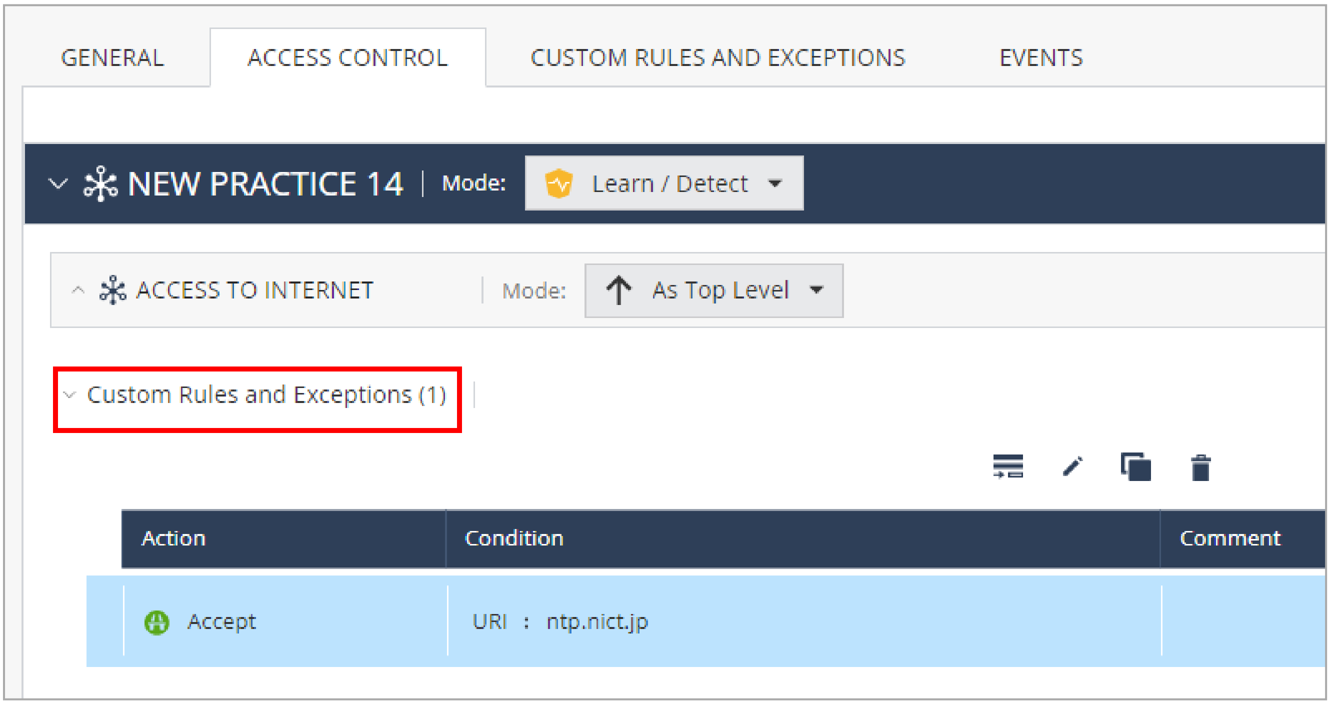
ACCESS TO INTERNET | Mode: As Top Level

Access is allowed only to approved destinations, traffic to other destinations is blocked

1 manufacturers

Name	Manufacturer	Destination	Services	Description
Yamaha AV receiver https to .yamaha.com	Yamaha	.yamaha.com	https http	
Yamaha AV receiver http to vtuner	Yamaha	.vtuner.com	http https	

To allow access to a destination not in the approved destination list, add a custom rule or exception. To add or edit a custom rule or exception, expand the **Custom Rules and Exceptions** drop-down and follow the steps in *"Custom Rules and Exceptions" on page 49*.



NEW PRACTICE 14 | Mode: Learn / Detect

ACCESS TO INTERNET | Mode: As Top Level

Custom Rules and Exceptions (1)

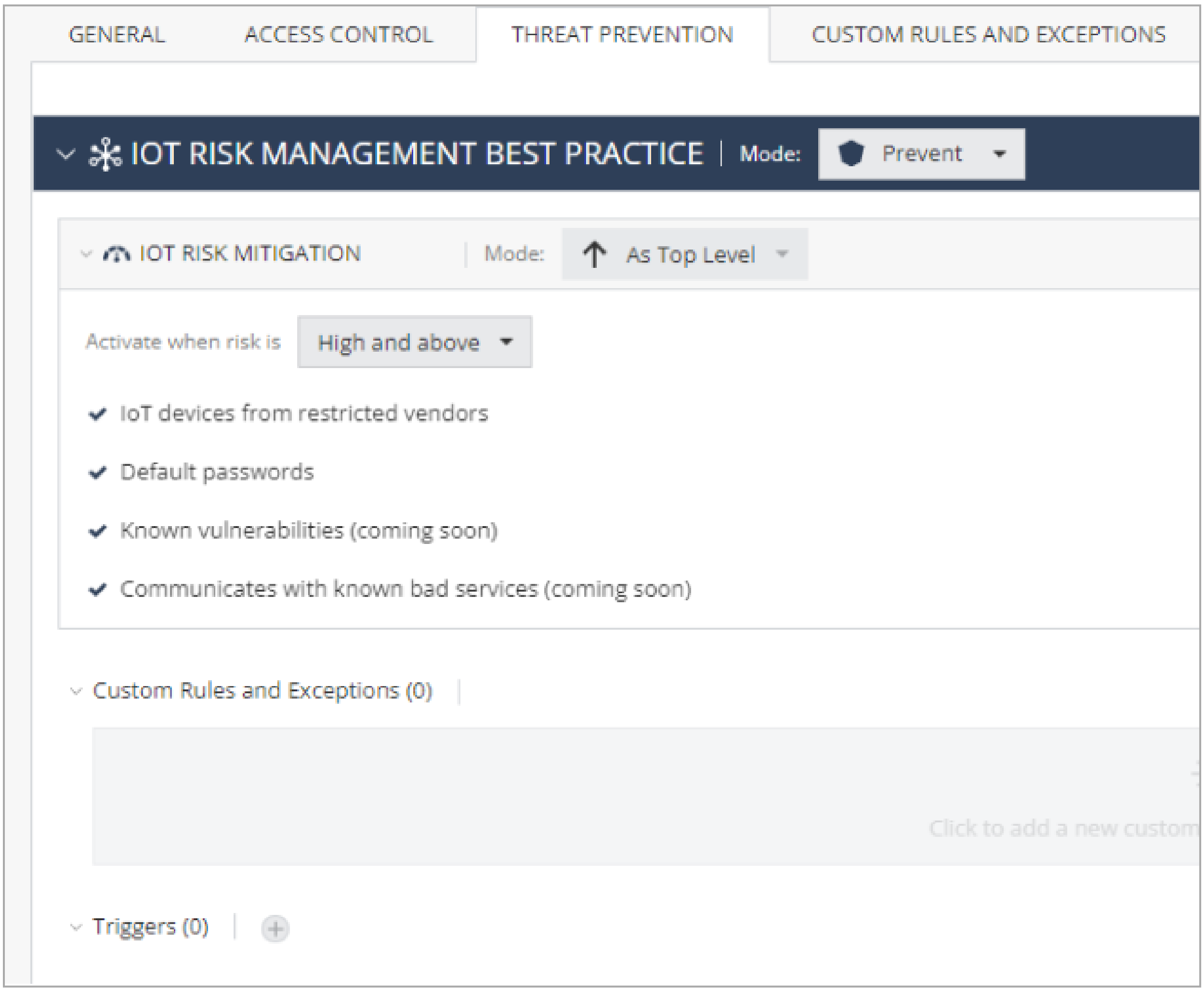
Action	Condition	Comment
Accept	URI : ntp.nict.jp	

Note - For Quantum IoT Protect, the data fields in the **Triggers** section are automatically populated. Do not make any changes in this section.

Threat Prevention

Threat Prevention allows you to set a mode of action when an asset's risk level matches the specified risk level. The supported modes are:

- **Learn / Detect** - Monitors the traffic without blocking it.This is the recommended mode for the initial three to six months after you provision the asset. This helps in analyzing the traffic and setting up policies. Once the policies are configured, the mode should be switched to **Prevent**.
- **Prevent** - Blocks the traffic if the asset's risk level matches the specified level.
- **Disabled** - Threat Prevention is disabled. No action is taken if the asset's risk level matches the specified level.


GENERAL
ACCESS CONTROL
THREAT PREVENTION
CUSTOM RULES AND EXCEPTIONS
IOT RISK MANAGEMENT BEST PRACTICE
IOT RISK MITIGATION
Custom Rules and Exceptions (0)
Click to add a new custom
Triggers (0)

Mode: Prevent

Mode: As Top Level

Activate when risk is: High and above

- ✓ IoT devices from restricted vendors
- ✓ Default passwords
- ✓ Known vulnerabilities (coming soon)
- ✓ Communicates with known bad services (coming soon)

Notes:

- Make sure you have configured the *"IoT Risk Profile" on page 59*.
- If you have subscribed to Check Point Infinity Playblocks and configured a workflow to handle IoT assets with a certain risk level, then skip this procedure. Infinity Playblocks automatically sends you a notification to enforce an action.

To set a mode for an IoT asset with a certain risk level:

1. Go to **Threat Prevention** and set the practice **Mode** to one of these:
   - **Learn / Detect**
   - **Prevent**
   - **Disabled**
2. In the **Activate when risk is** drop-down list, select the risk level.
3. Click **Enforce**.

   All the IoT assets in the zone with the selected risk level are blocked.
4. To allow traffic to an asset identified as risky, add an exception in **Custom Rules and Exceptions**. For more information, see *"Custom Rules and Exceptions" below*.

Note - For Quantum IoT Protect, the data fields in the **Triggers** section are automatically populated. Do not make any changes in this section.

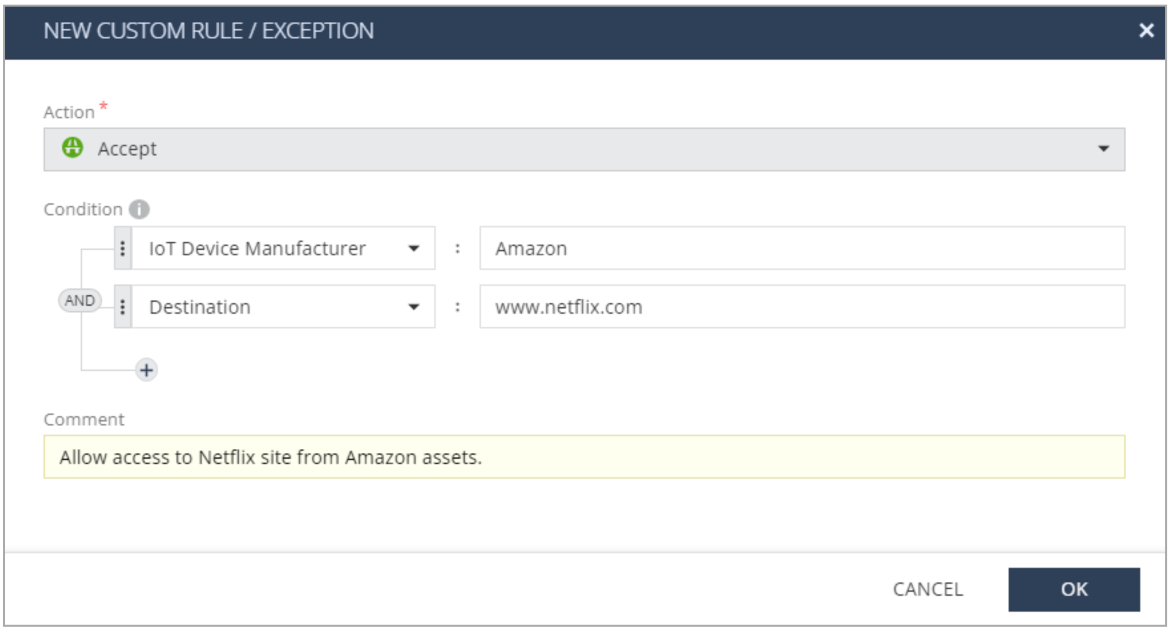
Custom Rules and Exceptions

You can create custom rules and exceptions, for example, to allow or block traffic between an IoT asset and destination.

To add a new custom rule or exception:

1. Click ✳.
2. In the **New Custom Rule / Exception** window:

- Select an **Action**.
- Set the **Condition**:
  1. Select the parameter:
     - IoT Device Manufacturer
     - Destination
     - Service
  2. Click **:** to select the qualifier.
  3. Enter the value for the parameter.
  4. To add the second condition, click ⋮ to specify the operator (AND or OR) and repeat the steps from a to c.
- (Optional) **Comment**



NEW CUSTOM RULE / EXCEPTION

Action *

Accept

Condition

AND

IoT Device Manufacturer : Amazon

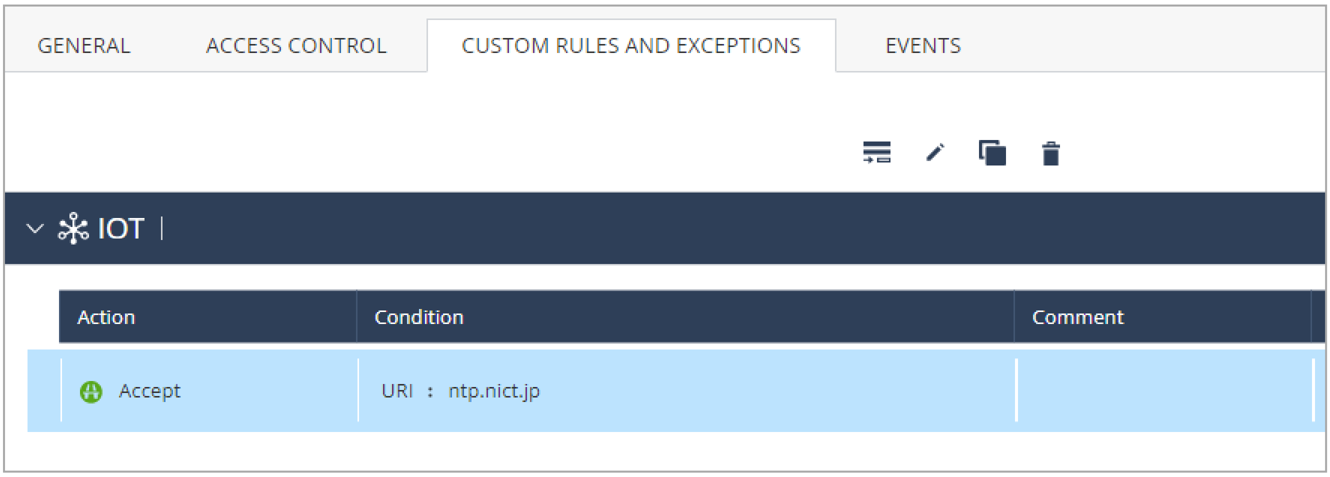
Destination : www.netflix.com

Comment

Allow access to Netflix site from Amazon assets.

3. Click **OK**.

To edit, clone and delete an existing custom rule or exception:



Action	Condition	Comment
Accept	URI : ntp.nict.jp	

1. To edit:
   a. Click ✎.
   b. In the **Edit Exception** window, enter the required changes.
   c. Click **OK**.
2. To clone, click ⧉ .

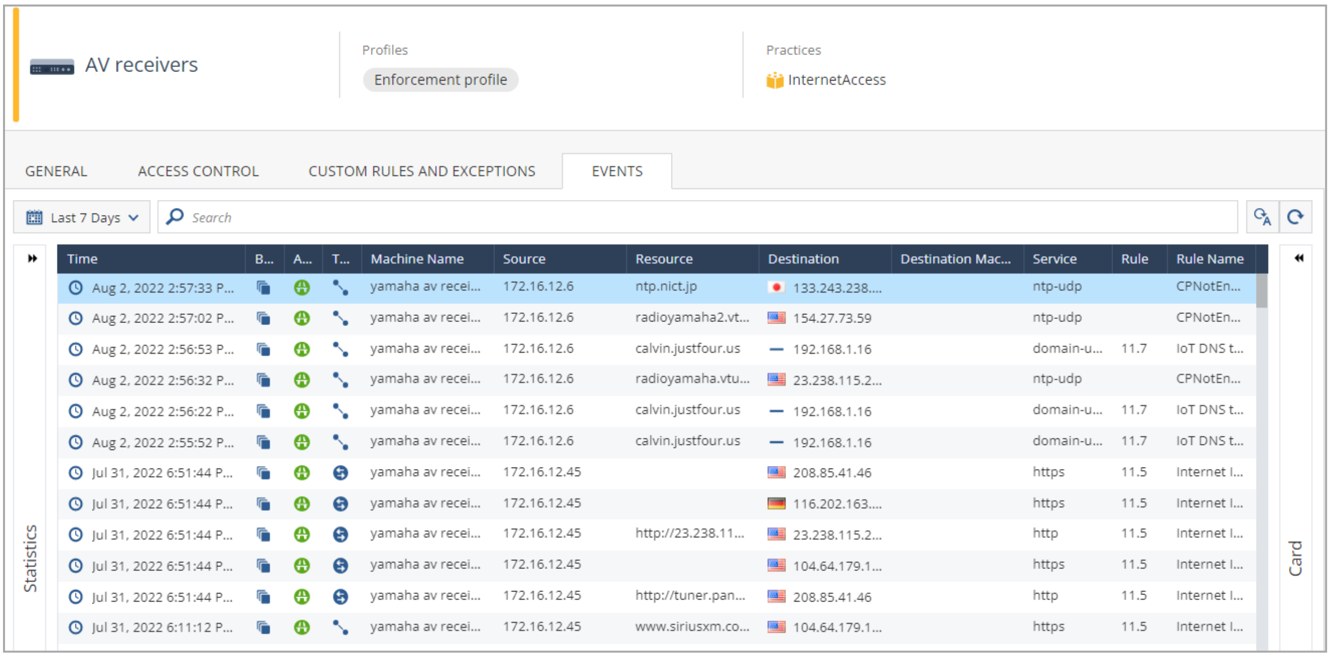
   The existing exception is cloned and added to the list.
3. To delete, select the exception and click 🗑 .

Events

View the events logged for all the assets in the zone.

To view the event statistics, click ⏩ in the **Statistics** bar on the left.

For card view, click ⏪ in the **Card** bar on the right.



AV receivers

Profiles

Enforcement profile

Practices

InternetAccess

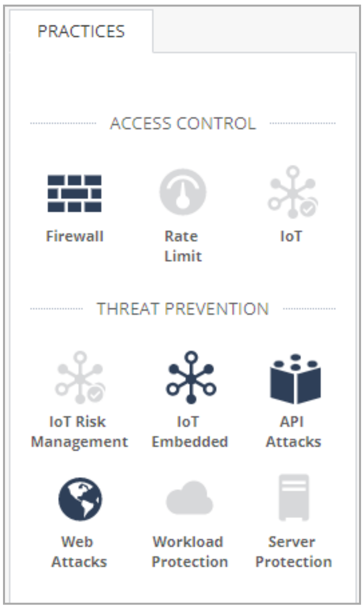
Time	B...	A...	T...	Machine Name	Source	Resource	Destination	Destination Mac...	Service	Rule	Rule Name
Aug 2, 2022 2:57:33 P...				yamaha av recei...	172.16.12.6	ntp.nict.jp	133.243.238....		ntp-udp		CPNotEn...
Aug 2, 2022 2:57:02 P...				yamaha av recei...	172.16.12.6	radioyamaha2.vt...	154.27.73.59		ntp-udp		CPNotEn...
Aug 2, 2022 2:56:53 P...				yamaha av recei...	172.16.12.6	calvin.justfour.us	— 192.168.1.16		domain-u...	11.7	IoT DNS t...
Aug 2, 2022 2:56:32 P...				yamaha av recei...	172.16.12.6	radioyamaha.vtu...	23.238.115.2...		ntp-udp		CPNotEn...
Aug 2, 2022 2:56:22 P...				yamaha av recei...	172.16.12.6	calvin.justfour.us	— 192.168.1.16		domain-u...	11.7	IoT DNS t...
Aug 2, 2022 2:55:52 P...				yamaha av recei...	172.16.12.6	calvin.justfour.us	— 192.168.1.16		domain-u...	11.7	IoT DNS t...
Jul 31, 2022 6:51:44 P...				yamaha av recei...	172.16.12.45		208.85.41.46		https	11.5	Internet I...
Jul 31, 2022 6:51:44 P...				yamaha av recei...	172.16.12.45		116.202.163....		https	11.5	Internet I...
Jul 31, 2022 6:51:44 P...				yamaha av recei...	172.16.12.45	http://23.238.11...	23.238.115.2...		http	11.5	Internet I...
Jul 31, 2022 6:51:44 P...				yamaha av recei...	172.16.12.45		104.64.179.1...		https	11.5	Internet I...
Jul 31, 2022 6:51:44 P...				yamaha av recei...	172.16.12.45	http://tuner.pan...	208.85.41.46		http	11.5	Internet I...
Jul 31, 2022 6:11:12 P...				yamaha av recei...	172.16.12.45	www.siriusxm.co...	104.64.179.1...		https	11.5	Internet I...

Event Parameter	Description
Time	Time of the event.
Blade	Software blade which triggered the logs: - Firewall - IoT - IoT URL Filtering - Application Control IoT
Action	Action enforced on the event: - Drop - Block. - Accept - Allow.
Type	- Connection - Event generated in an individual connection. - Session - Event generated in a session.
Machine Name	Name of the asset.
Source	IP address of the IoT asset.
Resource	Resource accessed by the asset.
Destination	IP address of the destination.
Destination Machine Name	Name of the destination asset.
Service	Service that generated the event.

Event Parameter	Description
Rule	Rule number from the relevant policy package and Rulebase (Examples - 7.1, 11.5).
Rule Name	Name of the rule (Examples - Internet IoT all, IoT DNS to internal).

Practices

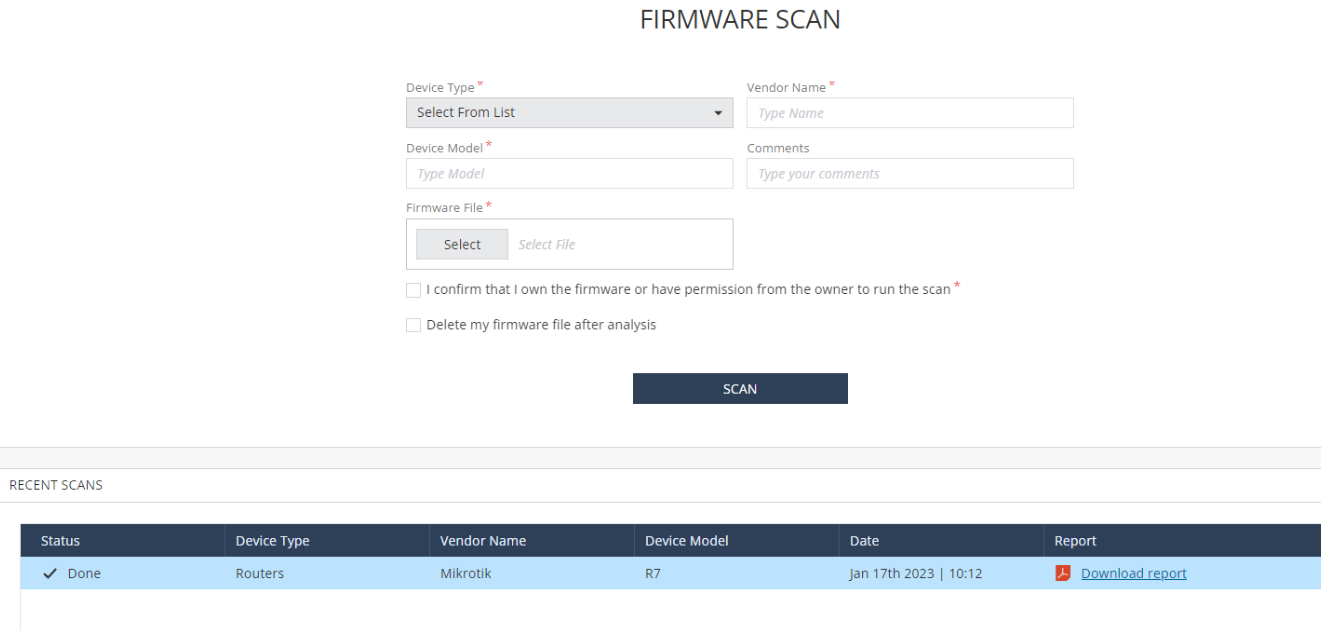
Shows the different **Access Control** and **Threat Prevention** practices applied on the zone.



Firmware Scan

With firmware scan, you can scan the firmware of an IoT device and view its risk assessment report.

The Firmware Risk Assessment Report is generated based on static analysis.



FIRMWARE SCAN

Device Type *
Select From List

Vendor Name *
Type Name

Device Model *
Type Model

Comments
Type your comments

Firmware File *
Select | Select File

□ I confirm that I own the firmware or have permission from the owner to run the scan *

□ Delete my firmware file after analysis

SCAN

RECENT SCANS

Status	Device Type	Vendor Name	Device Model	Date	Report
✓ Done	Routers	Mikrotik	R7	Jan 17th 2023 | 10:12	Download report

Firmware File Prerequisites

- To get the firmware file of the IoT device, visit the device manufacturer's website or contact the manufacturer. For example, support.hp.com.
- The firmware file must not be password protected or encrypted.
- The firmware file must be an archived Linux file system.

  The supported archive formats are:

  - gzip (.gz)
  - lzma (.7z)
  - xz (.xz)
  - bzip2 (.bz2)
  - tar (.tar)
  - rar (.rar)
  - arj (.arj)

    - lha (.lha)
    - iso 9660 (.iso)
    - cabinet archives (.cab)
    - stuffit (.sit)
    - OS X archives (.dmg)
    - lzo (.lzo)
    - intel hex (.hex)
    - motorola s-record (.srec)
    - zip (.zip)
    - squashfs (.squashfs)
    - cramfs (.cramfs)
    - EXT (.ext2)
    - romfs (.romfs)
    - jffs2 (.jffs2)
    - ubifs (.ubi)

- To obtain a compressed firmware file:
    - On Windows, use 7-Zip.
    - On Linux, use tar to create a .tar.gz of the entire folder. For example, to compress everything under the folder `/usr`, run:

      ```
      ./tar --one-file-system -pczf ./firmware.tar.gz /usr
      ```

      On Linux, to compress everything under root and add exclusions for temporary or irrelevant runtime directories, run:

      ```
      ./tar --one-file-system -pczf --exclude=mnt --exclude=var --exclude=tmp --exclude=run --exclude=proc --exclude=sys ./firmware.tar.gz /
      ```

To scan a firmware and generate the risk assessment report:

1. Go to **IoT** > **Firmware Scan**.
2. Enter:
    - **Device Type**
    - **Vendor Name**

  - **Device Model**
  - (Optional) **Comments**

3. In **Firmware File** field, click **Select** and upload the firmware file.
4. Select the **I confirm that I own the firmware or have the permission from the owner to run the scan** checkbox.
5. (Optional) Select the **Delete my firmware file after analysis** checkbox.

   If you select it, the firmware file is deleted from the service's storage after the scan. Otherwise, the file is archived for future analytics or debug purposes.
6. Click **Scan**.
7. In the **Recent Scans** section, you can view the status of the file scan.

   When the scan is complete, the Firmware Risk Assessment report is available for download. If the scan fails, a Check Point representative will contact you.
8. To download the report, in the **Report** column, click **Download report**.

   For a sample report, click here.

   The report shows:

   - Known Vulnerabilities - List of all CVEs classified based on their severity and attack vector (network/physical attack).
   - Weak Credentials - Credentials that are easy to crack or publicly available.
   - High Risk Domains / IP Addresses - Suspicious domains and IP addresses.
   - Action Items - Key recommendations to mitigate security flaws.
9. Share the risk assessment report with the device vendor or manufacturer to take the required action.

Triggers

Quantum IoT Protect automatically sets the parameters for logs when you onboard an IoT asset.

To view log trigger settings, go to **IoT** > **Triggers**.

Note - We do not recommend changing the default settings.

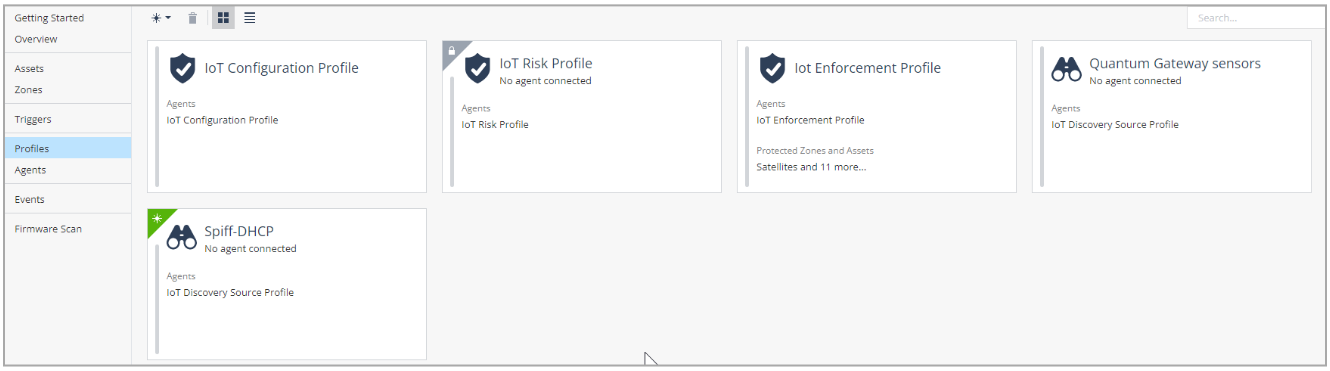
Profiles

Quantum IoT Protect automatically creates a profile for the gateway that is connected to the IoT assets in your network. A profile shows the source and the technologies used to discover IoT assets, and the Quantum Security Gateways that function as sensors.

When you complete onboarding IoT assets, Quantum IoT Protect creates these profiles by default:

- Enforcement Profile
- IoT Risk Profile
- IoT Configuration Profile
- Quantum Gateway Sensor Profile (with **Discovery source type** as **Security Gateway Sensor**)

The **Profiles** page shows the default profiles and profiles that you manually create. **Spiff-DHCP** is an example of a manually created profile.



IoT Configuration Profile
Agents
IoT Configuration Profile

IoT Risk Profile
No agent connected
Agents
IoT Risk Profile

Iot Enforcement Profile
Agents
IoT Enforcement Profile
Protected Zones and Assets
Satellites and 11 more...

Quantum Gateway sensors
No agent connected
Agents
IoT Discovery Source Profile

Spiff-DHCP
No agent connected
Agents
IoT Discovery Source Profile

Enforcement Profile

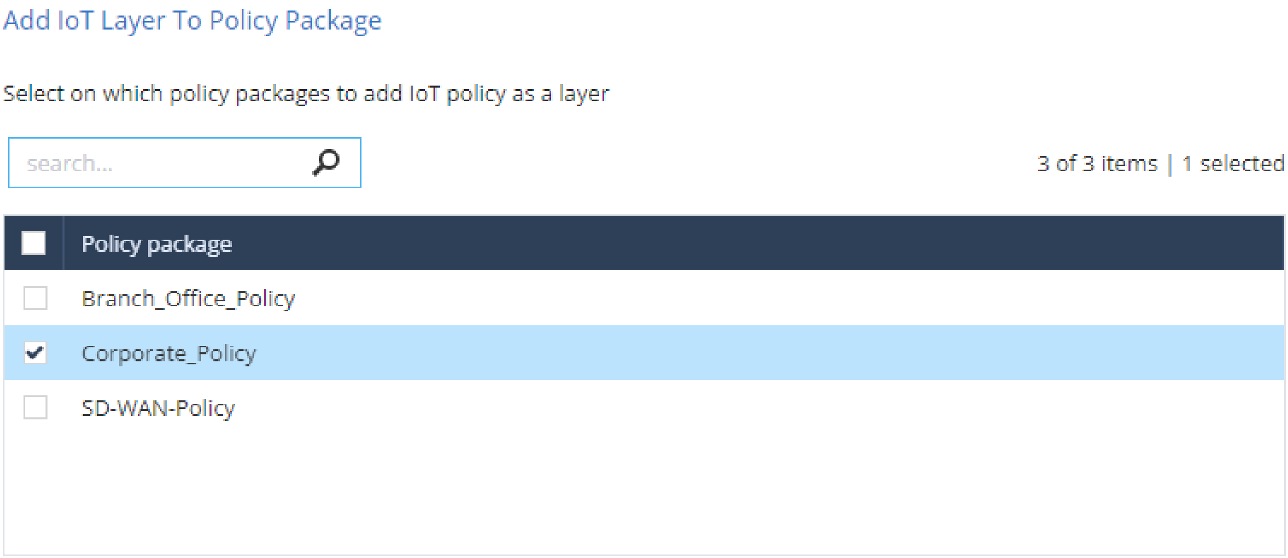
The Enforcement profile (or IoT Enforcement profile) maps the IoT policy to the Assets and Zones discovered in other profiles, for enforcement on Security Gateway(s).

Note - Assets and Zones are tied to the Enforcement profile when they are discovered by other profile(s).

You can select the policy package and the Security Gateway(s) in the profile configuration settings explained below.

Add IoT Layer To Policy Package

Select a policy package to enforce on the onboarded IoT assets.



Add IoT Layer To Policy Package

Select on which policy packages to add IoT policy as a layer

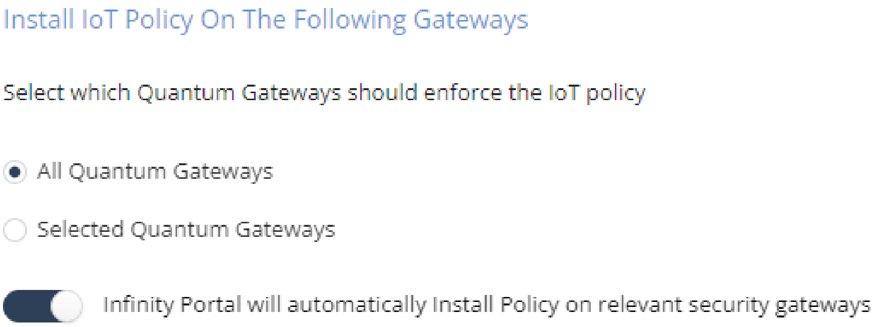
search...

3 of 3 items | 1 selected

□	Policy package
□	Branch_Office_Policy
☑	Corporate_Policy
□	SD-WAN-Policy

Install IoT Policy On the Following Gateways

Select the gateway to install the policy package. The **Infinity Portal will automatically install policy on relevant security gateways** option is enabled by default.



Install IoT Policy On The Following Gateways

Select which Quantum Gateways should enforce the IoT policy

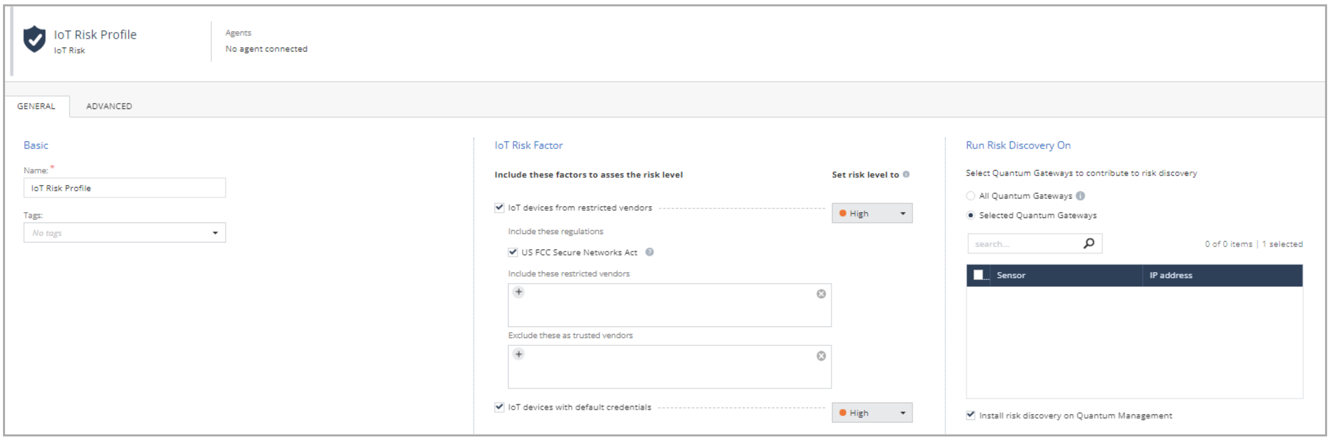
● All Quantum Gateways

○ Selected Quantum Gateways

Infinity Portal will automatically Install Policy on relevant security gateways

IoT Risk Profile

IoT Risk Profile shows the different factors that are considered to evaluate the risk of IoT assets and allows you to set a risk level for these factors. You can view the risk value of assets in the Assets page.



IoT Risk Profile
IoT Risk

Agents
No agent connected

Basic

Name: *
IoT Risk Profile

Tags:
No tags

IoT Risk Factor

Include these factors to asses the risk level — Set risk level to

☑ IoT devices from restricted vendors — High

Include these regulations

☑ US FCC Secure Networks Act

Include these restricted vendors

Exclude these as trusted vendors

☑ IoT devices with default credentials — High

Run Risk Discovery On

Select Quantum Gateways to contribute to risk discovery

○ All Quantum Gateways

● Selected Quantum Gateways

search...

0 of 0 items | 1 selected

□	Sensor	IP address

☑ Install risk discovery on Quantum Management

IoT Risk Factor

The risk level of an IoT asset is assessed based on the risk values set for these factors:

Restricted Vendors

You can define the list of restricted IoT vendors and set a risk level. When a restricted IoT vendor is detected, the system applies the set risk level and enforces the responsive action configured in Infinity Playblocks or *"Threat Prevention" on page 48*.

To define the list of restricted IoT vendors and set a risk level:

1. Select the **IoT devices from restricted vendors** checkbox and set one of these risk levels:
   - (Recommended) High
   - Critical
   - Medium
   - Low
2. To include vendors restricted by the US FCC Secure Network Act to the restricted vendors list, select the **US FCC Secure Networks Act** checkbox.

   The restricted vendors are:
   - Huawei
   - ZTE
   - Hytera
   - Hikvision
   - Dahua
3. To add a vendor to the restricted list:
   1. In the **Include these restricted vendors** section, click **+**.
   2. Select the vendors that you want to add to the restricted vendors list.
   3. Click **OK**.
   4. Click **Enforce**.

      The vendor is now considered as a restricted vendor and the assets from this vendor will be set with risk level.
4. To remove a vendor from restricted list:

a. In the **Exclude these as trusted vendors** section, click **+**.

b. Select the vendors that you want to exclude from the restricted list.

c. Click **OK**.

d. Click **Enforce**.

   The vendor is now considered as a trusted vendor and the assets from this vendor are not assigned any risk level.

Default Credentials

You can set a risk level for IoT assets that use commonly exploited login credentials or use default credentials supplied by the manufacturer.

Check Point maintains an up-to-date database of commonly exploited login credentials and the default credentials supplied by the manufacturer. It attempts to log in to the IoT assets using these credentials through protocols, such as SSH, Telnet, FTP and so on. A successful attempt implies a significant risk of compromise and allows you to set a risk level for such IoT assets.

To assign a risk level, select the **IoT devices with default credentials** checkbox and set one of these risk levels:

- (Recommended) High
- Critical
- Medium
- Low

Run Risk Discovery On

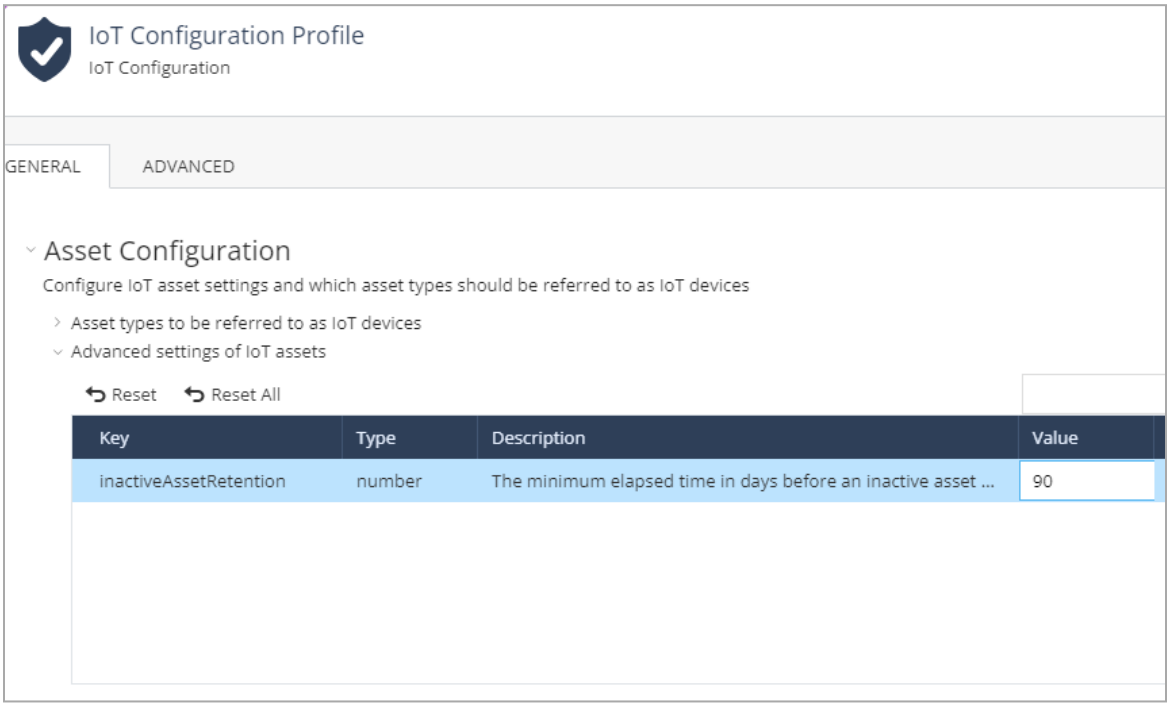
Shows the Quantum Security Gateways used to discover IoT assets with risk.

To run risk discovery on Quantum Management Server, select the **Install risk discovery on Quantum Management** checkbox.

IoT Configuration Profile

The IOT Configuration profile shows the asset types that should be discovered as IoT assets, advanced configuration, and default settings for zones.

- **Asset Configuration**:
  - Select whether the asset types must be considered as IoT assets or not.
  - Set the retention period for inactive assets in the **inactiveAssetRetention** key. The default is 90 days. After the retention period, Quantum IoT Protect automatically deletes the asset.



IoT Configuration Profile

IoT Configuration

Asset Configuration

Configure IoT asset settings and which asset types should be referred to as IoT devices

Asset types to be referred to as IoT devices
Advanced settings of IoT assets
Reset
Reset All

Key	Type	Description	Value
inactiveAssetRetention	number	The minimum elapsed time in days before an inactive asset ...	90

- **Collector Configuration**:

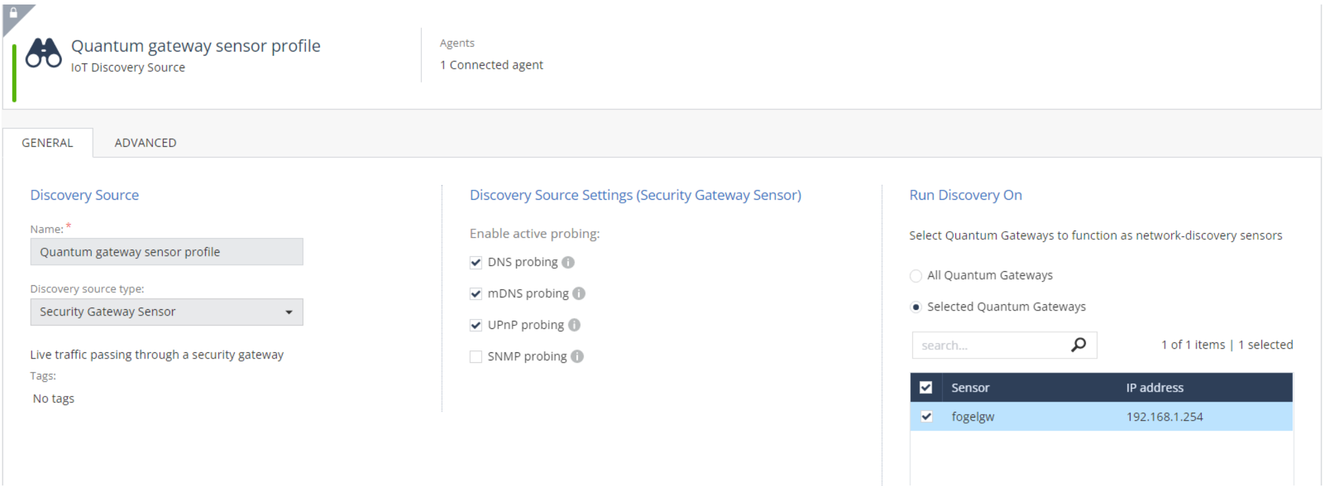
  Shows settings for the IoT discovery engines.

- **Zone Matcher Configuration**:

  Shows settings for the IoT zones.

Note - We recommend not to modify these settings. If you want to modify, contact *Check Point Support*.

Quantum Gateway Sensor Profile



Quantum gateway sensor profile
IoT Discovery Source

Agents
1 Connected agent

Discovery Source

Name: *
Quantum gateway sensor profile

Discovery source type:
Security Gateway Sensor

Live traffic passing through a security gateway

Tags:
No tags

Discovery Source Settings (Security Gateway Sensor)

Enable active probing:

☑ DNS probing
☑ mDNS probing
☑ UPnP probing
□ SNMP probing

Run Discovery On

Select Quantum Gateways to function as network-discovery sensors

○ All Quantum Gateways
● Selected Quantum Gateways

search...

1 of 1 items | 1 selected

☑	Sensor	IP address
☑	fogelgw	192.168.1.254

Discovery Source

Shows the discovery source name and source type.

Discovery Source Settings

Shows the technologies used to discover IoT assets.

Run Discovery On

Shows the Quantum Security Gateways used to discover IoT assets.

Profiles for Advanced IoT Discovery Engines

You can manually create a profile if you want to use a different discovery source type. For more information, see:

- *"Appendix B - Using SNMP as the IoT Discovery Engine" on page 78*.
- *"Appendix C - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory)" on page 89*.
- *"Appendix D - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Splunk)" on page 106*.
- *"Appendix E - Using Unix DHCP - Syslog as the IoT Discovery Engine" on page 115*.
- *"Appendix F - Using Unix DHCP as the IoT Discovery Engine" on page 129*.
- *"Appendix G - Using Cisco ISE as the IoT Discovery Engine" on page 143*.
- *"Appendix H - Using Infoblox DHCP - Syslog as the IoT Discovery Engine" on page 154*.
- *"Appendix I - Integrating IoT Assets using Third-Party Discovery Engines through APIs" on page 162*

Agents

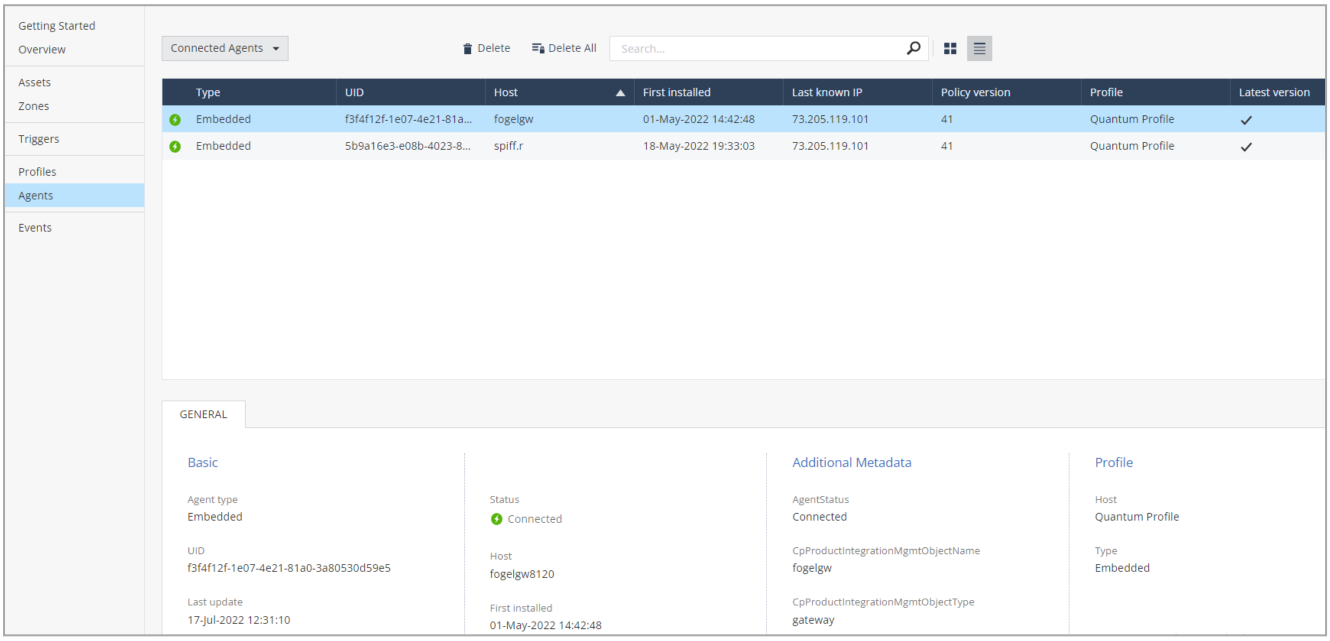
An agent is a piece of software installed and deployed automatically on the Security Gateway or on the Management Server that gathers and reports the IoT asset metadata to Quantum IoT Protect. The **Agent** page shows the details of the agent to know whether an agent is running or not.

To access the **Agents** page, go to **IoT** > **Agents**.

Filter and select the required agent view from the drop-down list in the top-right corner:

- All Agents
- Connected Agents (Default) - Agents that communicated with the Gateway or the Management Server in the last 15 minutes, indicated with a green banner.
- Disconnected Agents - Agents that have not communicated with the Gateway or the Management Server for over 15 minutes.

  Note - A disconnected agent may also indicate that the gateway it is installed on is offline, or the connectivity to Check Point cloud is disrupted. When an agent which should be connected, is disconnected, verify the Web Server/Reverse Proxy that agent is installed on is live and is with connectivity.



	Type	UID	Host	First installed	Last known IP	Policy version	Profile	Latest version
●	Embedded	f3f4f12f-1e07-4e21-81a...	fogelgw	01-May-2022 14:42:48	73.205.119.101	41	Quantum Profile	✓
●	Embedded	5b9a16e3-e08b-4023-8...	spiff.r	18-May-2022 19:33:03	73.205.119.101	41	Quantum Profile	✓

Basic

Agent type: Embedded

UID: f3f4f12f-1e07-4e21-81a0-3a80530d59e5

Last update: 17-Jul-2022 12:31:10

Status: ● Connected

Host: fogelgw8120

First installed: 01-May-2022 14:42:48

Additional Metadata

AgentStatus: Connected

CpProductIntegrationMgmtObjectName: fogelgw

CpProductIntegrationMgmtObjectType: gateway

Profile

Host: Quantum Profile

Type: Embedded

Item	Description
Type	Type of agent installation. **Embedded** - Agent installed on the security gateway.
UID	Unique ID of the agent.

Item	Description
Host	Gateway on which the agent is installed.
First Installed	Date when the agent was first installed.
Last known IP	Last known IP address of the agent.
Policy version	Number of times the policy was enforced on the agent. If the field is empty, it means the agent has registered but is currently being installed and has not yet received its first policy.
Profile	Gateway profile associated with the agent.
Latest version	Indicates whether the agent's software version is latest. It is recommended you always keep the agent updated as new versions are released frequently.
🗑	Delete an agent. **Note** - Before you delete an agent, make sure that you remove it from the gateway.

General

Shows the generic information about the selected agent.

Item	Description
Basic	
Agent type	Type of agent installation.
UID	Unique ID of the agent.
Last update	Date and time when the agent information was last updated.
Architecture	Specification of the processor used for the agent (For example, x86_64 indicates a 64-bit processor).
Agent version	Version of the agent.
Last known IP	Last known IP address of the agent.
Status	Indicates the connection status of the agent: ▪ Connected ▪ Disconnected

Item	Description
Host	Gateway on which the agent is installed.
First Installed	Date when the agent was first installed.
Platform	OS on which the agent is installed.
Policy version	Number of times the policy was enforced on the agent. If the field is empty, it means the agent has registered but is currently being installed and has not yet received its first policy.
IsLatestVersion	Indicates whether the latest version of the agent is running on the gateway: ■ True ■ False
Additional Metadata	
Shows additional metadata for the selected agent.	
Profile	
Host	Gateway profile associated with the agent.
Type	Type of agent installation.

Events

The **Events** page shows logs for:

- Important and generic events for the agent.
- IoT assets events.

To access the **Events** page, go to **IoT** > **Events**.

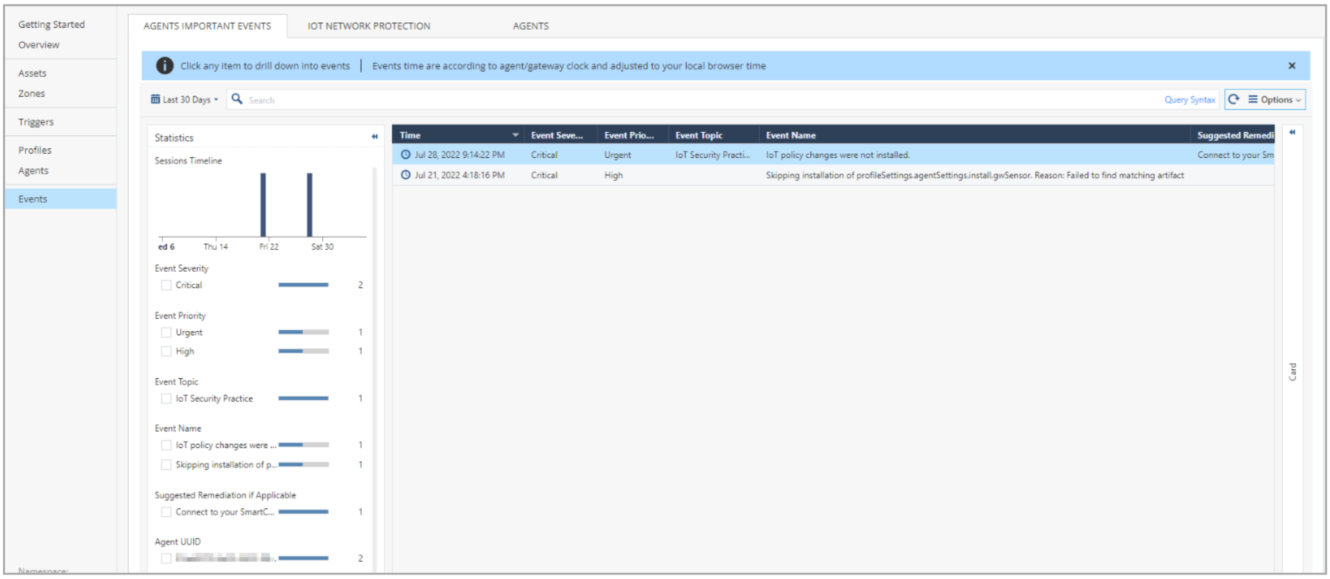
Note - You can also view the IoT events information in **IoT Protect** > **Monitor** > **IoT Events**.

Agent Important Events

Shows the logged important events for the agents.

To view the event statistics, click ⏩ in the **Statistics** bar on the left.

For card view, click ⏪ in the **Card** bar on the right.



Click any item to drill down into events | Events time are according to agent/gateway clock and adjusted to your local browser time

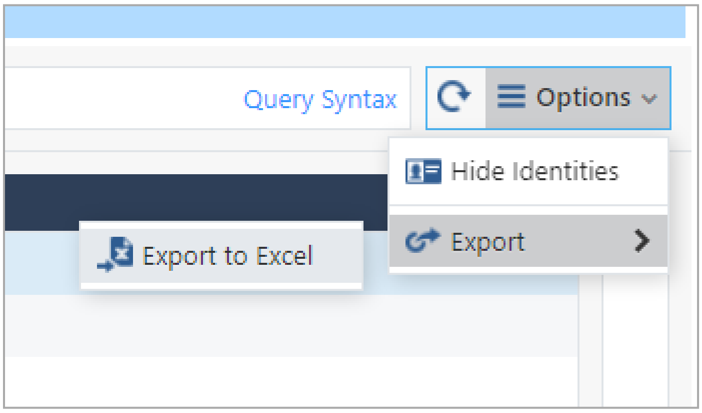
Time	Event Seve...	Event Prio...	Event Topic	Event Name	Suggested Remedi
Jul 28, 2022 9:14:22 PM	Critical	Urgent	IoT Security Practi...	IoT policy changes were not installed.	Connect to your Sm
Jul 21, 2022 4:18:16 PM	Critical	High		Skipping installation of profileSettings.agentSettings.install.gwSensor. Reason: Failed to find matching artifact	

Event Parameter	Description
Time	Time of the event.
Event Severity	Severity of the event: ■ Critical ■ Medium ■ Info

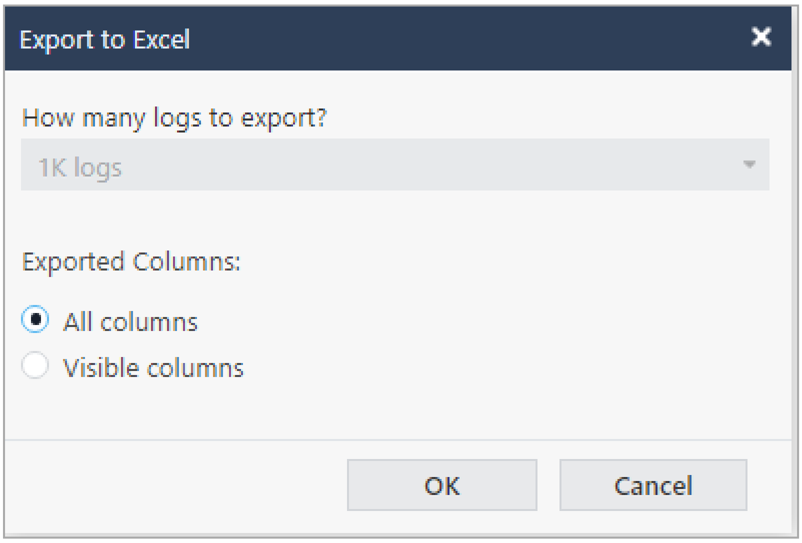
Event Parameter	Description
Event Priority	Priority to address the event: ■ Urgent ■ High ■ Medium ■ Low
Event Topic	Topic of the event.
Event Name	Name of the event.
Suggested Remediation if Applicable	Suggested solution to fix the issue (If applicable).
Agent UUID	Unique UID of the agent.

To export the Agents details to an Excel sheet:

1. Click **Options** > **Export** > **Export to Excel**.



2. In the **Export to Excel** window, select the columns you want to export.



Export to Excel

How many logs to export?

1K logs

Exported Columns:

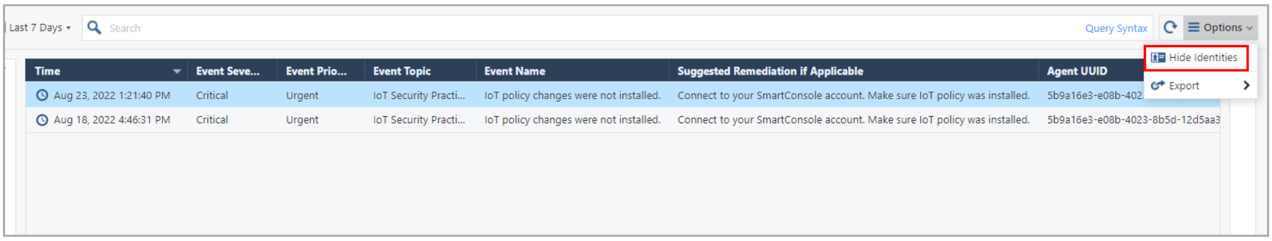
● All columns

○ Visible columns

3. Click **OK**.
4. In the **Exported Completed Successfully** pop-up, click **Download**.

   The logs Excel sheet is downloaded with the name format: Logs_Date_Time.xls (For example, *Logs_Aug_5__2022_11_58_50_AM.xls*)

Note - To obscure any user specific information in the events table, click the **Hide Identities** option.



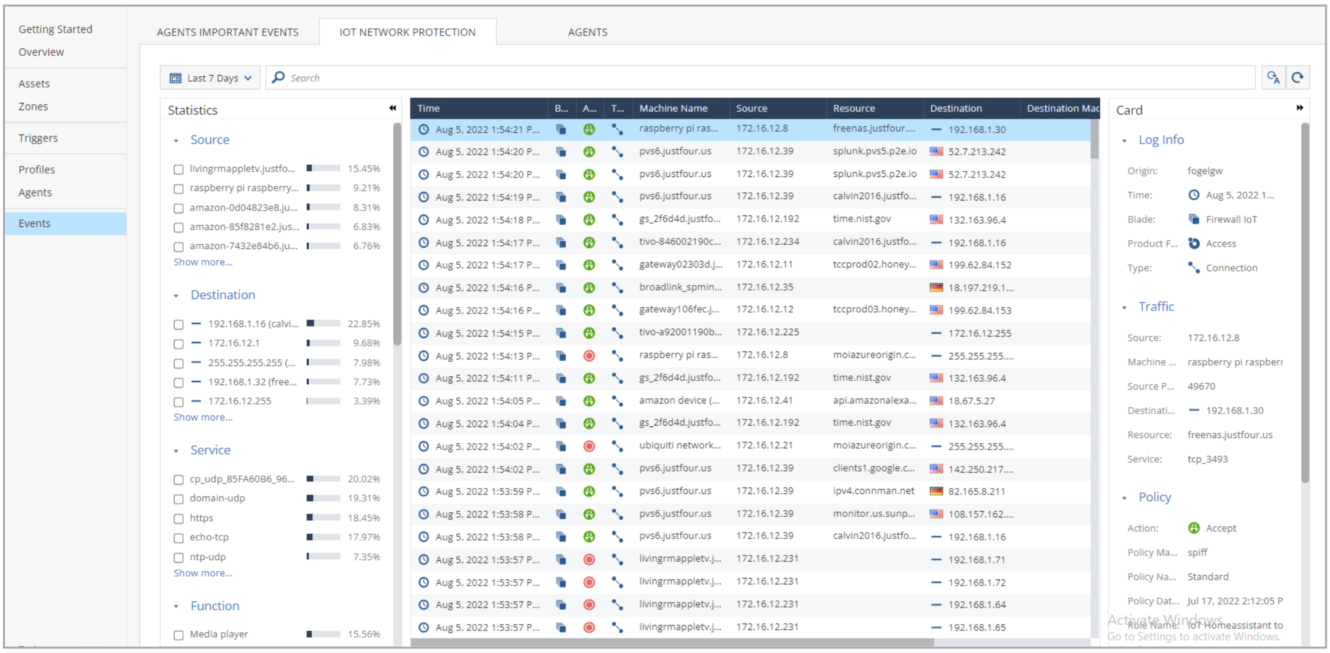
Time	Event Seve...	Event Prio...	Event Topic	Event Name	Suggested Remediation if Applicable	Agent UUID
Aug 23, 2022 1:21:40 PM	Critical	Urgent	IoT Security Practi...	IoT policy changes were not installed.	Connect to your SmartConsole account. Make sure IoT policy was installed.	5b9a16e3-e08b-402
Aug 18, 2022 4:46:31 PM	Critical	Urgent	IoT Security Practi...	IoT policy changes were not installed.	Connect to your SmartConsole account. Make sure IoT policy was installed.	5b9a16e3-e08b-4023-8b5d-12d5aa3

IoT Network Protection

Shows the logged events for all onboarded IoT assets.

To view the event statistics, click ⏩ in the **Statistics** bar on the left.

For card view, click ⏪ in the **Card** bar on the right.



Statistics

Source

□	livingrmappletv.justfo...	15.45%
□	raspberry pi raspberry...	9.21%
□	amazon-0d04823e8.ju...	8.31%
□	amazon-85f8281e2.jus...	6.83%
□	amazon-7432e84b6.ju...	6.76%

Show more...

Destination

□	— 192.168.1.16 (calvi...	22.85%
□	— 172.16.12.1	9.68%
□	— 255.255.255.255 (...	7.98%
□	— 192.168.1.32 (free...	7.73%
□	— 172.16.12.255	3.39%

Show more...

Service

□	cp_udp_85FA60B6_96...	20.02%
□	domain-udp	19.31%
□	https	18.45%
□	echo-tcp	17.97%
□	ntp-udp	7.35%

Show more...

Function

□	Media player	15.56%

Time	B...	A...	T...	Machine Name	Source	Resource	Destination	Destination Mac
Aug 5, 2022 1:54:21 P...	⧉	⊕	⤡	raspberry pi ras...	172.16.12.8	freenas.justfour....	— 192.168.1.30	
Aug 5, 2022 1:54:20 P...	⧉	⊕	⤡	pvs6.justfour.us	172.16.12.39	splunk.pvs5.p2e.io	52.7.213.242	
Aug 5, 2022 1:54:20 P...	⧉	⊕	⤡	pvs6.justfour.us	172.16.12.39	splunk.pvs5.p2e.io	52.7.213.242	
Aug 5, 2022 1:54:19 P...	⧉	⊕	⤡	pvs6.justfour.us	172.16.12.39	calvin2016.justfo...	— 192.168.1.16	
Aug 5, 2022 1:54:18 P...	⧉	⊕	⤡	gs_2f6d4d.justfo...	172.16.12.192	time.nist.gov	132.163.96.4	
Aug 5, 2022 1:54:17 P...	⧉	⊕	⤡	tivo-846002190c...	172.16.12.234	calvin2016.justfo...	— 192.168.1.16	
Aug 5, 2022 1:54:17 P...	⧉	⊕	⤡	gateway02303d.j...	172.16.12.11	tccprod02.honey...	199.62.84.152	
Aug 5, 2022 1:54:16 P...	⧉	⊕	⤡	broadlink_spmin...	172.16.12.35		18.197.219.1...	
Aug 5, 2022 1:54:16 P...	⧉	⊕	⤡	gateway106fec.j...	172.16.12.12	tccprod03.honey...	199.62.84.153	
Aug 5, 2022 1:54:15 P...	⧉	⊕	⤡	tivo-a92001190b...	172.16.12.225		— 172.16.12.255	
Aug 5, 2022 1:54:13 P...	⧉	◉	⤡	raspberry pi ras...	172.16.12.8	moiazureorigin.c...	— 255.255.255....	
Aug 5, 2022 1:54:11 P...	⧉	⊕	⤡	gs_2f6d4d.justfo...	172.16.12.192	time.nist.gov	132.163.96.4	
Aug 5, 2022 1:54:05 P...	⧉	⊕	⤡	amazon device (...	172.16.12.41	api.amazonalexa...	18.67.5.27	
Aug 5, 2022 1:54:04 P...	⧉	⊕	⤡	gs_2f6d4d.justfo...	172.16.12.192	time.nist.gov	132.163.96.4	
Aug 5, 2022 1:54:02 P...	⧉	◉	⤡	ubiquiti network...	172.16.12.21	moiazureorigin.c...	— 255.255.255....	
Aug 5, 2022 1:54:02 P...	⧉	⊕	⤡	pvs6.justfour.us	172.16.12.39	clients1.google.c...	142.250.217....	
Aug 5, 2022 1:53:59 P...	⧉	⊕	⤡	pvs6.justfour.us	172.16.12.39	ipv4.connman.net	82.165.8.211	
Aug 5, 2022 1:53:58 P...	⧉	⊕	⤡	pvs6.justfour.us	172.16.12.39	monitor.us.sunp...	108.157.162....	
Aug 5, 2022 1:53:58 P...	⧉	⊕	⤡	pvs6.justfour.us	172.16.12.39	calvin2016.justfo...	— 192.168.1.16	
Aug 5, 2022 1:53:57 P...	⧉	◉	⤡	livingrmappletv.j...	172.16.12.231		— 192.168.1.71	
Aug 5, 2022 1:53:57 P...	⧉	◉	⤡	livingrmappletv.j...	172.16.12.231		— 192.168.1.72	
Aug 5, 2022 1:53:57 P...	⧉	◉	⤡	livingrmappletv.j...	172.16.12.231		— 192.168.1.64	
Aug 5, 2022 1:53:57 P...	⧉	◉	⤡	livingrmappletv.j...	172.16.12.231		— 192.168.1.65	

Card

Log Info

Origin:	fogelgw
Time:	Aug 5, 2022 1...
Blade:	Firewall IoT
Product F...	Access
Type:	Connection

Traffic

Source:	172.16.12.8
Machine ...	raspberry pi raspberr
Source P...	49670
Destinati...	— 192.168.1.30
Resource:	freenas.justfour.us
Service:	tcp_3493

Policy

Action:	Accept
Policy Ma...	spiff
Policy Na...	Standard
Policy Dat...	Jul 17, 2022 2:12:05 P
Rule Name:	IoT Homeassistant to

Event Parameter	Description
Time	Time of the event.
Blade	Software blade which triggered the logs: ■ Firewall ■ IoT ■ IoT URL Filtering ■ Application Control IoT
Action	Action enforced on the event: ■ Drop - Block. ■ Accept - Allow.
Type	■ Connection - Event generated in an individual connection. ■ Session - Event generated in a session.
Machine Name	Name of the asset.
Source	IP address of the IoT asset.
Resource	Resource accessed by the asset.
Destination	IP address of the destination.
Destination Machine Name	Name of the destination asset.
Service	Service that generated the event.

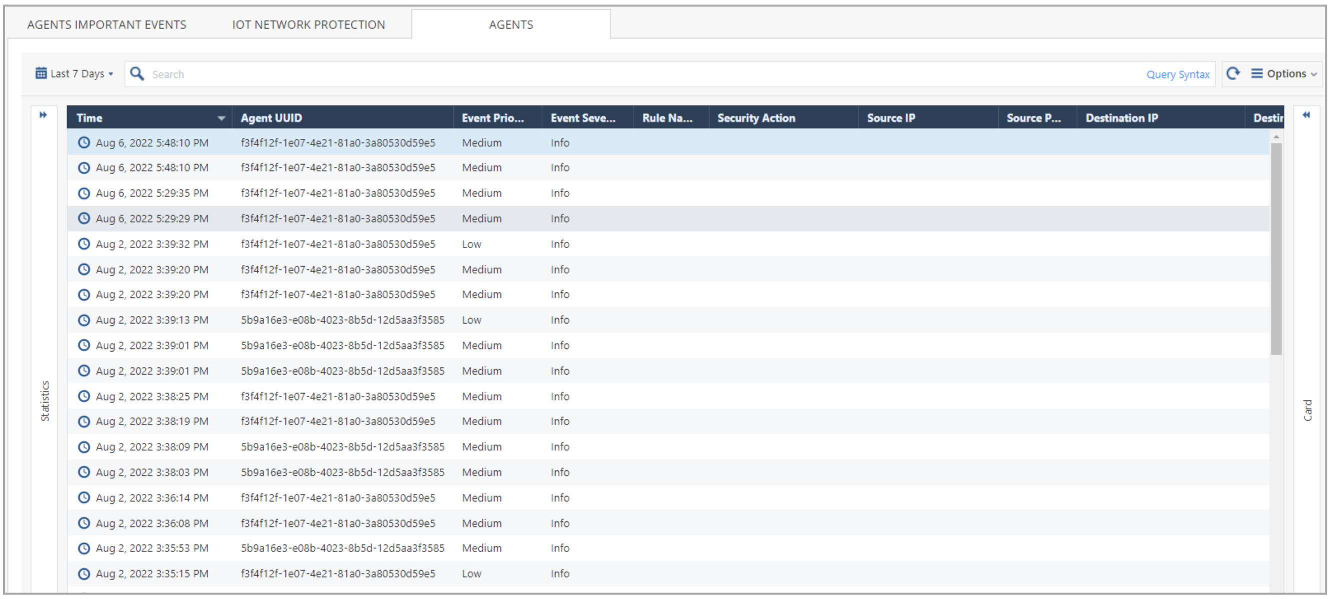
Event Parameter	Description
Rule	Rule number from the relevant policy package and Rulebase (Examples - 7.1, 11.5).
Rule Name	Name of the rule (Examples - Internet IoT all, IoT DNS to internal).

Agents

Shows the logged events for all agents.

To view the event statistics, click ⏩ in the **Statistics** bar on the left.

For card view, click ⏪ in the **Card** bar on the right.



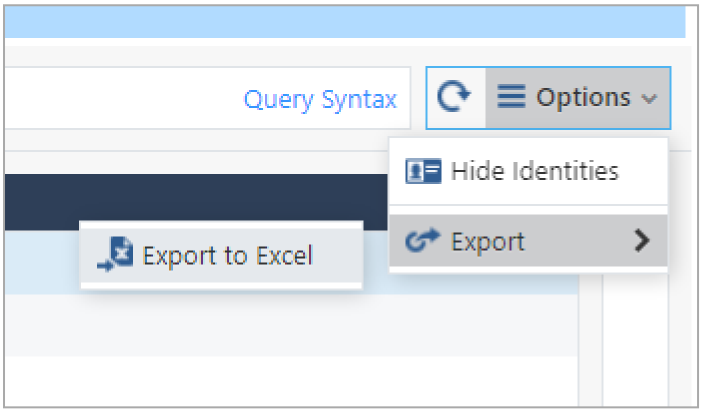
Time	Agent UUID	Event Prio...	Event Seve...	Rule Na...	Security Action	Source IP	Source P...	Destination IP	Destir
Aug 6, 2022 5:48:10 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 6, 2022 5:48:10 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 6, 2022 5:29:35 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 6, 2022 5:29:29 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 2, 2022 3:39:32 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Low	Info						
Aug 2, 2022 3:39:20 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 2, 2022 3:39:20 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 2, 2022 3:39:13 PM	5b9a16e3-e08b-4023-8b5d-12d5aa3f3585	Low	Info						
Aug 2, 2022 3:39:01 PM	5b9a16e3-e08b-4023-8b5d-12d5aa3f3585	Medium	Info						
Aug 2, 2022 3:39:01 PM	5b9a16e3-e08b-4023-8b5d-12d5aa3f3585	Medium	Info						
Aug 2, 2022 3:38:25 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 2, 2022 3:38:19 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 2, 2022 3:38:09 PM	5b9a16e3-e08b-4023-8b5d-12d5aa3f3585	Medium	Info						
Aug 2, 2022 3:38:03 PM	5b9a16e3-e08b-4023-8b5d-12d5aa3f3585	Medium	Info						
Aug 2, 2022 3:36:14 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 2, 2022 3:36:08 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Medium	Info						
Aug 2, 2022 3:35:53 PM	5b9a16e3-e08b-4023-8b5d-12d5aa3f3585	Medium	Info						
Aug 2, 2022 3:35:15 PM	f3f4f12f-1e07-4e21-81a0-3a80530d59e5	Low	Info						

Event Parameter	Description
Time	Time of the event.
Agent UUID	Unique UID of the agent.
Event Priority	Priority to address the event: ■ Urgent ■ High ■ Medium ■ Low

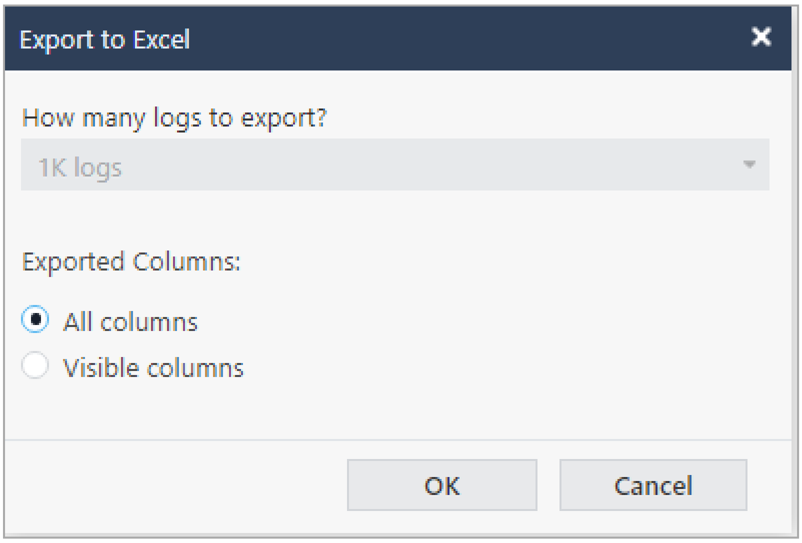
Event Parameter	Description
Event Severity	Severity of the event: - Critical - Medium - Info
Rule Name	Name of the rule (Examples - Internet IoT all, IoT DNS to internal).
Security Action	Action enforced on the event: - Drop - Block. - Accept - Allow.
Source IP	IP address of the source agent.
Source Port	Port number of the source.
Destination IP	IP address of the destination agent.
Destination Port	Port number of the destination.
Event Name	Name of the event.

To export the Agents details to an Excel sheet:

1. Click **Options** > **Export** > **Export to Excel**.



2. In the **Export to Excel** window, select the columns you want to export.



How many logs to export?

1K logs

Exported Columns:

● All columns

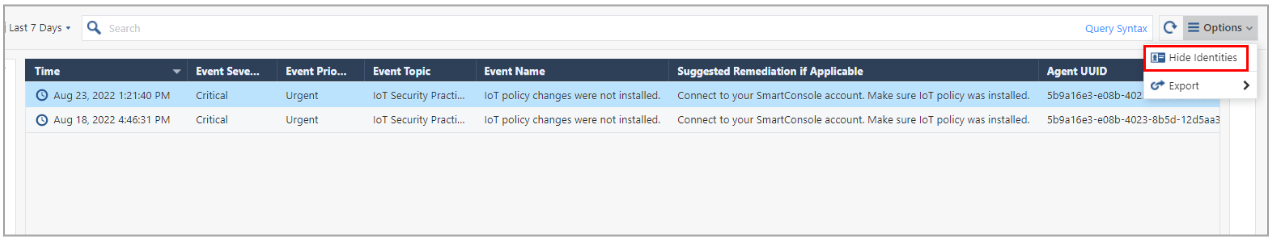
○ Visible columns

3. Click **OK**.

4. In the **Exported Completed Successfully** pop-up, click **Download**.

   The logs Excel sheet is downloaded with the name format: Logs_Date_Time.xls (For example, *Logs_Aug_5__2022_11_58_50_AM.xls*)

Note - To obscure any user specific information in the events table, click the **Hide Identities** option.



Time	Event Seve...	Event Prio...	Event Topic	Event Name	Suggested Remediation if Applicable	Agent UUID
Aug 23, 2022 1:21:40 PM	Critical	Urgent	IoT Security Practi...	IoT policy changes were not installed.	Connect to your SmartConsole account. Make sure IoT policy was installed.	5b9a16e3-e08b-402
Aug 18, 2022 4:46:31 PM	Critical	Urgent	IoT Security Practi...	IoT policy changes were not installed.	Connect to your SmartConsole account. Make sure IoT policy was installed.	5b9a16e3-e08b-4023-8b5d-12d5aa3

Disabling Quantum IoT Protect

You can temporarily disable Quantum IoT Protect for troubleshooting purposes. When you disable, it:

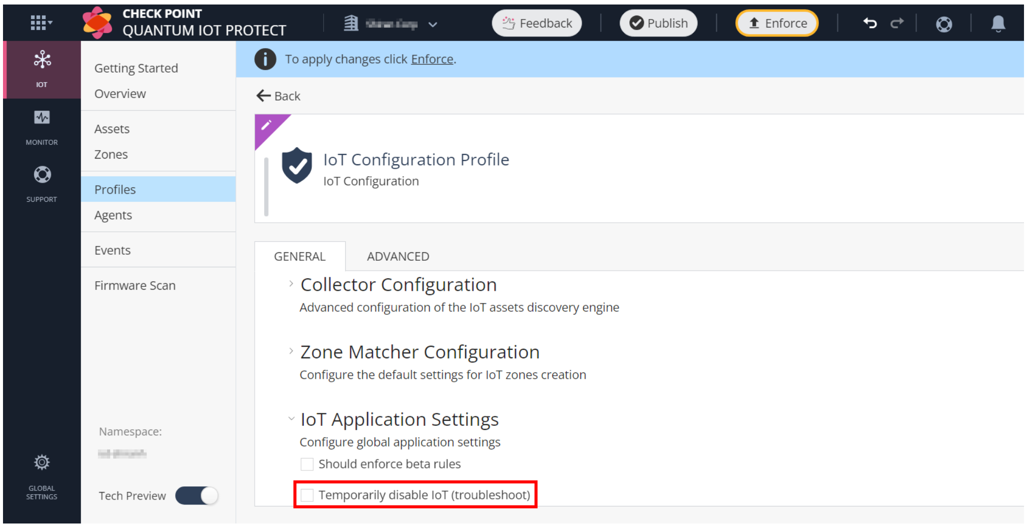
- Stops discovering IoT assets from the sources.
- Stops IoT cloud services and IoT local nano-agents.
- Disables integration with SmartConsole.

To disable Quantum IoT Protect:

1. In the Infinity Portal, go to **Quantum** > **IoT Protect** > **IoT**.

   Note - To view this feature, enable **Tech Preview** option at the bottom of the page.

2. Go to **Profiles** > **IoT Configuration Profile** and click the **General** tab.
3. Expand **IoT Application Settings** and select the **Temporarily disable IoT (troubleshoot)** checkbox.



To apply changes click Enforce.

IoT Configuration Profile
IoT Configuration

Collector Configuration
Advanced configuration of the IoT assets discovery engine

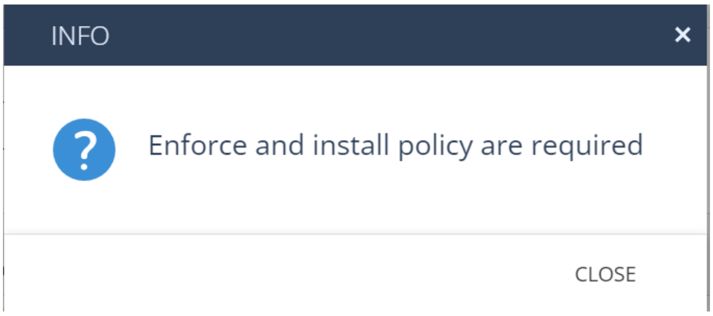
Zone Matcher Configuration
Configure the default settings for IoT zones creation

IoT Application Settings
Configure global application settings
□ Should enforce beta rules
□ Temporarily disable IoT (troubleshoot)

Namespace: [redacted]

Tech Preview ●

   A prompt appears.



INFO

Enforce and install policy are required

CLOSE

4. Click **Close**.

5. Click **Enforce**.
6. (Optional) To remove the IoT policy and its objects from SmartConsole, follow the instructions in sk180984.

ⓘ **Note** - To enable Quantum IoT Protect again, revert step 3 and click **Enforce**.

Appendix A - Onboarding Quantum IoT Protect on a Multi-Domain Management Server with Single Domain

1. Run SmartConsole.
2. Enter your username and password.
3. Enter the Multi-Domain Server IP address, and then click **Login**.
4. Select the **MDS** context and click **Proceed**.
5. From the left navigation pane, click **Multi Domain** > **Domains**.
6. From the **Domains** column, note down the name of the applicable Domain object (case-sensitive).
7. Connect to the Multi-Domain Server through SSH.
8. Log in to the Expert mode.
9. Run this command to back up the current `$MDS_FWDIR/conf/iot-on-board.conf` file:

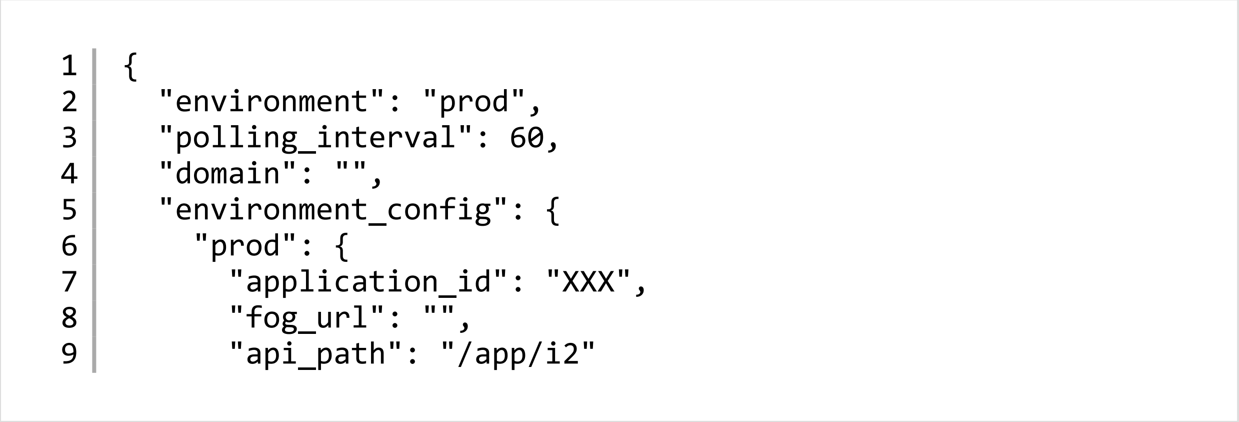
   ```
   cp -v $MDS_FWDIR/conf/iot-on-board.conf{,_BKP}
   ```

10. Run this command to edit the current `$MDS_FWDIR/conf/iot-on-board.conf` file:

    ```
    vi $MDS_FWDIR/conf/iot-on-board.conf
    ```

11. In line 4 **"domain": ""**, enter the name of the Domain object.

    Change line 4 from:



```
1  {
2    "environment": "prod",
3    "polling_interval": 60,
4    "domain": "",
5    "environment_config": {
6      "prod": {
7        "application_id": "XXX",
8        "fog_url": "",
9        "api_path": "/app/i2"
```

```
    },
    "pre_prod": {
      "application_id": "XXX",
      "fog_url": "https://XXX.checkpoint.com",
      "api_path": "/app/i2"
    },
    "dev": {
      "application_id": "XXX",
      "fog_url": "https://XXX.checkpoint.com",
      "api_path": "/app/infinity2gem"
    }
  }
}
```

to

```
{
  "environment": "prod",
  "polling_interval": 60,
  "domain": "<NAME OF DOMAIN OBJECT>",
  "environment_config": {
    "prod": {
      "application_id": "XXX",
      "fog_url": "",
      "api_path": "/app/i2"
    },
    "pre_prod": {
      "application_id": "XXX",
      "fog_url": "https://XXX.checkpoint.com",
      "api_path": "/app/i2"
    },
    "dev": {
      "application_id": "XXX",
      "fog_url": "https://XXX.checkpoint.com",
      "api_path": "/app/infinity2gem"
    }
  }
}
```

12. Save the changes in the file.

13. Exit the Vi editor.

For a Management High Availability environment, repeat the procedure on each peer Multi-Domain Server.

Appendix B - Using SNMP as the IoT Discovery Engine

You can set up an IoT discovery engine on the Check Point Security Gateway or Management Server to discover IoT assets in your network. The IoT discovery engine uses the network devices in the network, such as switches, routers, gateways, or Network Access Control (NAC) devices to discover IoT assets.

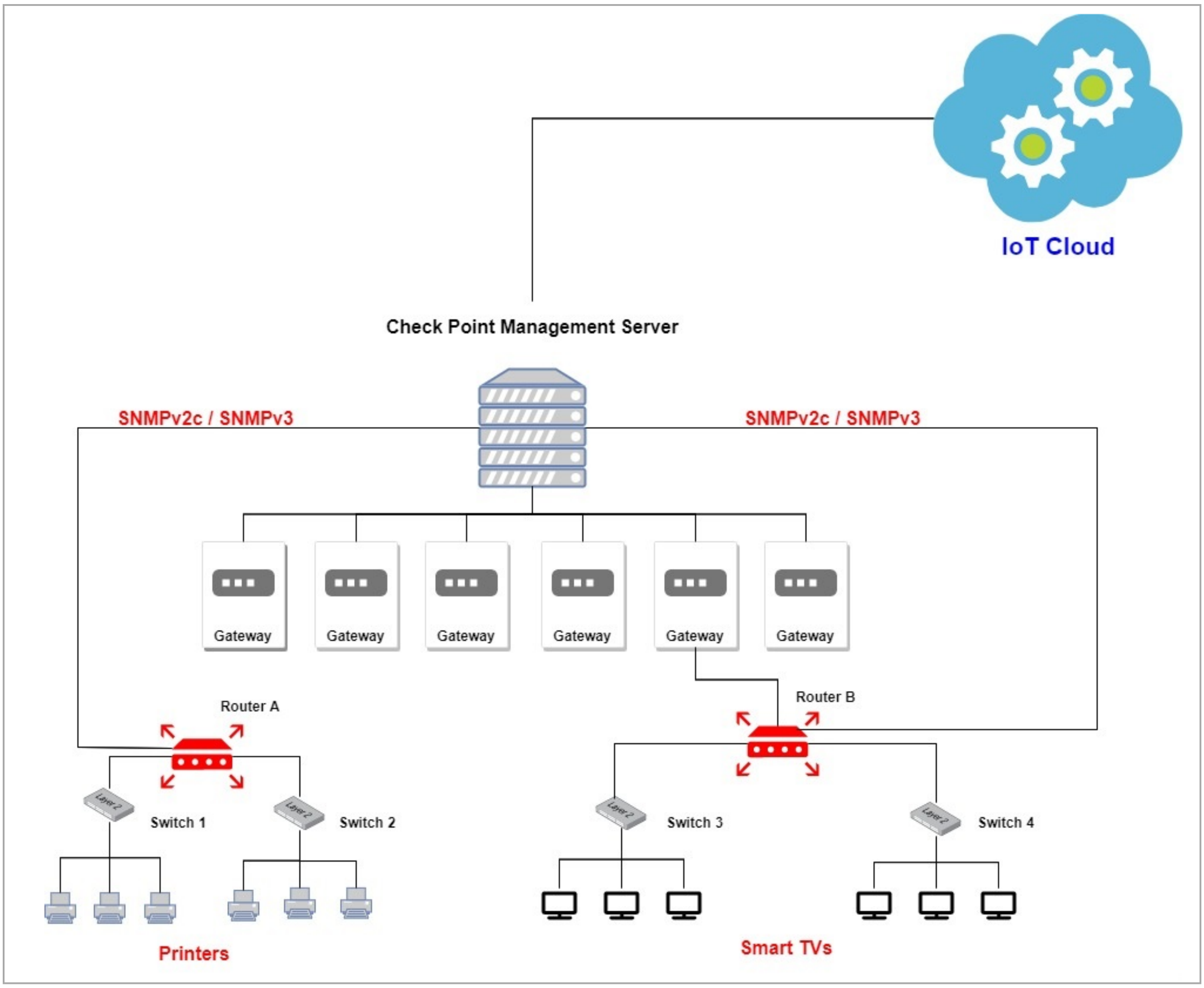
The Simple Network Management Protocol (SNMP) integration sends queries to network devices such as switches, routers, or gateways to get the data stored in their Address Resolution Protocol (ARP) tables. SNMP integration can be configured on the Management Server or on the Security Gateway.

SNMP integration supports both SNMPv2c and SNMPv3. SNMPv3 is the most secure version of the SNMP protocol.

SNMP uses `snmp get` and `snmp walk` to send commands and messages. SNMP packets are typically sent over UDP, though SNMP over TCP port is possible.

The SNMP profiles are tested on these SNMP servers:

- Cisco Catalyst 9300
- Cisco Catalyst 9500
- Check Point Security Gateways
- HPE Networking Comware Switch Series 5940
- MikroTik CRS317
- FortiGate 200F firewall
- Any router which supports RFC 1213.

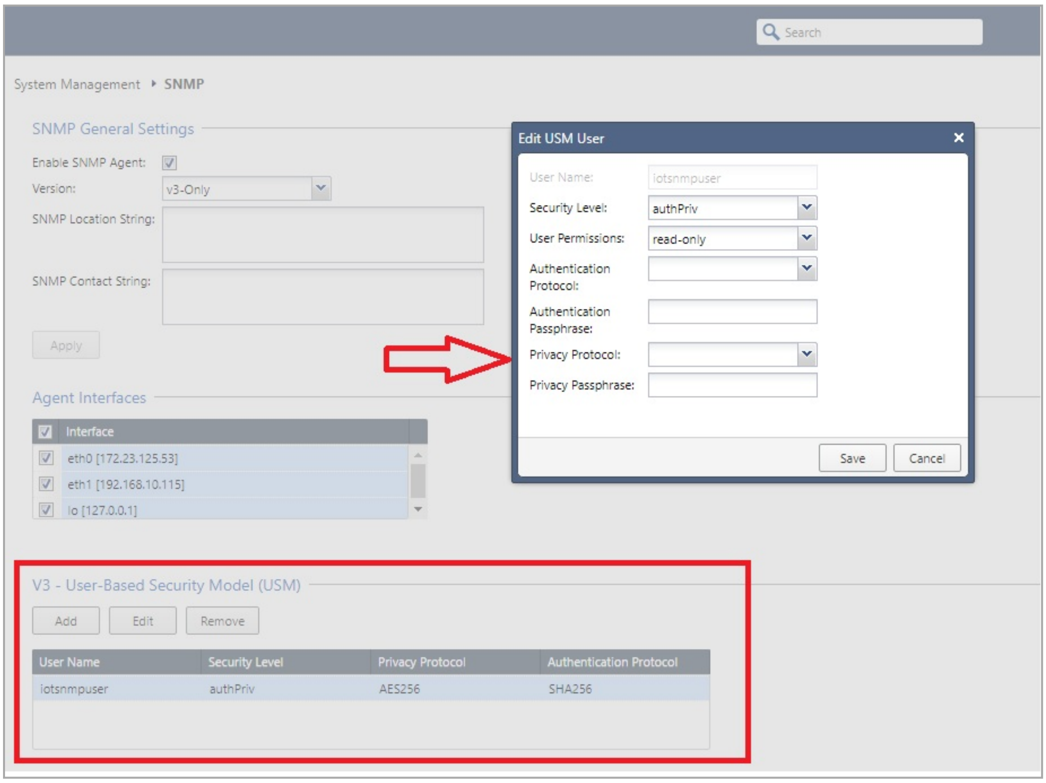


Prerequisites

1. Configure the SNMP service on the network device (switch, router or gateway) to be queried. For more information, refer to your router documentation.

Notes:

- When you configure the SNMP built-in discovery integration to query the ARP table of Check Point cluster of gateways, configure it for both cluster members: Active and Standby.



System Management ▸ SNMP

SNMP General Settings

Enable SNMP Agent: ☑

Version: v3-Only

SNMP Location String:

SNMP Contact String:

Agent Interfaces

☑	Interface
☑	eth0 [172.23.125.53]
☑	eth1 [192.168.10.115]
☑	lo [127.0.0.1]

Edit USM User

User Name: iotsnmpuser

Security Level: authPriv

User Permissions: read-only

Authentication Protocol:

Authentication Passphrase:

Privacy Protocol:

Privacy Passphrase:

V3 - User-Based Security Model (USM)

User Name	Security Level	Privacy Protocol	Authentication Protocol
iotsnmpuser	authPriv	AES256	SHA256

- **Cisco VRF Router**

  Virtual Routing and Forwarding (VRF) technology lets multiple instances of a routing table co-exist on the same router at the same time.

  To configure a different SNMP context for each VRF, run this command on the router's shell (only when using SNMPv3):

  ```
  snmp-server context <context-1-name> vrf <vrf-1-name>
  ```

2. Allow SNMP traffic between the Security Gateway or Management Server on which the integration is installed and the switch or router which needs to be queried, configure relevant security rules on the gateway.

   a. From SmartConsole, connect to Security Gateway or Security Management Server or Domain Management Server.

   b. Configure the relevant security rules to allow the SNMP traffic:

      i. To allow the SNMP Request and SNMP Response, use the pre-defined service **snmp**.

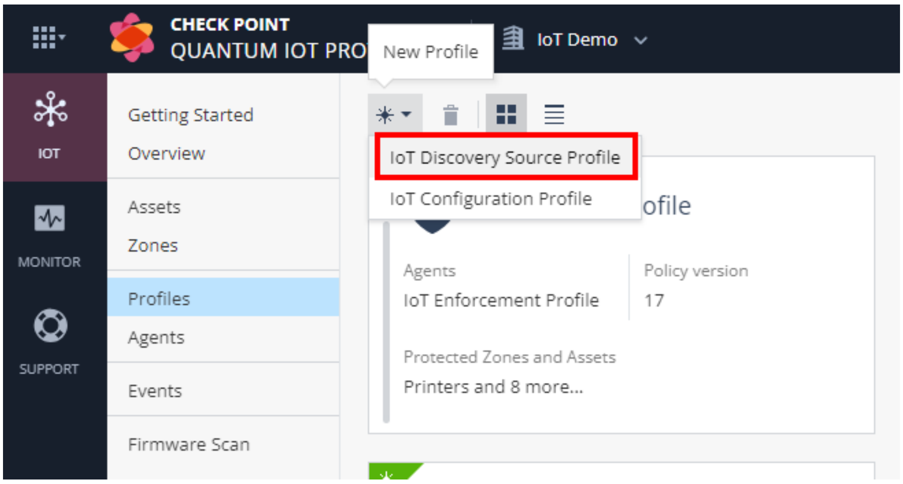
      ii. To allow the SNMP Trap packets, use the pre-defined service **snmp-trap**.

   c. Install the policy on the relevant Security Gateway or Cluster.

Setting Up SNMP - IoT Discovery Integration

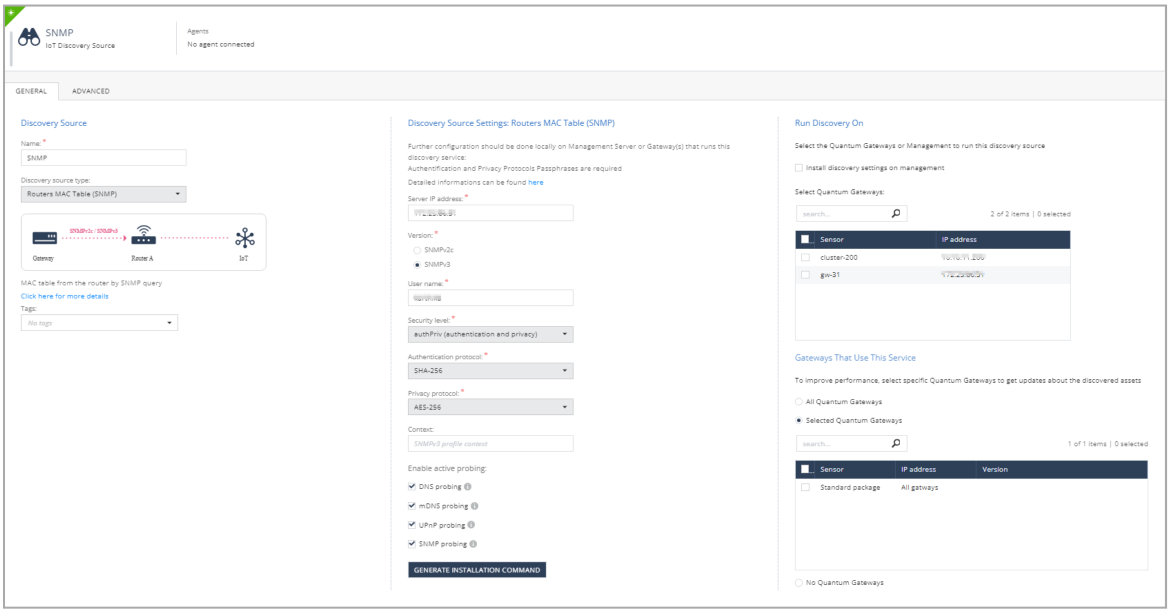
To set up SNMP as the IoT Discovery Engine:

1. Configure SNMP Integration in Quantum IoT Protect.
   a. Log in to *Check Point Infinity Portal*.
   b. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.
   c. Click ✳ and select **IoT Discovery Source Profile**.



   d. In the **Discovery Source** section, from the **Discovery source type** list, select **Routers MAC Table (SNMP)**.

e. In the **Discovery Source Settings** section:



SNMP
IoT Discovery Source

Agents
No agent connected

GENERAL | ADVANCED

Discovery Source

Name: *
SNMP

Discovery source type:
Routers MAC Table (SNMP) ▾

MAC table from the router by SNMP query

Click here for more details

Tags:
No tags ▾

Discovery Source Settings: Routers MAC Table (SNMP)

Further configuration should be done locally on Management Server or Gateway(s) that runs this discovery service:
Authentification and Privacy Protocols Passphrases are required

Detailed informations can be found here

Server IP address: *
[redacted]

Version: *
○ SNMPv2c
● SNMPv3

User name: *
[redacted]

Security level: *
authPriv (authentication and privacy) ▾

Authentication protocol: *
SHA-256 ▾

Privacy protocol: *
AES-256 ▾

Context:
SNMPv3 profile context

Enable active probing:
☑ DNS probing
☑ mDNS probing
☑ UPnP probing
☑ SNMP probing

GENERATE INSTALLATION COMMAND

Run Discovery On

Select the Quantum Gateways or Management to run this discovery source

□ Install discovery settings on management

Select Quantum Gateways:

search... 2 of 2 items | 0 selected

□	Sensor	IP address
□	cluster-200	[redacted]
□	gw-31	[redacted]

Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways
● Selected Quantum Gateways

search... 1 of 1 items | 0 selected

□	Sensor	IP address	Version
□	Standard package	All gatways	

○ No Quantum Gateways

i. In the **Server IP address** field, enter the IP address of the SNMP server.

ii. In the **Version** section, select the SNMP version.

If you selected **SNMPv3**:

- In the **User name** field, enter the SNMP user name.
- From the **Security level** drop-down list, select the security level for SNMP integration.
- From the **Authentication protocol** drop-down list, select the authentication protocol for SNMP integration.
- From the **Privacy protocol** drop-down list, select the privacy protocol for SNMP integration.

SNMP built-in discovery integration depends on local configuration:

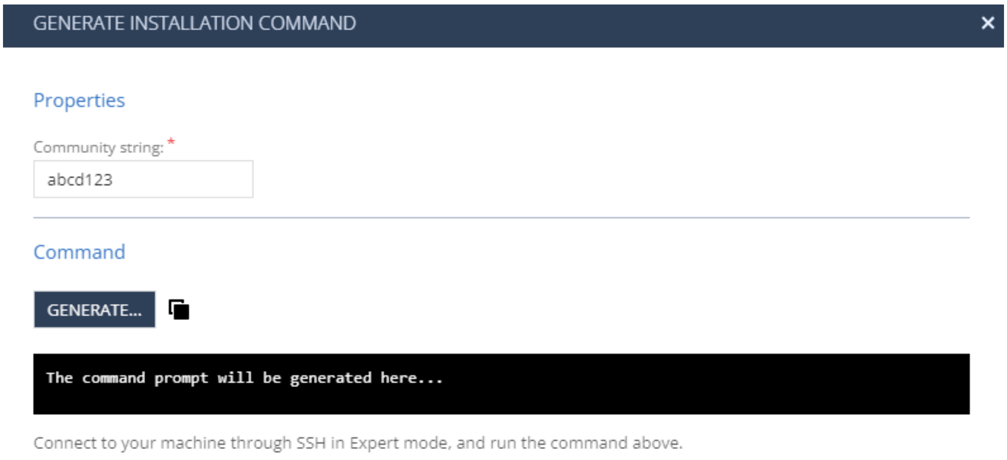
SNMP Integration Type	Local Configuration
SNMPv2c	Community String
SNMPv3, Security Level: Authentication and Privacy (authPriv)	■ Authentication Protocol Passphrase ■ Privacy Protocol Passphrase
SNMPv3, Security Level: Authentication no Privacy (authNoPriv)	Authentication Protocol Passphrase

iii. Click **Generate Installation Command**.

The **Generate Installation Command** window appears.

iv. In the **Properties** section:

- For SNMPv2c, enter the **Community string**.



GENERATE INSTALLATION COMMAND

Properties

Community string: *

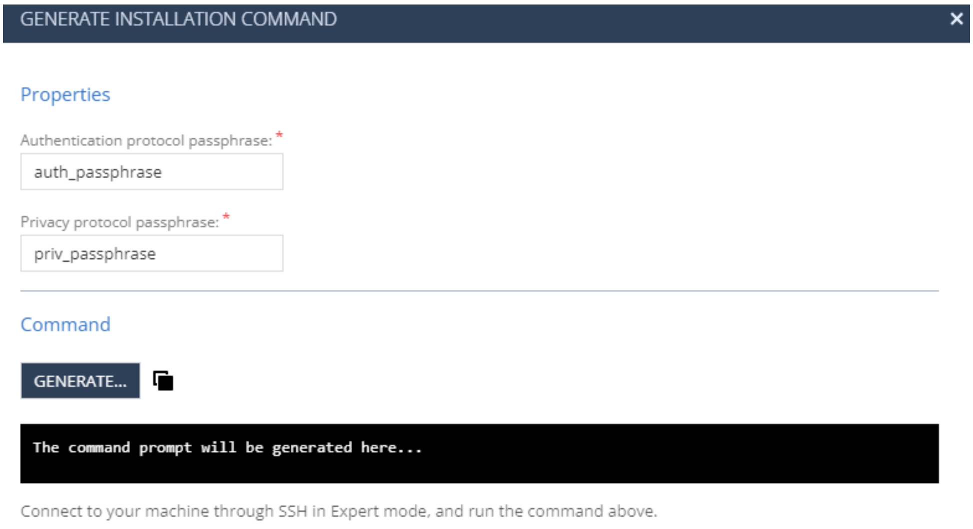
abcd123

Command

```
The command prompt will be generated here...
```

Connect to your machine through SSH in Expert mode, and run the command above.

- For SNMPv3, enter:
  - **Authentication protocol passphrase**
  - **Privacy protocol passphrase**



GENERATE INSTALLATION COMMAND

Properties

Authentication protocol passphrase: *

auth_passphrase

Privacy protocol passphrase: *

priv_passphrase

Command

```
The command prompt will be generated here...
```

Connect to your machine through SSH in Expert mode, and run the command above.

v. In the **Command** section, click **Generate**.

The system generates the command to configure the SNMP discovery engine on the Check Point Security Gateway / Management Server.

vi. Copy the generated command.

vii. Access your Check Point Security Gateway / Management Server through SSH, for example using PuTTY.

viii. Log in to Expert mode.

ix. Paste the generated command.

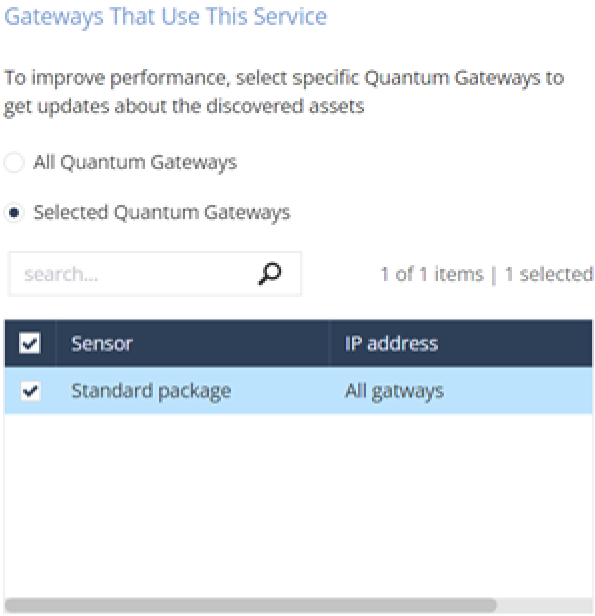
x. If the integration is installed on a cluster gateway or Management Server with High Availability (HA) or Multi-Domain Server (MDS) with HA:

   i. Access each member through SSH and log in to Expert mode.

   ii. Paste the generated command.

f. In the **Run Discovery On** section, select the Security Gateway / Management Server on which the integration must be installed.

g. In the **Gateways That Use This Service** section, select the gateways relevant to your discovered assets, or select the policy-package for all gateways.



Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways

● Selected Quantum Gateways

search...

1 of 1 items | 1 selected

☑	Sensor	IP address
☑	Standard package	All gatways

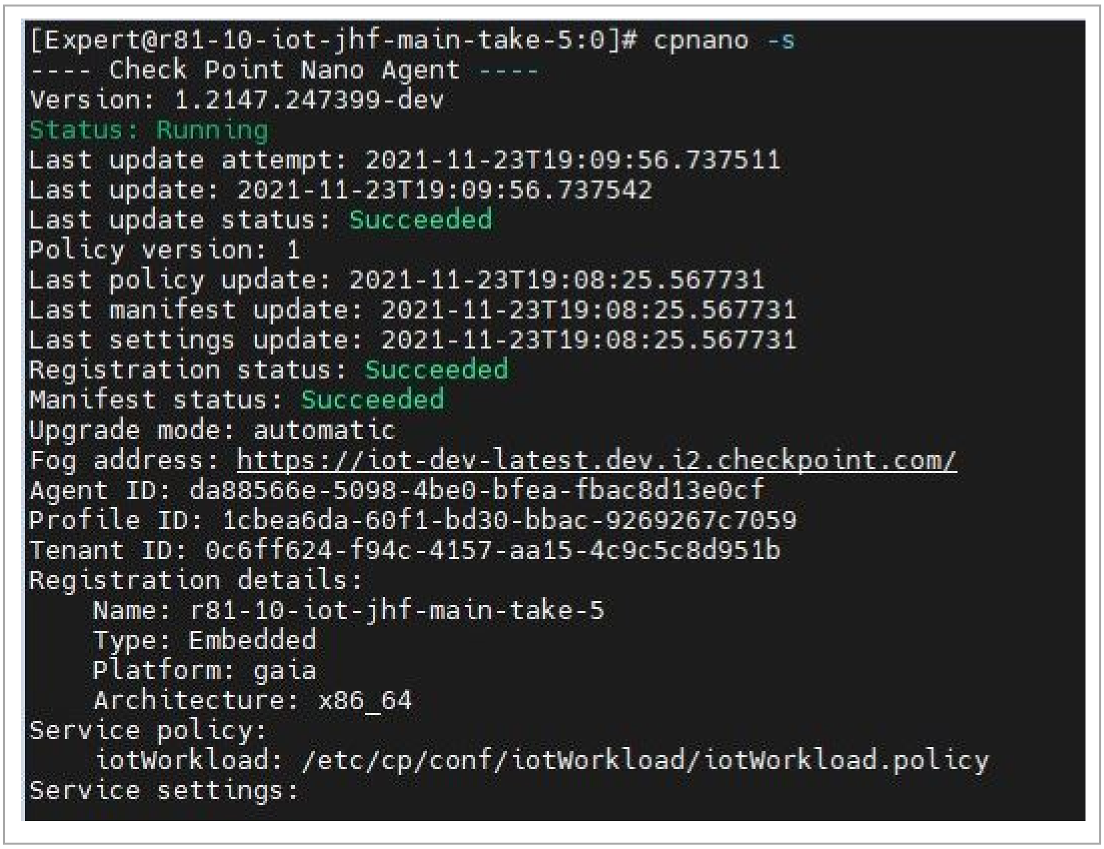
h. Click **Enforce**.

Testing the SNMP- IoT Discovery Integration

1. Access the Check Point Security Gateway / Management Server through SSH and run:

   ```
   cpnano -s
   ```

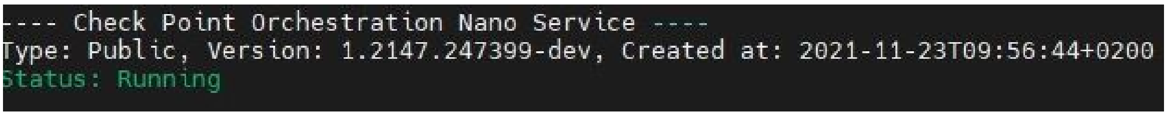
   Sample output:



```
[Expert@r81-10-iot-jhf-main-take-5:0]# cpnano -s
---- Check Point Nano Agent ----
Version: 1.2147.247399-dev
Status: Running
Last update attempt: 2021-11-23T19:09:56.737511
Last update: 2021-11-23T19:09:56.737542
Last update status: Succeeded
Policy version: 1
Last policy update: 2021-11-23T19:08:25.567731
Last manifest update: 2021-11-23T19:08:25.567731
Last settings update: 2021-11-23T19:08:25.567731
Registration status: Succeeded
Manifest status: Succeeded
Upgrade mode: automatic
Fog address: https://iot-dev-latest.dev.i2.checkpoint.com/
Agent ID: da88566e-5098-4be0-bfea-fbac8d13e0cf
Profile ID: 1cbea6da-60f1-bd30-bbac-9269267c7059
Tenant ID: 0c6ff624-f94c-4157-aa15-4c9c5c8d951b
Registration details:
    Name: r81-10-iot-jhf-main-take-5
    Type: Embedded
    Platform: gaia
    Architecture: x86_64
Service policy:
    iotWorkload: /etc/cp/conf/iotWorkload/iotWorkload.policy
Service settings:
```

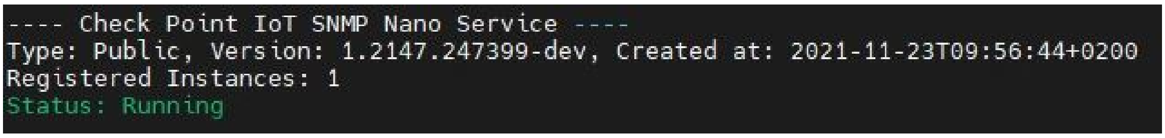
2. Make sure these nano services are running:

   a. Check Point Orchestration



```
---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2147.247399-dev, Created at: 2021-11-23T09:56:44+0200
Status: Running
```

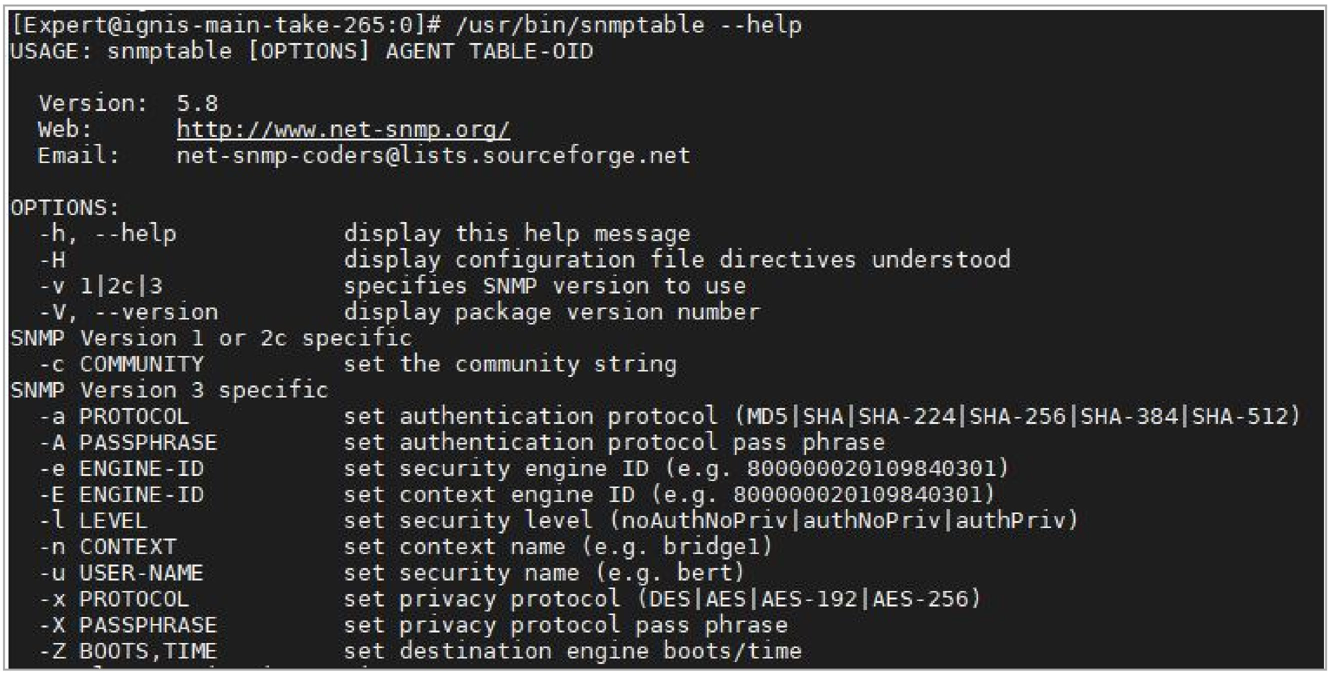
   b. Check Point IoT SNMP



```
---- Check Point IoT SNMP Nano Service ----
Type: Public, Version: 1.2147.247399-dev, Created at: 2021-11-23T09:56:44+0200
Registered Instances: 1
Status: Running
```

Troubleshooting the SNMP- IoT Discovery Integration

To troubleshoot, access the Check Point Security Gateway / Management Server through SSH and query the network device.



```
[Expert@ignis-main-take-265:0]# /usr/bin/snmptable --help
USAGE: snmptable [OPTIONS] AGENT TABLE-OID

  Version:  5.8
  Web:      http://www.net-snmp.org/
  Email:    net-snmp-coders@lists.sourceforge.net

OPTIONS:
  -h, --help            display this help message
  -H                    display configuration file directives understood
  -v 1|2c|3             specifies SNMP version to use
  -V, --version         display package version number
SNMP Version 1 or 2c specific
  -c COMMUNITY          set the community string
SNMP Version 3 specific
  -a PROTOCOL           set authentication protocol (MD5|SHA|SHA-224|SHA-256|SHA-384|SHA-512)
  -A PASSPHRASE         set authentication protocol pass phrase
  -e ENGINE-ID          set security engine ID (e.g. 800000020109840301)
  -E ENGINE-ID          set context engine ID (e.g. 800000020109840301)
  -l LEVEL              set security level (noAuthNoPriv|authNoPriv|authPriv)
  -n CONTEXT            set context name (e.g. bridge1)
  -u USER-NAME          set security name (e.g. bert)
  -x PROTOCOL           set privacy protocol (DES|AES|AES-192|AES-256)
  -X PASSPHRASE         set privacy protocol pass phrase
  -Z BOOTS,TIME         set destination engine boots/time
```

- For SNMP v2c:

```
snmptable -v 2c -c<community> <snmp server>
ipNetToMediaTable -C H -C f "," | awk -F ',' '{print $3 " " $2
":"}'|
sed -e 's/\b[0-9a-f]\b:/0&/g;s/:*$//'
```

Example:

```
snmptable -v 2c -cpublic <snmp server>
ipNetToMediaTable -C H -C f "," | awk -F ',' '{print $3 " " $2
":"}'|
sed -e 's/\b[0-9a-f]\b:/0&/g;s/:*$//'
```

- For SNMP v3:

```
snmptable -v3 -a<authentication_protocol> -x<privacy_protocol> -
u<username> -A<authphrase> -X<privphase>
-l<security_level> <snmp server> ipNetToMediaTable -C H -C f ","
|
awk -F ',' '{print $3 " " $2 ":"}' |
sed -e 's/\b[0-9a-f]\b:/0&/g;s/:*$//'
```

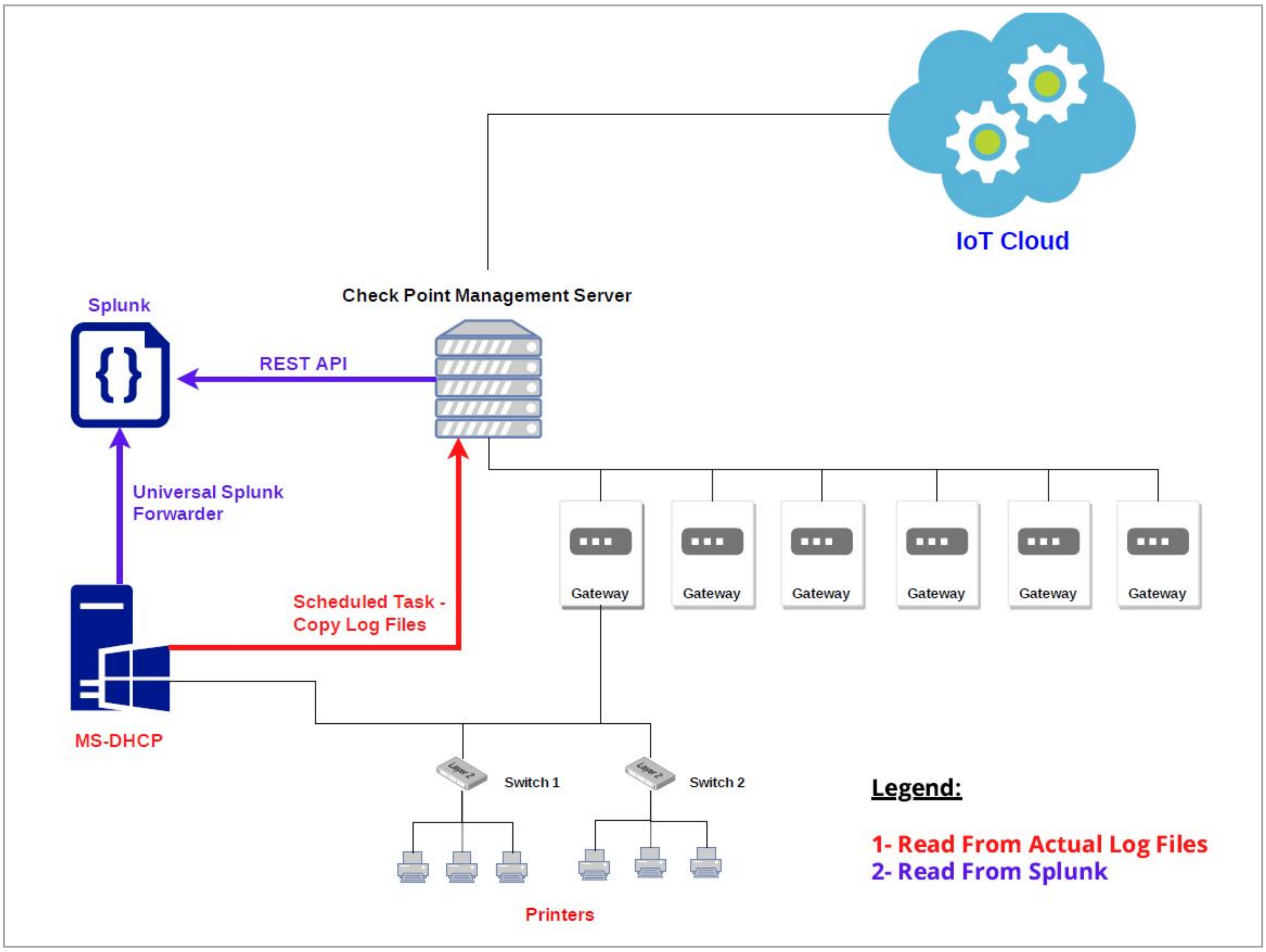
Example:

```
snmptable -v3 -aSHA -xAES -u<username> -A<authphrase> -
X<privphase>
-lauthPriv <snmp server> ipNetToMediaTable -C H -C f "," |
awk -F ',' '{print $3 " " $2 ":"}' |
sed -e 's/\b[0-9a-f]\b:/0&/g;s/:*$//'
```

Appendix C - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory)

You can set up an IoT discovery engine on the Check Point Security Gateway or Management Server to discover IoT assets in your network. The IoT discovery engine uses the network devices in the network, such as switches, routers, gateways, or Network Access Control (NAC) devices to discover IoT assets.

You can use the Microsoft Dynamic Host Configuration Protocol (MS-DHCP) server to discover IoT assets. It maintains a pool of IP addresses and provides (leases) an IP address to every new DHCP-enabled client. MS-DHCP integration is based on events log files created by the MS-DHCP server. The events may include the MAC address of the device (DHCP-enabled client) and the leased IP address.



MS-DHCP server reads the DHCP events by one of these methods:

- The event logs from the MS-DHCP server are copied to a local directory and the logs are read from this local directory.
- The event logs from the MS-DHCP server are forwarded to the Splunk server and the logs are read from the Splunk server.

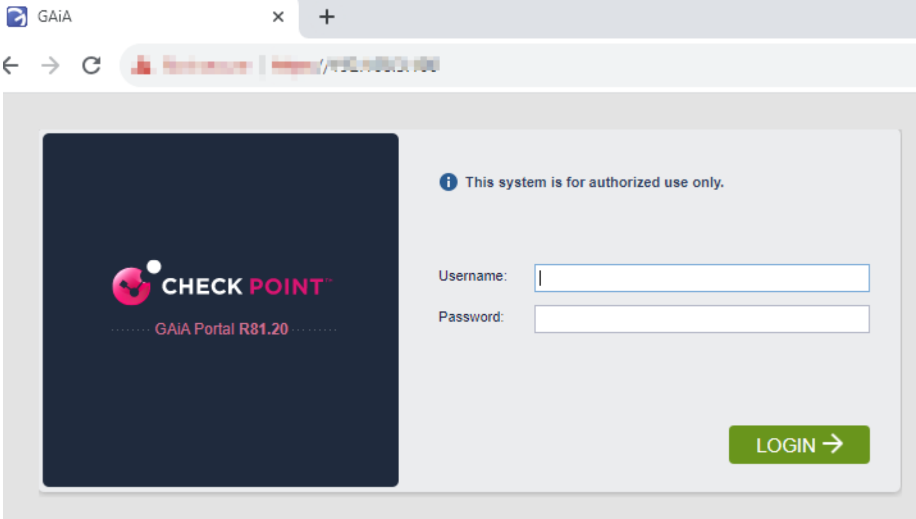
This appendix describes the MS-DHCP integration when the event logs are read from the local directory.

Prerequisites

- MS-DHCP Server 2012 (R2) and higher.
- For MS-DHCP Server 2016 and lower, install OpenSSH. See *"Installing OpenSSH on the MS-DHCP Server" on page 101*.
- IP address and login credentials of your Check Point Security Gateway / Management Server that is used to discover IoT assets in your network.
- Verify that your Check Point Security Gateway / Management Server is accessible. To verify, go to:

  ```
  https://<IP address of Gaia Management Interface on Security
  Gateway>
  ```

  If the Gaia Portal login page appears, then the Security Gateway / Management Server is accessible.



This system is for authorized use only.

Username:

Password:

- On your Check Point Security Gateway / Management Server, the default shell must be the Expert mode (`/bin/bash`).

To change the default user shell:

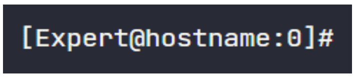
a. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console).

b. Next step depends on the current configuration:

   - If you default shell is the Expert mode, then the prompt shows the word "`Expert`" in front of the hostname.

     There is nothing else to configure.

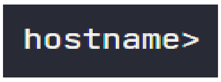
     Example:

     ```
     [Expert@hostname:0]#
     ```

   - If you default shell is Gaia Clish, then the prompt shows only the hostname.

     Example:

     ```
     hostname>
     ```

     You can change the default shell in **one** of these ways:

     - In Gaia Portal, configure:

       a. Go to **User Management** > **Users**.

       b. Select and edit the **admin** user.

       c. In the **Shell** field, select **/bin/bash**.

       d. Click **OK**.

     - In Gaia Clish, run:

       a. `set user admin shell /bin/bash`

       b. `save config`

c. Restart your SSH session and check if you are in Expert mode by default.

   If you are still in Clish mode, make sure you have entered the correct commands and restart the SSH session.

d. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console) again.

e. The prompt must show the word "`Expert`" in front of the hostname.

Setting Up MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory)

To set up MS-DHCP as the IoT Discovery Engine:

1. Create a scheduled task to securely copy the leased log files from the MS-DHCP server to the Check Point Security Gateway server / Management Server.

   a. Download the `ms-dest.bat` file:

      i. Click here.

         The **Download Details** page appears.

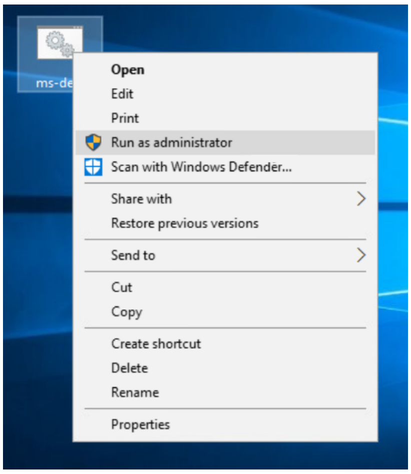
      ii. Click **Download**.

         The system downloads a zip file.

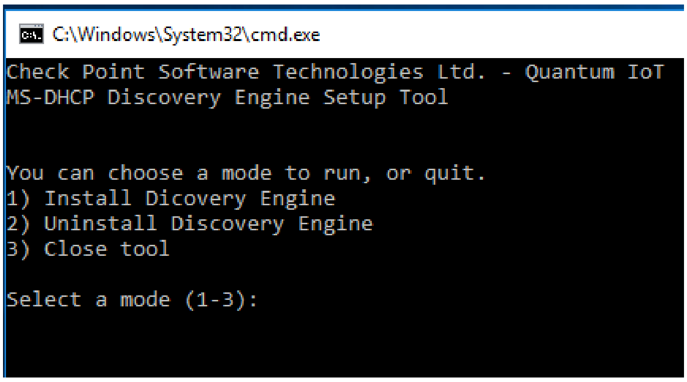
      iii. Extract the `ms-dest.bat` file from the zip file.

      iv. Transfer the file to the MS-DHCP server.

b. On the MS-DHCP server, right-click the **ms-dest.bat** file and click **Run as administrator**.



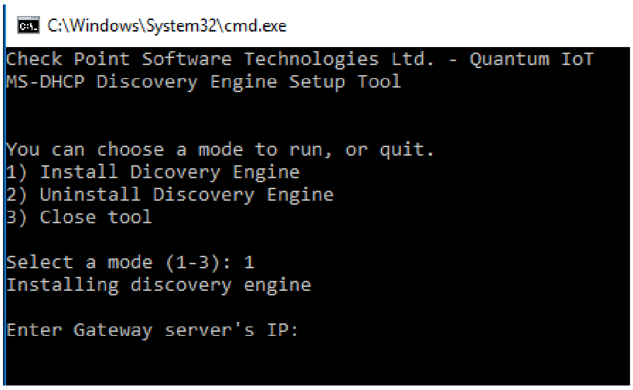
The Command Prompt window opens:



```
Check Point Software Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


You can choose a mode to run, or quit.
1) Install Dicovery Engine
2) Uninstall Discovery Engine
3) Close tool

Select a mode (1-3):
```

c. To install the discovery engine, enter **1** and press **Enter**.

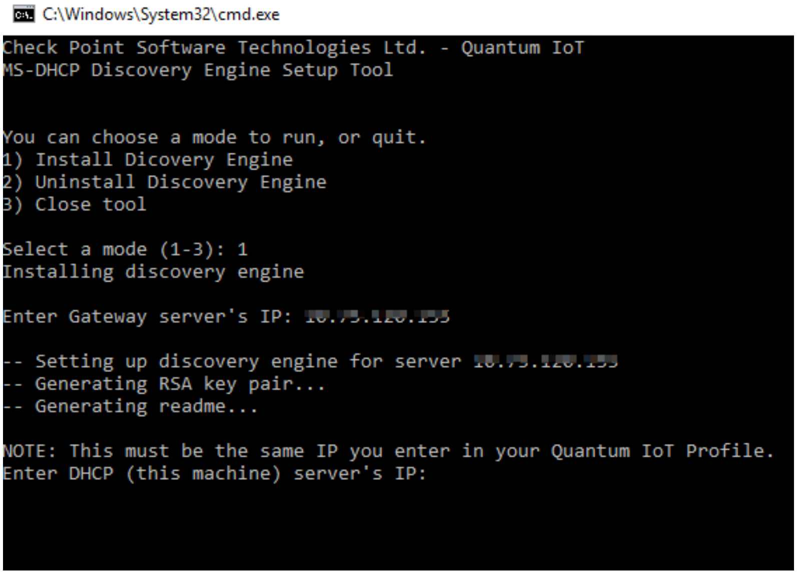
Output:



```
Check Point Software Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


You can choose a mode to run, or quit.
1) Install Dicovery Engine
2) Uninstall Discovery Engine
3) Close tool

Select a mode (1-3): 1
Installing discovery engine

Enter Gateway server's IP:
```

d. Enter the IP address of your Security Gateway, and press **Enter**.

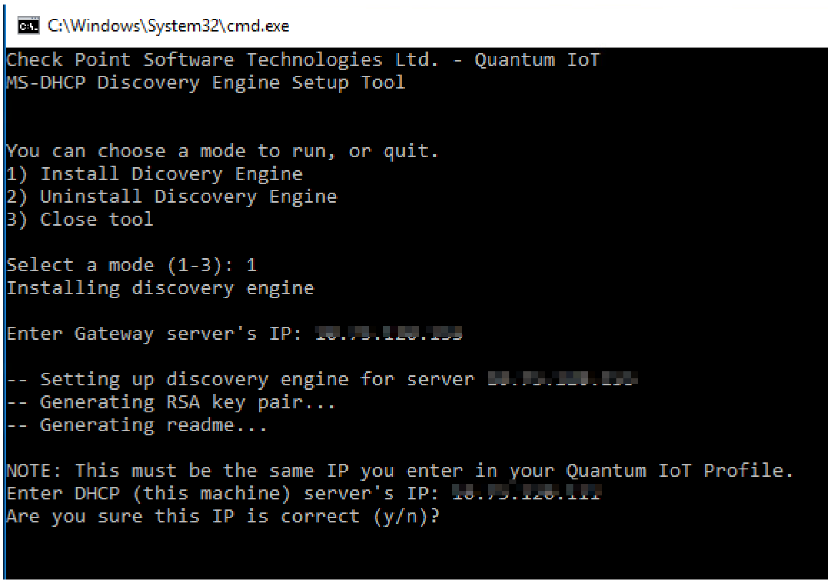
Output:



```
Check Point Software Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


You can choose a mode to run, or quit.
1) Install Dicovery Engine
2) Uninstall Discovery Engine
3) Close tool

Select a mode (1-3): 1
Installing discovery engine

Enter Gateway server's IP: [redacted]

-- Setting up discovery engine for server [redacted]
-- Generating RSA key pair...
-- Generating readme...

NOTE: This must be the same IP you enter in your Quantum IoT Profile.
Enter DHCP (this machine) server's IP:
```

e. Enter the IP address of the MS-DHCP server.

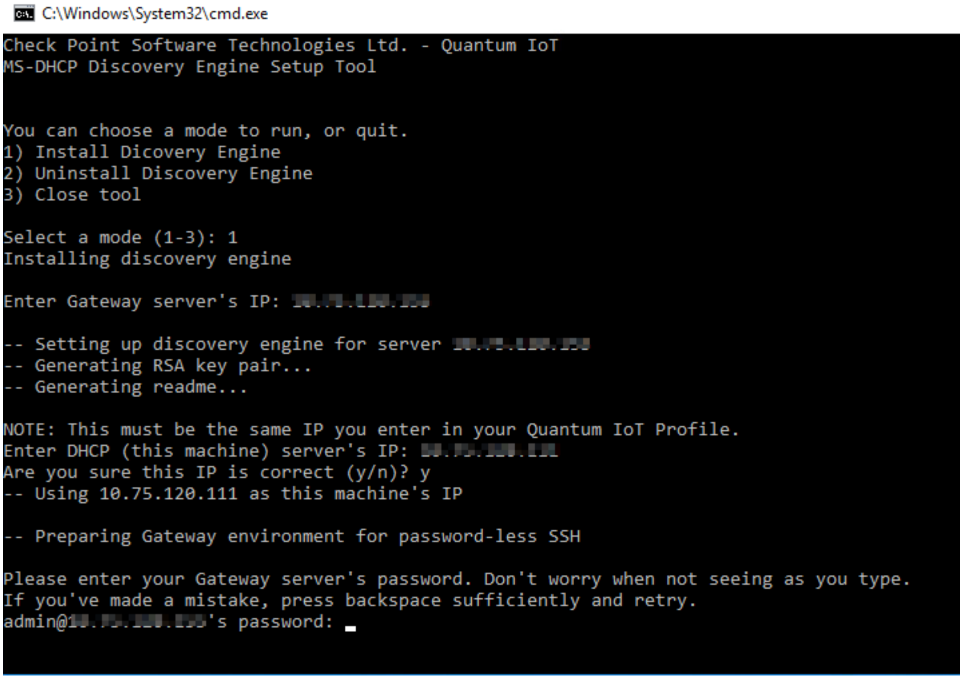
Output:



```
Check Point Software Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


You can choose a mode to run, or quit.
1) Install Dicovery Engine
2) Uninstall Discovery Engine
3) Close tool

Select a mode (1-3): 1
Installing discovery engine

Enter Gateway server's IP: [redacted]

-- Setting up discovery engine for server [redacted]
-- Generating RSA key pair...
-- Generating readme...

NOTE: This must be the same IP you enter in your Quantum IoT Profile.
Enter DHCP (this machine) server's IP: [redacted]
Are you sure this IP is correct (y/n)?
```

f. Enter **y** and then press **Enter**.

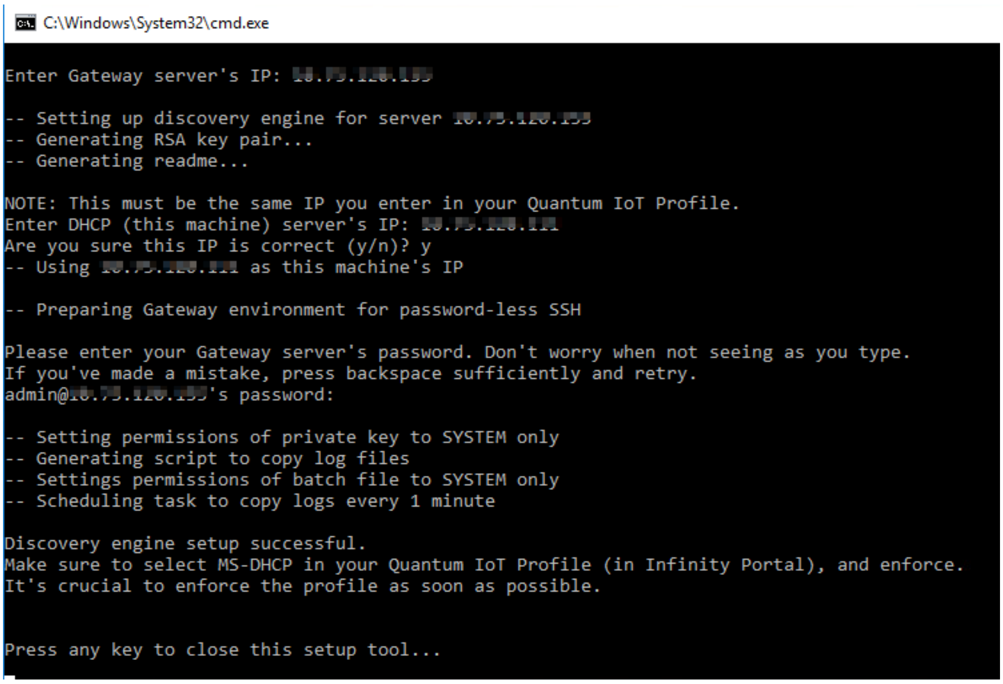
Output:



```
Check Point Software Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


You can choose a mode to run, or quit.
1) Install Dicovery Engine
2) Uninstall Discovery Engine
3) Close tool

Select a mode (1-3): 1
Installing discovery engine

Enter Gateway server's IP: [redacted]

-- Setting up discovery engine for server [redacted]
-- Generating RSA key pair...
-- Generating readme...

NOTE: This must be the same IP you enter in your Quantum IoT Profile.
Enter DHCP (this machine) server's IP: [redacted]
Are you sure this IP is correct (y/n)? y
-- Using 10.75.120.111 as this machine's IP

-- Preparing Gateway environment for password-less SSH

Please enter your Gateway server's password. Don't worry when not seeing as you type.
If you've made a mistake, press backspace sufficiently and retry.
admin@[redacted]'s password: _
```

g. Enter the Expert mode password of your Security Gateway / Management Server.

Output:



```
Enter Gateway server's IP: [redacted]

-- Setting up discovery engine for server [redacted]
-- Generating RSA key pair...
-- Generating readme...

NOTE: This must be the same IP you enter in your Quantum IoT Profile.
Enter DHCP (this machine) server's IP: [redacted]
Are you sure this IP is correct (y/n)? y
-- Using [redacted] as this machine's IP

-- Preparing Gateway environment for password-less SSH

Please enter your Gateway server's password. Don't worry when not seeing as you type.
If you've made a mistake, press backspace sufficiently and retry.
admin@[redacted]'s password:

-- Setting permissions of private key to SYSTEM only
-- Generating script to copy log files
-- Settings permissions of batch file to SYSTEM only
-- Scheduling task to copy logs every 1 minute

Discovery engine setup successful.
Make sure to select MS-DHCP in your Quantum IoT Profile (in Infinity Portal), and enforce.
It's crucial to enforce the profile as soon as possible.


Press any key to close this setup tool...
```

The discovery engine setup is complete.

h. To close the setup tool, press any key.

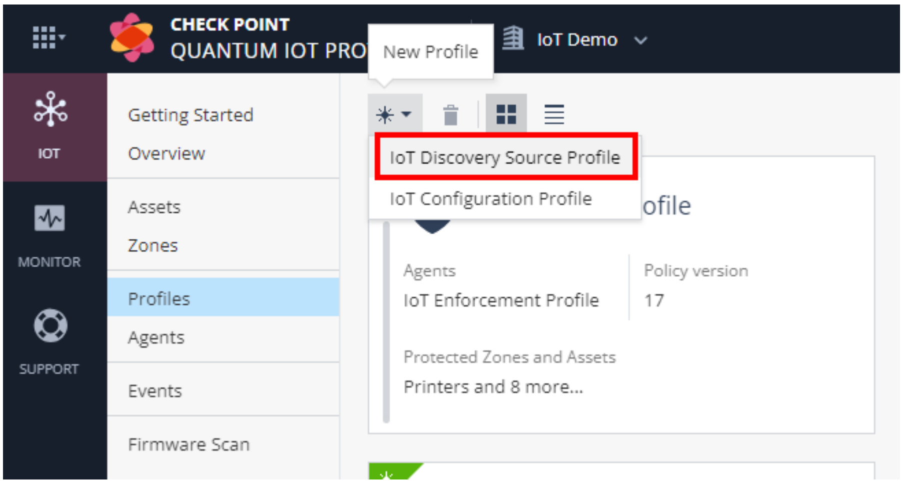
   After the installation, the system copies the DHCP logs to your Security Gateway / Management Server at one-minute intervals.

2. Configure MS-DHCP as the discovery engine in Quantum IoT Protect:

   a. Log in to *Check Point Infinity Portal*.

   b. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.

   c. Click ✳ and select **IoT Discovery Source Profile**.



   d. Enter these:

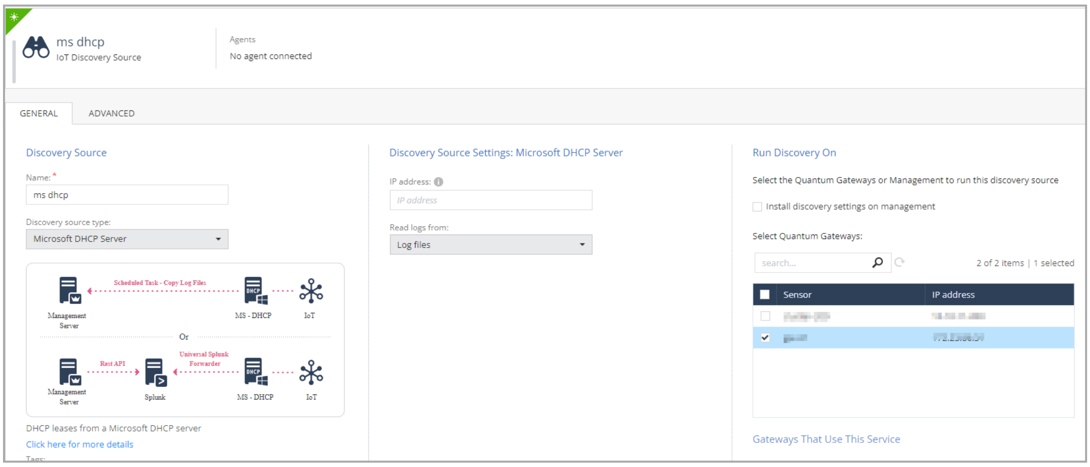
      i. In the **Discovery Source** section, from the **Discovery source type** list, select **Microsoft DHCP Server**.

      ii. In the **Discovery Source Settings** section:

         - In the **IP address** field, enter the IP address of the MS-DHCP server.
         - From the **Read logs from** list, select **Log files**.

iii. In the **Run Discovery On** section, select the Security Gateway from the list.

If you use a Standalone or Management server, select **Install discovery settings on management**.



ms dhcp
IoT Discovery Source

Agents
No agent connected

GENERAL | ADVANCED

Discovery Source

Name: * ms dhcp

Discovery source type: Microsoft DHCP Server

DHCP leases from a Microsoft DHCP server

Click here for more details

Tags:

Discovery Source Settings: Microsoft DHCP Server

IP address: IP address

Read logs from: Log files

Run Discovery On

Select the Quantum Gateways or Management to run this discovery source

□ Install discovery settings on management

Select Quantum Gateways:

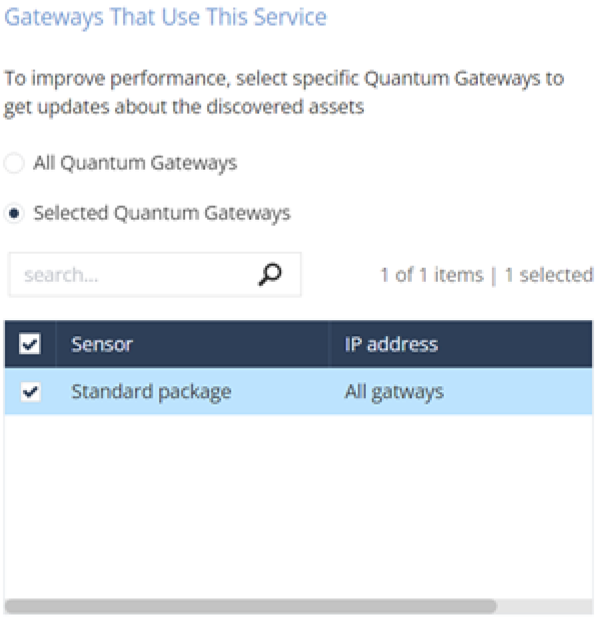
search...

2 of 2 items | 1 selected

□	Sensor	IP address
□	[redacted]	[redacted]
☑	[redacted]	[redacted]

Gateways That Use This Service

iv. In the **Gateways That Use This Service** section, select the gateways relevant to your discovered assets, or select the policy-package for all gateways.



Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways

● Selected Quantum Gateways

search...

1 of 1 items | 1 selected

☑	Sensor	IP address
☑	Standard package	All gatways

e. Click **Enforce**.

The system installs the MS-DHCP discovery engine and starts running on the Check Point Security Gateway / Management Server.

Testing the MS-DHCP - IoT Discovery Engine

1. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console).

2. Log in to the Expert mode.

3. Run:

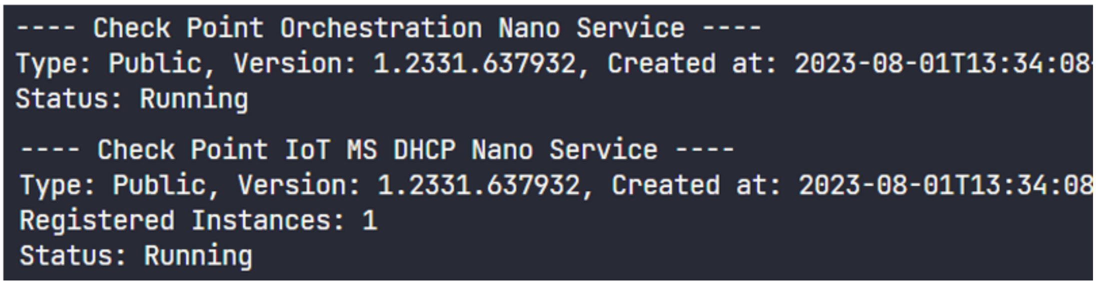
   ```
   cpnano -s
   ```

   Note - The output for this command may take time to appear depending on how long the system takes to enforce the profile. If you do not see the output, then verify whether you have selected the correct Security Gateway / Management Server in the Profiles setting.

4. These nano services must be running:

   - `Check Point Orchestration`
   - `Check Point IoT MS DHCP`

   Output:

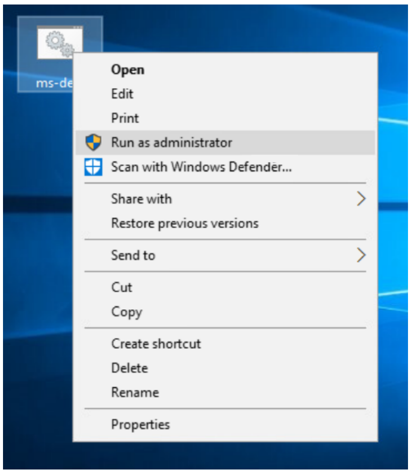


```
---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2331.637932, Created at: 2023-08-01T13:34:08
Status: Running

---- Check Point IoT MS DHCP Nano Service ----
Type: Public, Version: 1.2331.637932, Created at: 2023-08-01T13:34:08
Registered Instances: 1
Status: Running
```

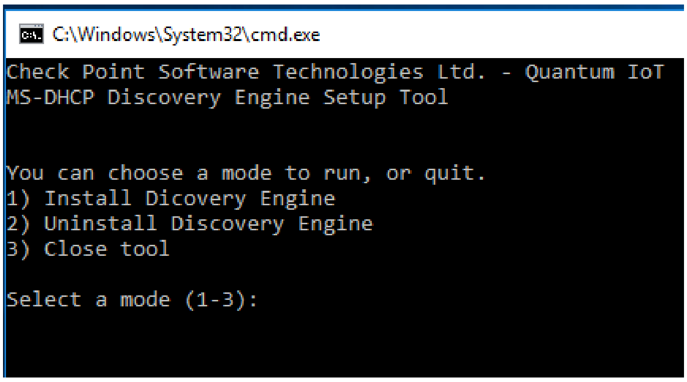
Removing MS-DHCP as the IoT Discovery Engine (Logs Read from Local Directory)

To remove MS-DHCP as the IoT discovery engine from the MS-DHCP server:

1. On the MS-DHCP server, right-click the setup tool **ms-dest.bat** and click **Run as administrator**.



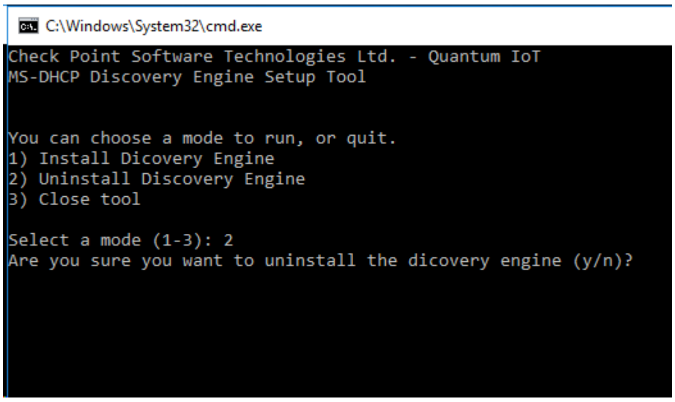
Output:



```
Check Point Software Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


You can choose a mode to run, or quit.
1) Install Dicovery Engine
2) Uninstall Discovery Engine
3) Close tool

Select a mode (1-3):
```

2. Enter **2** and press **Enter**.

   Output:

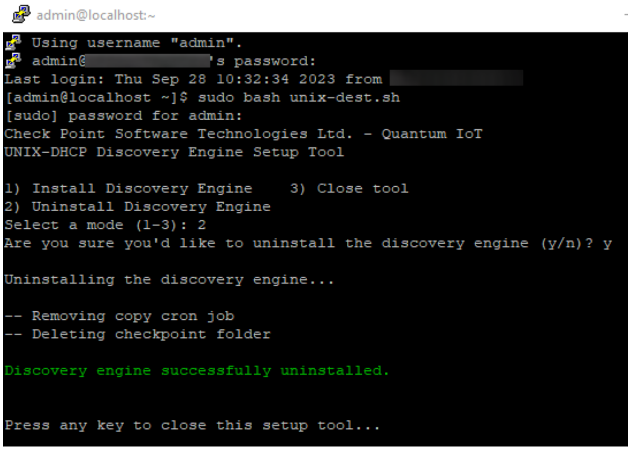


C:\Windows\System32\cmd.exe

```
Check Point Software Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


You can choose a mode to run, or quit.
1) Install Dicovery Engine
2) Uninstall Discovery Engine
3) Close tool

Select a mode (1-3): 2
Are you sure you want to uninstall the dicovery engine (y/n)?
```

3. To confirm, enter **y** and press **Enter**.

   The system removes the scheduled copy task and uninstalls the MS-DHCP server as the discovery engine.



admin@localhost:~

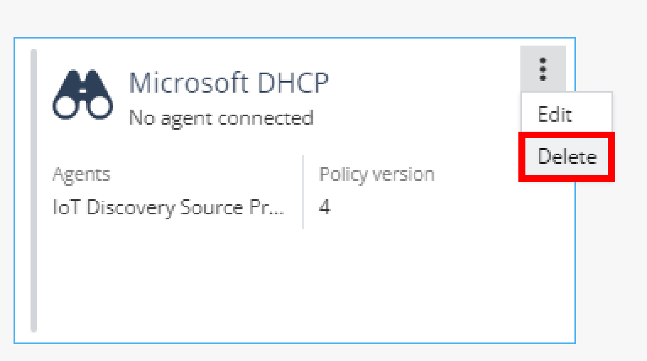
```
Using username "admin".
admin@[redacted]'s password:
Last login: Thu Sep 28 10:32:34 2023 from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 2
Are you sure you'd like to uninstall the discovery engine (y/n)? y

Uninstalling the discovery engine...

-- Removing copy cron job
-- Deleting checkpoint folder

Discovery engine successfully uninstalled.


Press any key to close this setup tool...
```

4. To close the tool, press any key.

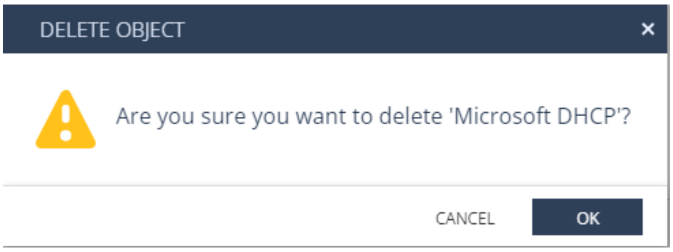
   DHCP logs are no longer copied to the Security Gateway / Management Server.

To remove the IoT Discovery Source Profile in Quantum IoT Protect:

1. Log in to *Check Point Infinity Portal*.
2. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.
3. On the **Microsoft DHCP** discovery engine profile, click ⋮ and then **Delete**.


Microsoft DHCP
No agent connected
Agents
IoT Discovery Source Pr...
Policy version
4

4. To confirm deletion, click **OK**.


DELETE OBJECT
Are you sure you want to delete 'Microsoft DHCP'?

5. Click **Enforce**.

Installing OpenSSH on the MS-DHCP Server

The MS-DHCP server requires OpenSSH to copy log files to the Check Point Security Gateway / Management Server over SSH.

It is installed by default on Windows Server 2019 and higher.

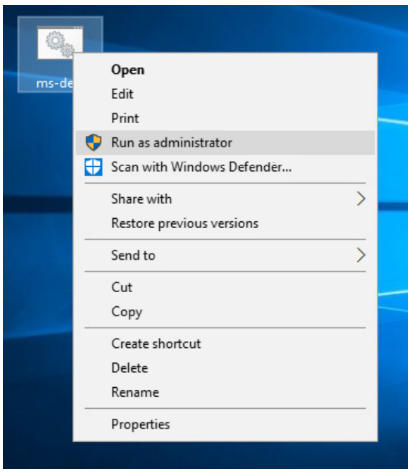
For older versions, you can manually install it or use the MS-DHCP Discover Engine Setup tool to install it for you.

Installing OpenSSH using the MS-DHCP Discovery Engine Setup Tool

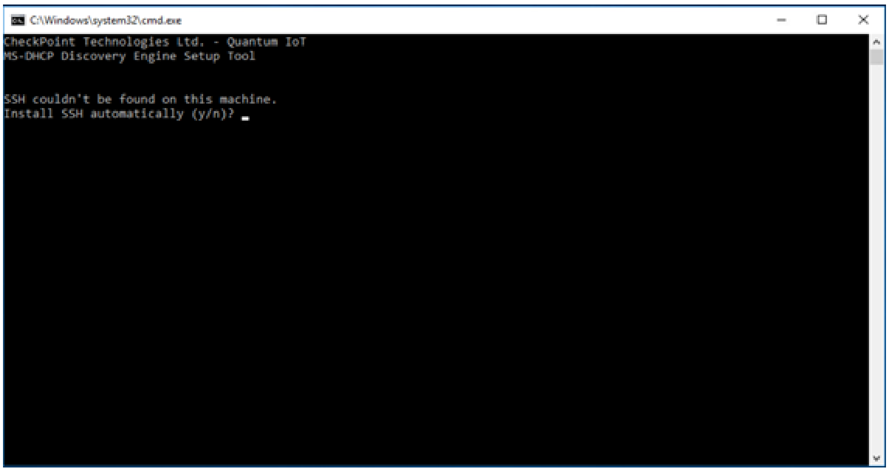
This procedure requires PowerShell 3.0 or higher installed on the MS-DHCP server.

To install OpenSSH using the MS-DHCP Discovery Engine Setup Tool:

1. On the MS-DHCP server, right-click the **ms-dest.bat** file and click **Run as administrator**.



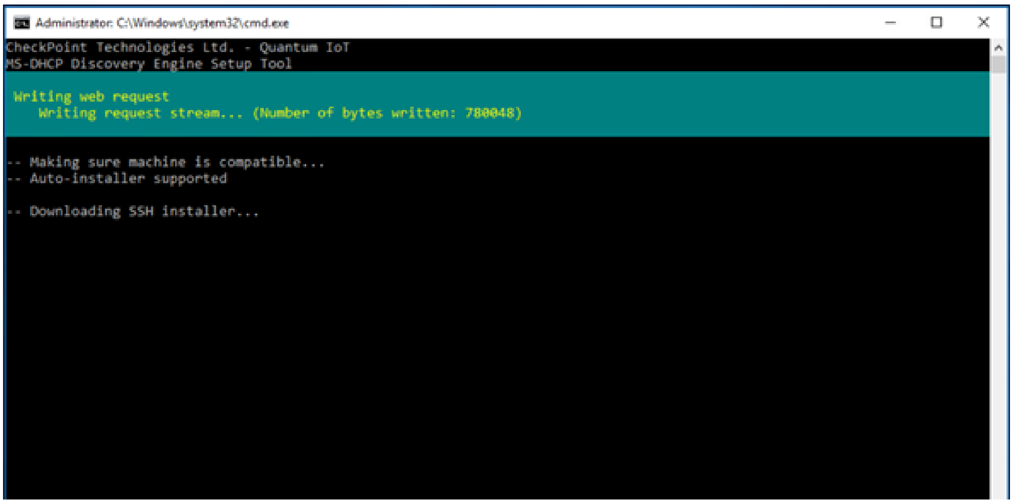
Output:



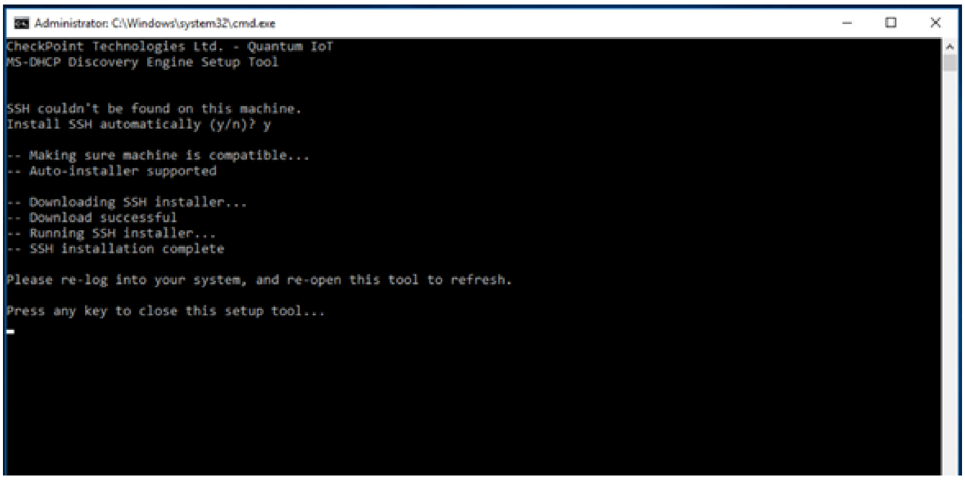
```
CheckPoint Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


SSH couldn't be found on this machine.
Install SSH automatically (y/n)? _
```

2. Enter **y** and then press **Enter**.

   Output:

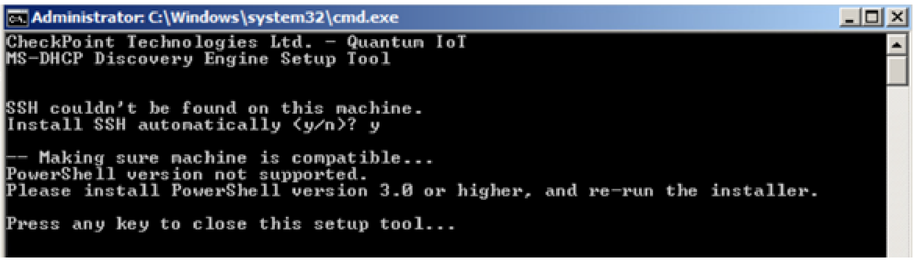


```
CheckPoint Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool

 Writing web request
    Writing request stream... (Number of bytes written: 780048)


-- Making sure machine is compatible...
-- Auto-installer supported

-- Downloading SSH installer...
```



```
CheckPoint Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


SSH couldn't be found on this machine.
Install SSH automatically (y/n)? y

-- Making sure machine is compatible...
-- Auto-installer supported

-- Downloading SSH installer...
-- Download successful
-- Running SSH installer...
-- SSH installation complete

Please re-log into your system, and re-open this tool to refresh.

Press any key to close this setup tool...
```

Note - If this output appears, you can either install OpenSSH manually or install PowerShell 3.0 and repeat the procedure.



```
CheckPoint Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


SSH couldn't be found on this machine.
Install SSH automatically (y/n)? y

-- Making sure machine is compatible...
PowerShell version not supported.
Please install PowerShell version 3.0 or higher, and re-run the installer.

Press any key to close this setup tool...
```

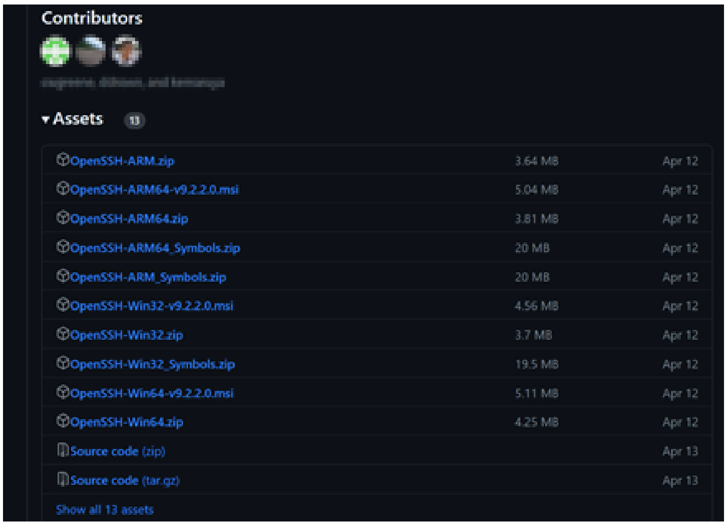
3. Press any key to close the window.

4. Continue with the installation of MS-DHCP Discovery Engine Setup tool.

Installing OpenSSH Manually

1. Go to OpenSSH release page.

2. For the version you want to install, scroll down and expand **Assets**.



Contributors

[illegible]

▾ Assets 13

OpenSSH-ARM.zip	3.64 MB	Apr 12
OpenSSH-ARM64-v9.2.2.0.msi	5.04 MB	Apr 12
OpenSSH-ARM64.zip	3.81 MB	Apr 12
OpenSSH-ARM64_Symbols.zip	20 MB	Apr 12
OpenSSH-ARM_Symbols.zip	20 MB	Apr 12
OpenSSH-Win32-v9.2.2.0.msi	4.56 MB	Apr 12
OpenSSH-Win32.zip	3.7 MB	Apr 12
OpenSSH-Win32_Symbols.zip	19.5 MB	Apr 12
OpenSSH-Win64-v9.2.2.0.msi	5.11 MB	Apr 12
OpenSSH-Win64.zip	4.25 MB	Apr 12
Source code (zip)		Apr 13
Source code (tar.gz)		Apr 13

Show all 13 assets

3. Download this package:

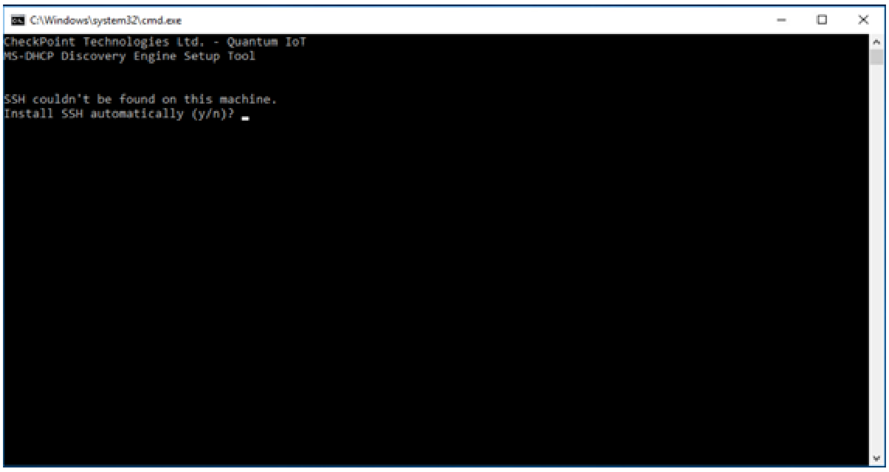
   `OpenSSH-Win64-<version>.msi`

4. Run the installer on the MS-DHCP server.

5. Continue with the installation of MS-DHCP Discovery Engine Setup tool.

Troubleshooting

If the prompt to automatically install SSH appears again, it indicates that the environment variables are not refreshed.



```
CheckPoint Technologies Ltd. - Quantum IoT
MS-DHCP Discovery Engine Setup Tool


SSH couldn't be found on this machine.
Install SSH automatically (y/n)? _
```

Do **one** of these:

- Close and open the **ms-dest.bat** file again directly from the Desktop.
- Sign out and log in again into the MS-DHCP server.
- Restart the MS-DHCP server.

Troubleshooting MS-DHCP IoT Discovery Engine (Logs Read from Local Directory)

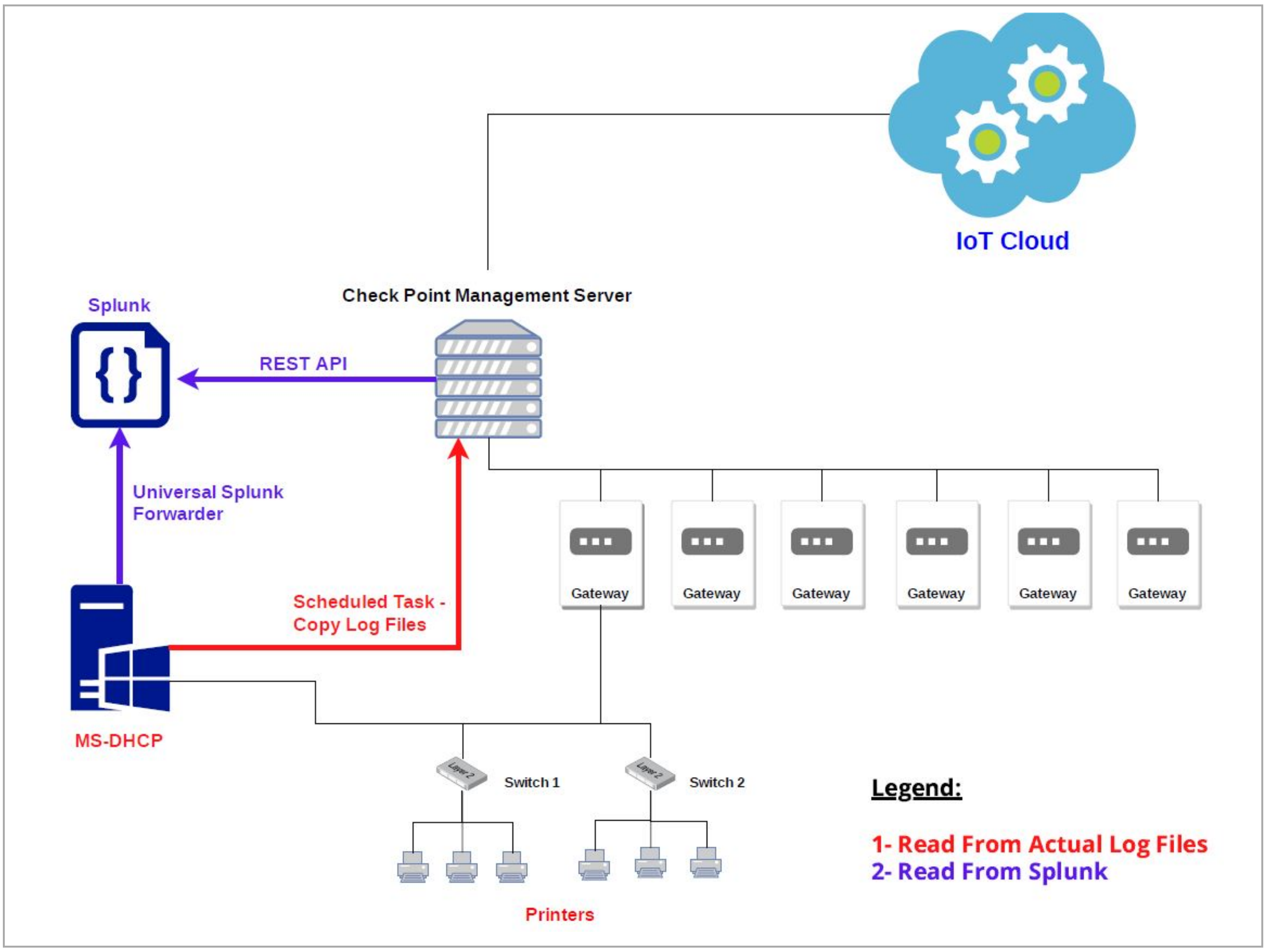
1. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console).
2. Log in to the Expert mode.
3. The DHCP logs files are available in this location:

   /var/log/iot-discovery/ms-dhcp-logs

Appendix D - Using MS-DHCP as the IoT Discovery Engine (Logs Read from Splunk)

You can set up an IoT discovery engine on the Check Point Management Server to discover IoT assets in your network. The IoT discovery engine uses the network devices in the network, such as switches, routers, gateways, or Network Access Control (NAC) devices to discover IoT assets.

You can use the Microsoft Dynamic Host Configuration Protocol (MS-DHCP) server to discover IoT assets. It maintains a pool of IP addresses and provides (leases) an IP address to every new DHCP-enabled client. MS-DHCP integration is based on events log files created by the MS-DHCP server. The events may include the MAC address of the device (DHCP-enabled client) and the leased IP address.



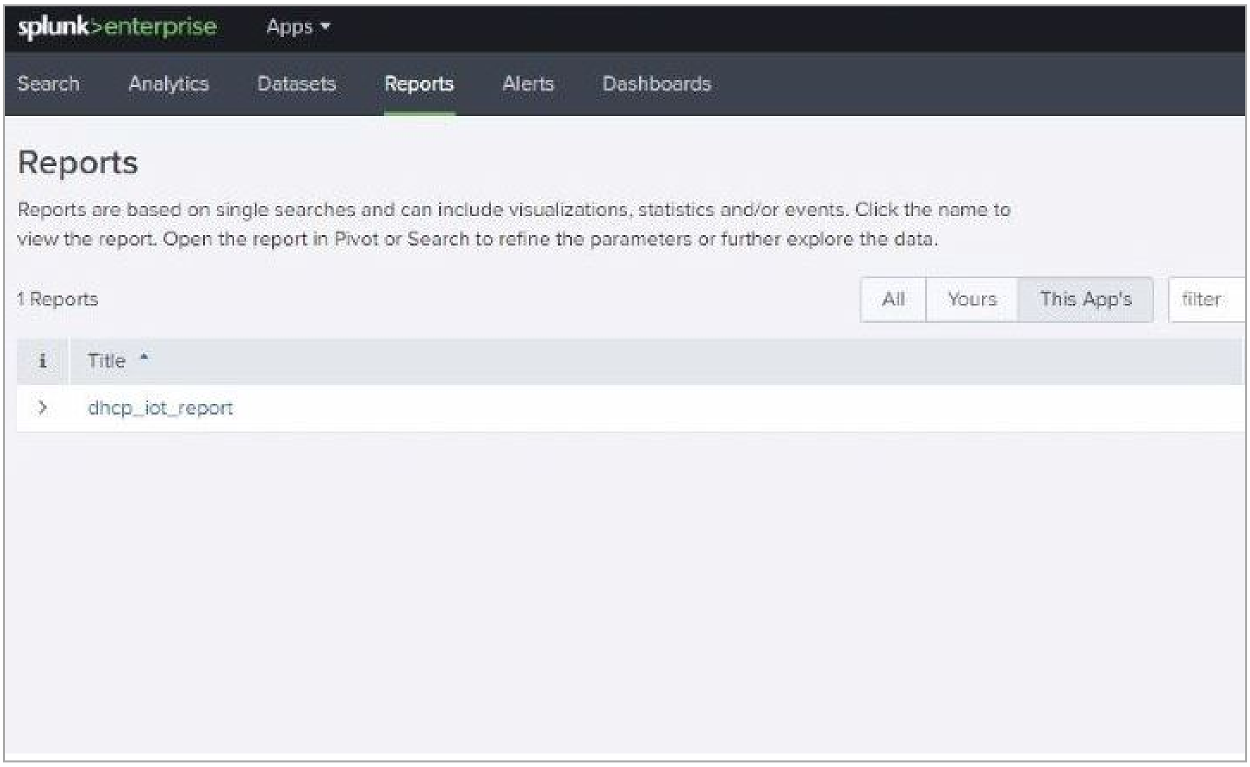
MS-DHCP server reads the DHCP events by one of these methods:

- The event logs from the MS-DHCP server are copied to a local directory and the logs are read from this local directory.
- The event logs from the MS-DHCP server are forwarded to the Splunk server and the logs are read from the Splunk server.

This appendix describes the MS-DHCP integration when the MS-DHCP event logs are read from the Splunk server.

Setting Up MS-DHCP as the IoT Discovery Engine (Logs Read from Splunk)

1. Set the Splunk server to index DHCP event logs created by the MS-DHCP server.
   a. To forward the logs to Splunk, install Splunk Universal Forwarder on the MS-DHCP server. To install the Splunk Universal Forwarder, see Splunk Universal Forwarder.
   b. To parse the MS-DHCP logs, install the Splunk Add-on for Microsoft Windows on the Splunk server. To install Splunk Add-on for Microsoft Windows, see Splunk Add-on for Microsoft Windows.
   c. Create a Custom Index for MS-DHCP logs (DHCP). To create a Custom Index, see Create Custom Indexes.
2. Create a scheduled report of the MS-DHCP event logs on the Splunk server. To create a scheduled report, see Creating Scheduled Reports in Splunk.



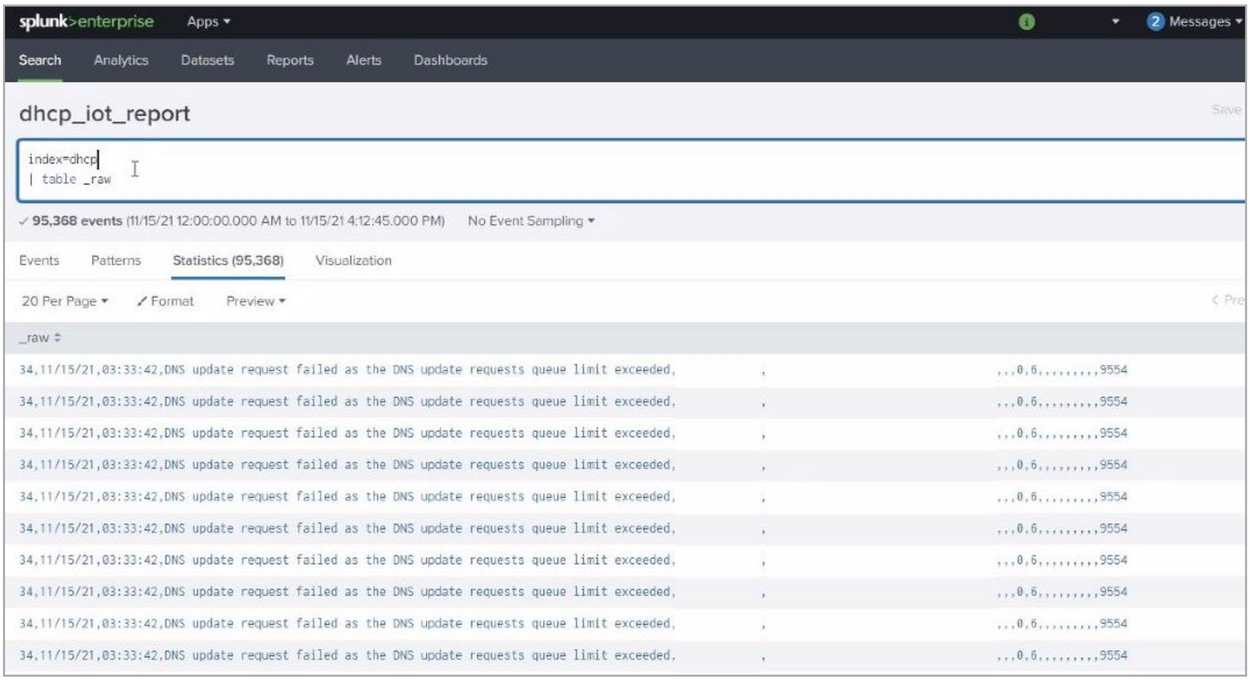
Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

1 Reports

dhcp_iot_report

3. In the report created, search for the keyword *index*dhcp*.



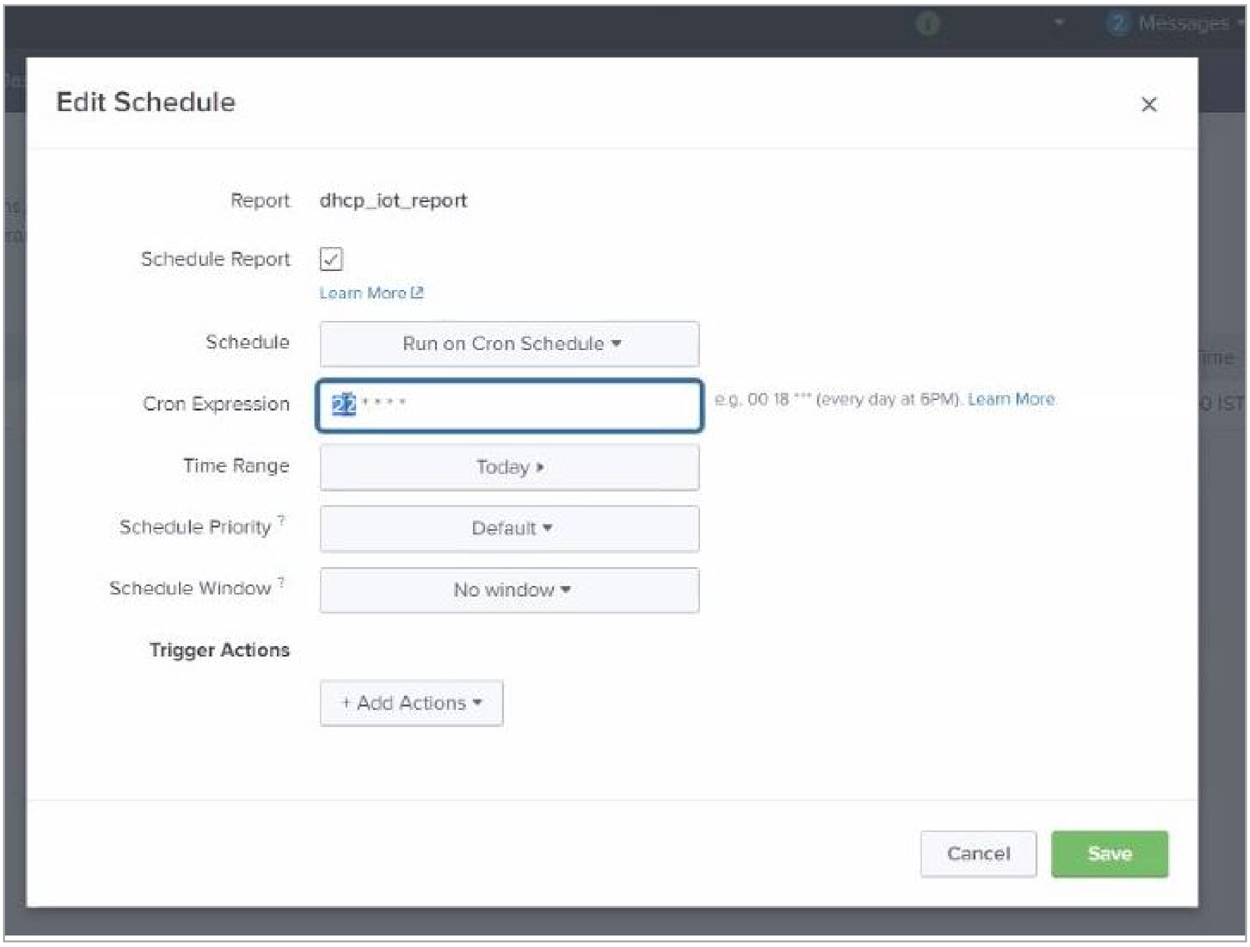
dhcp_iot_report

```
index=dhcp
| table _raw
```

✓ 95,368 events (11/15/21 12:00:00.000 AM to 11/15/21 4:12:45.000 PM)   No Event Sampling ▾

```
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
34,11/15/21,03:33:42,DNS update request failed as the DNS update requests queue limit exceeded,         ,                     ,,,0,6,,,,,,,,,9554
```

4. Edit the schedule for the report.

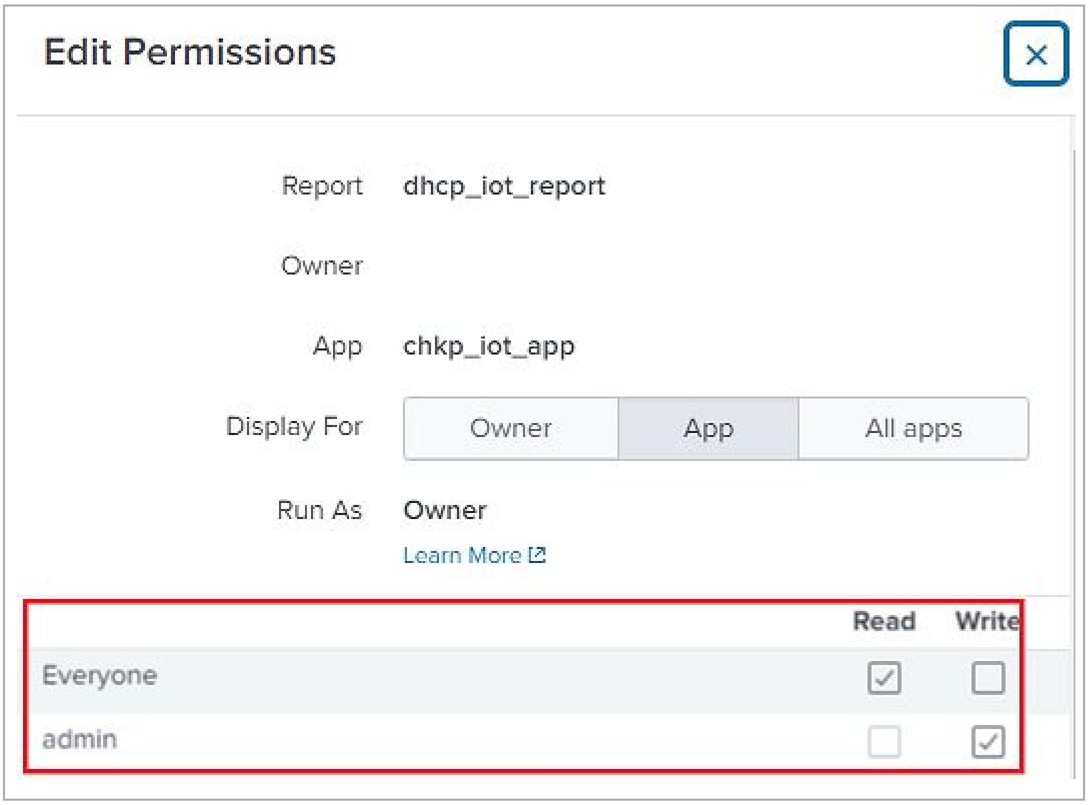


Edit Schedule

Report	dhcp_iot_report
Schedule Report	☑ Learn More
Schedule	Run on Cron Schedule ▾
Cron Expression	22 * * * *
Time Range	Today ▸
Schedule Priority ?	Default ▾
Schedule Window ?	No window ▾
Trigger Actions	+ Add Actions ▾

e.g. 00 18 *** (every day at 6PM). Learn More

5. Set **Read** permission for the report created.



Edit Permissions

Report dhcp_iot_report

Owner

App chkp_iot_app

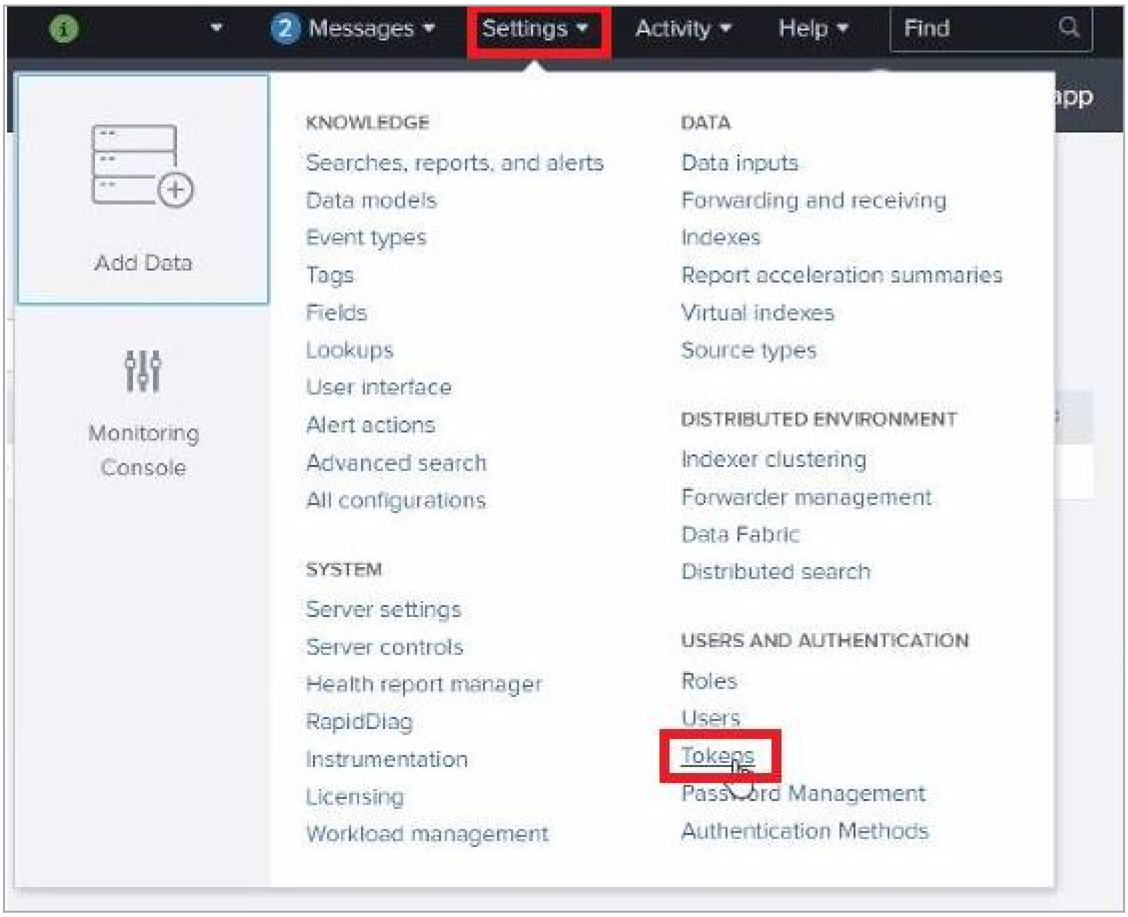
Display For: Owner | [✓ App] | All apps

Run As Owner

	Read	Write
Everyone	☑	□
admin	□	☑

6. Create an authentication token to securely access Splunk REST API to read MS-DHCP event logs (Reading from Splunk).

a. In the Splunk server, go to **Settings > Tokens**.

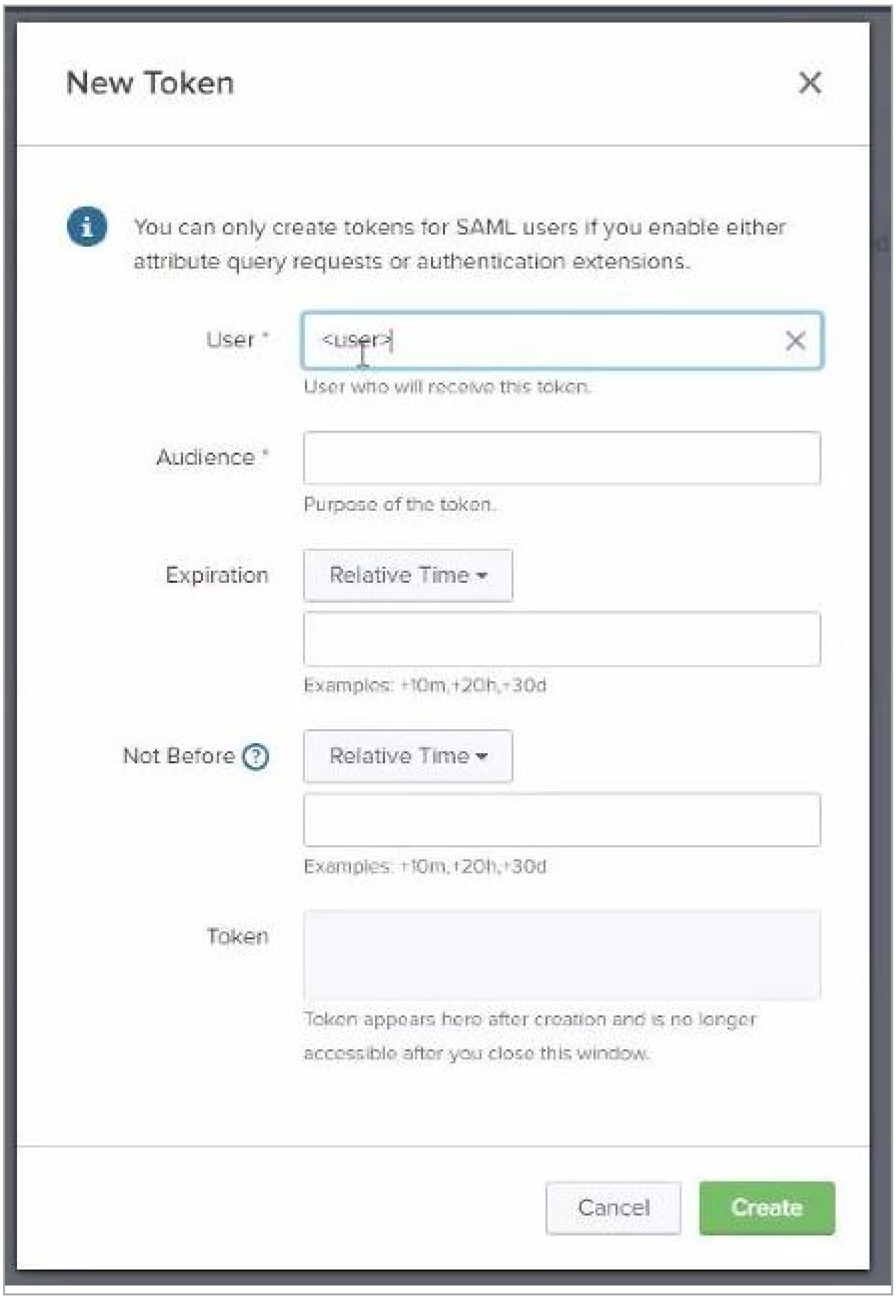


b. Click **New Token**.

c. In the **New Token** window, enter this information:

- **User** - The Splunk platform user that you want to create the token for.
- **Audience** - A short description on the purpose of the token.
- **(Optional) Expiration**- Select **Absolute Time** or **Relative Time**.
- **(Optional) Not Before** - Select **Absolute Time** or **Relative Time**.
- Click **Create**.

  The **New Token** window updates the **Token** field to display the generated token.



New Token

You can only create tokens for SAML users if you enable either attribute query requests or authentication extensions.

User * <user>

User who will receive this token.

Audience *

Purpose of the token.

Expiration Relative Time ▾

Examples: +10m,+20h,+30d

Not Before ? Relative Time ▾

Examples: +10m,+20h,+30d

Token

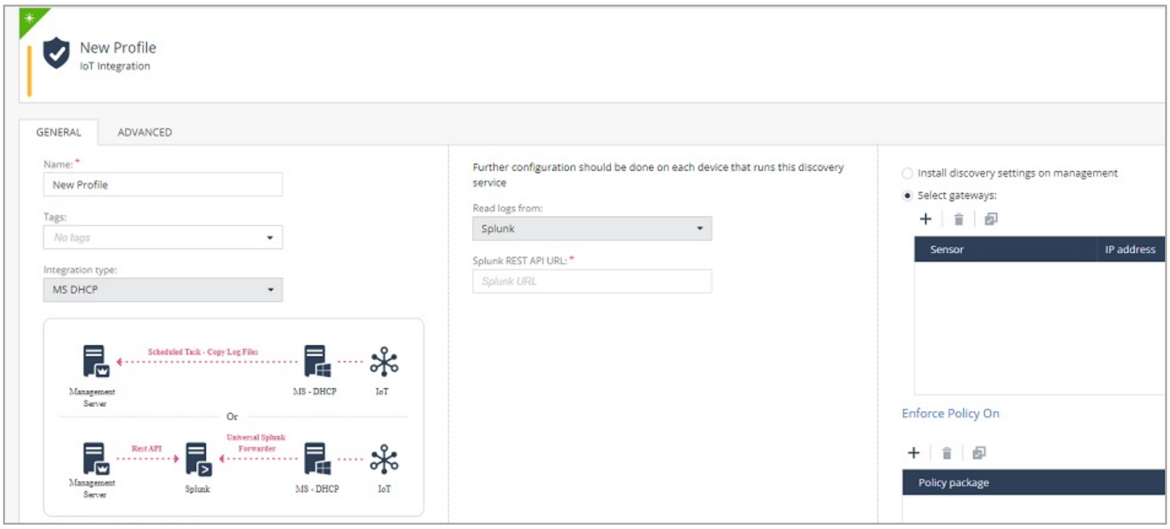
Token appears here after creation and is no longer accessible after you close this window.

7. Enable access to Splunk REST API in the Access Control policy (Reading from Splunk).

Set the relevant access rules in the Access Control policy on the relevant gateway to allow the Management Server to access the Splunk REST API.

Splunk REST API uses port 8089 (over TCP).

8. Set MS-DHCP as the IoT discovery engine in Quantum IoT Protect.
   a. Log in to *[Check Point Infinity Portal]*.
   b. Under **Quantum**, go to **IoT Protect** > **IoT** > **Profiles**.
   c. Set **Integration type** to **MS DHCP**.
   d. Set **Read logs from** to **Splunk**.
   e. Click **Enforce**.



Name: * New Profile

Tags: No tags

Integration type: MS DHCP

Further configuration should be done on each device that runs this discovery service

Read logs from: Splunk

Splunk REST API URL: * Splunk URL

○ Install discovery settings on management

● Select gateways:

Sensor	IP address

9. Set local configuration on the Management Server (When using Splunk).

   MS-DHCP built-in discovery integration can access the Splunk REST API to read the MS-DHCP event logs. To securely access the Splunk REST API, set an authentication token locally on the Management Server.

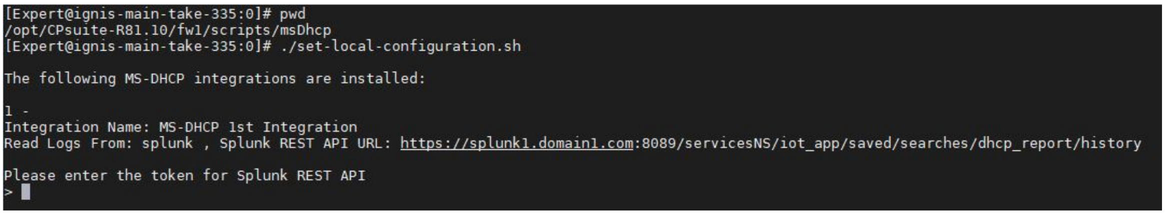
To set the authentication token:

a. Set the integration in Quantum IoT Protect.

b. Access (SSH) the Management Server.

c. Run this bash script:

```
/etc/cp/scripts/iot/msDhcp/set-local-configuration.sh
```



```
[Expert@ignis-main-take-335:0]# pwd
/opt/CPsuite-R81.10/fw1/scripts/msDhcp
[Expert@ignis-main-take-335:0]# ./set-local-configuration.sh

The following MS-DHCP integrations are installed:

1 -
Integration Name: MS-DHCP 1st Integration
Read Logs From: splunk , Splunk REST API URL: https://splunk1.domain1.com:8089/servicesNS/iot_app/saved/searches/dhcp_report/history

Please enter the token for Splunk REST API
> 
```

Configuring integration installed on a cluster gateway

a. Access each gateway through SSH and log in to Expert mode.

b. Change each gateway to active mode. For more information, see Initiating Manual Cluster Failover.

c. Run this bash script:

```
/etc/cp/scripts/iot/msDhcp/set-local-configuration.sh
```

Configuring integration installed on a Management Server with HA or on MDS with HA

a. Access each gateway through SSH and log in to Expert mode.

b. Change the gateway to active mode. For more information, see Changing a Server to Active or Standby.

c. Run the command `/etc/cp/scripts/iot/msDhcp/set-local-configuration.sh`

Testing the MS-DHCP - IoT Discovery Engine

1. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console).

2. Log in to the Expert mode.

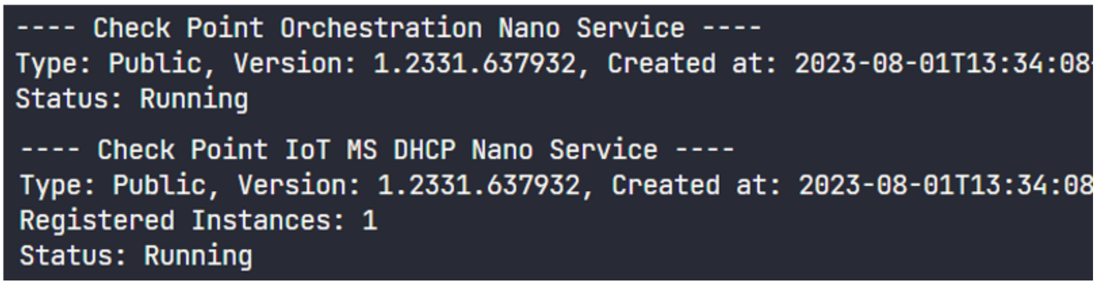
3. Run:

   ```
   cpnano -s
   ```

   Note - The output for this command may take time to appear depending on how long the system takes to enforce the profile. If you do not see the output, then verify whether you have selected the correct Security Gateway / Management Server in the Profiles setting.

4. These nano services must be running:
   - `Check Point Orchestration`
   - `Check Point IoT MS DHCP`

   Output:



```
---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2331.637932, Created at: 2023-08-01T13:34:08
Status: Running
---- Check Point IoT MS DHCP Nano Service ----
Type: Public, Version: 1.2331.637932, Created at: 2023-08-01T13:34:08
Registered Instances: 1
Status: Running
```

Troubleshooting MS-DHCP IoT Discovery Engine (Logs Read from Splunk)

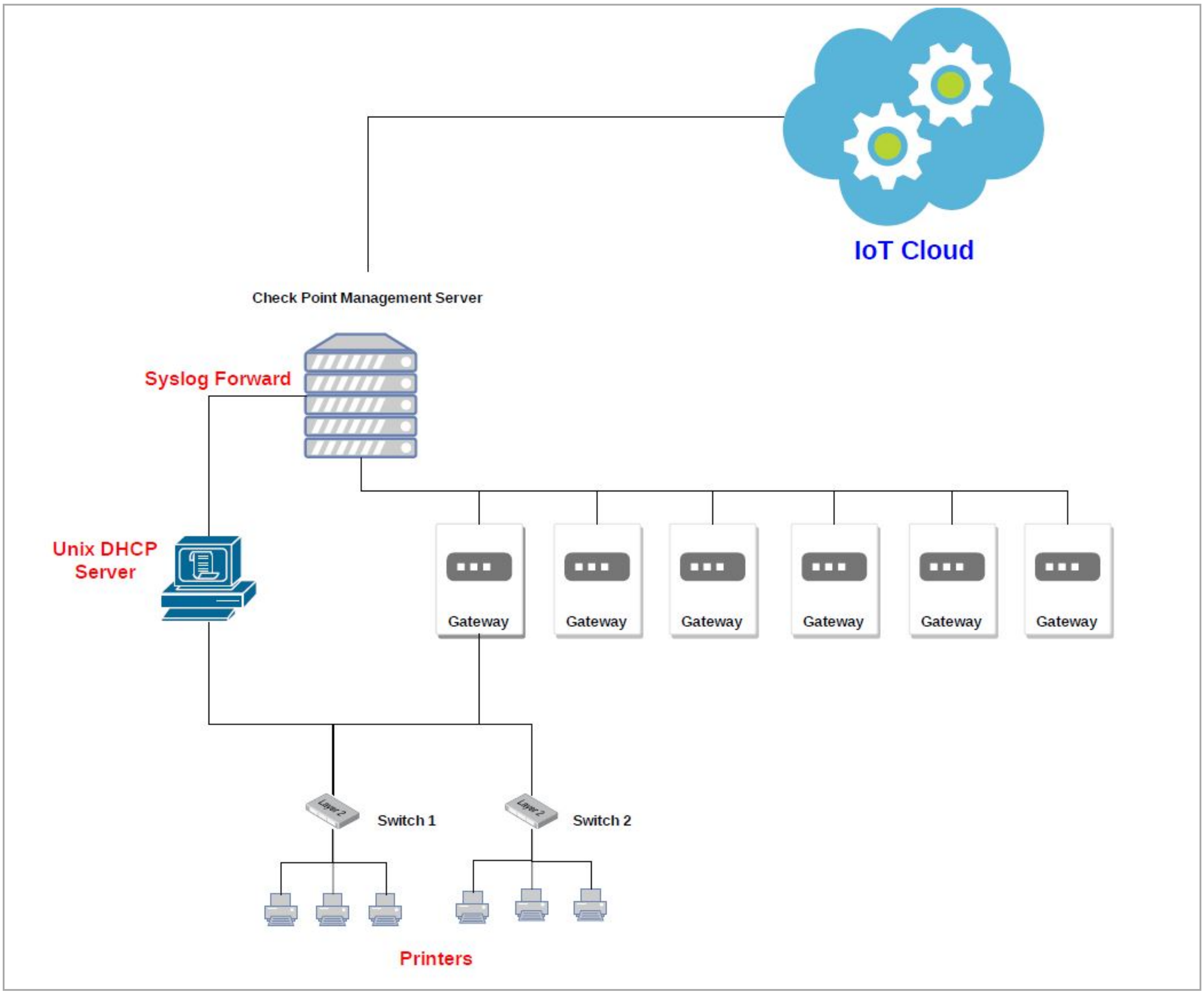
1. Access the Check PointManagement Server through SSH and log in to the Expert mode.
2. Run these commands to ensure that the network and access control rules have enabled the Check Point Management Server access to Splunk REST API:
   - `ping <Splunk server's IP Address>`
   - `ping <Splunk server's FQDN>`
   - `telnet <Splunk server's FQDN> 8089`

Appendix E - Using Unix DHCP - Syslog as the IoT Discovery Engine

You can set up an IoT discovery engine on the Check Point Management Server to discover IoT assets in your network. The IoT discovery engine uses the network devices in the network, such as switches, routers, gateways, or Network Access Control (NAC) devices to discover IoT assets.

You can use Unix DHCP server as an IoT discovery engine. The Unix DHCP server maintains a pool of IP addresses and provides an IP address to every new DHCP-enabled client.

Unix DHCP - Syslog integration is based on Syslog messages generated by the Unix DHCP server. The Syslog message includes the MAC address of the device (DHCP-enabled client) and the leased IP address. Syslog uses port 514 to send log messages over TCP or UDP.



Prerequisites

Set the relevant Access Control rules on the relevant gateway to allow Syslog traffic between the Unix DHCP server and the Check Point Management Server.

To configure the Access Control rule:

a. Connect with SmartConsole to the Check Point Management Server.

b. From the left navigation panel, click **Security Policies**.

c. In the **Access Control** section, click **Policy**.

d. Configure this rule:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Traffic from Unix DHCP to Mgmt	Unix DHCP Server	Check Point Management Server	`Any`	`syslog`	`Accept`	`None`	`Policy Targets`

Setting Up the Unix DHCP - Syslog as the IoT Discovery Engine

To set up Unix DHCP - Syslog as the IoT Discovery Engine:

1. Configure the Unix DHCP server:

   a. Download the `syslog-dest.sh` file.

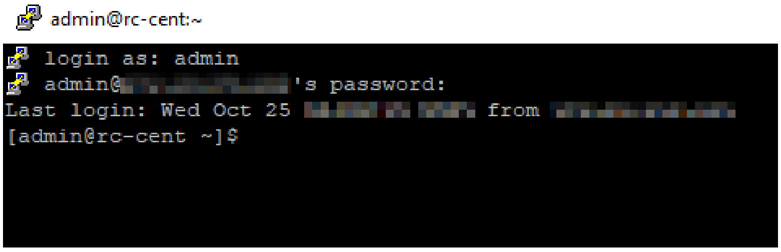
      The system downloads the file.

   b. Transfer the file to the Unix DHCP server.

   c. Connect to the command line on your Unix DHCP server (over SSH or console).

d. Log in with your administrator credentials.

Output:

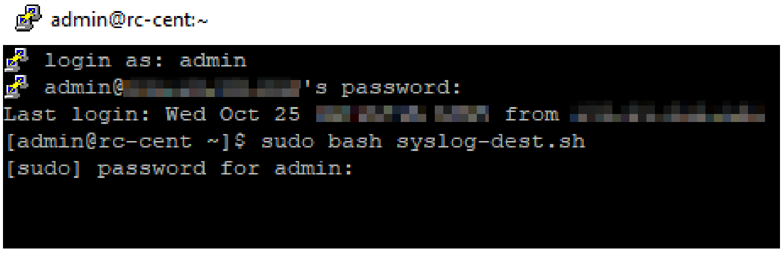


```
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$
```

e. Run:

```
sudo bash syslog-dest.sh
```

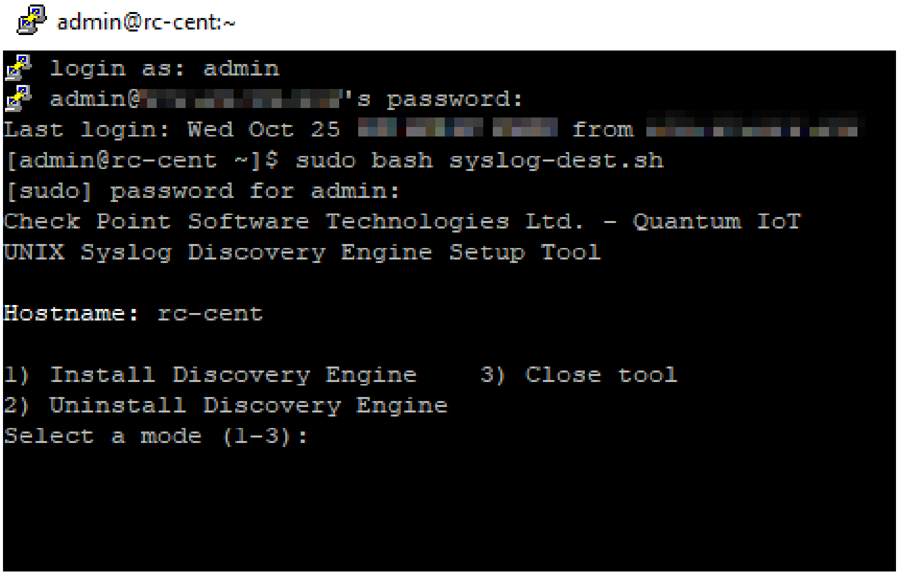
Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
```

f. Enter the administrator password.

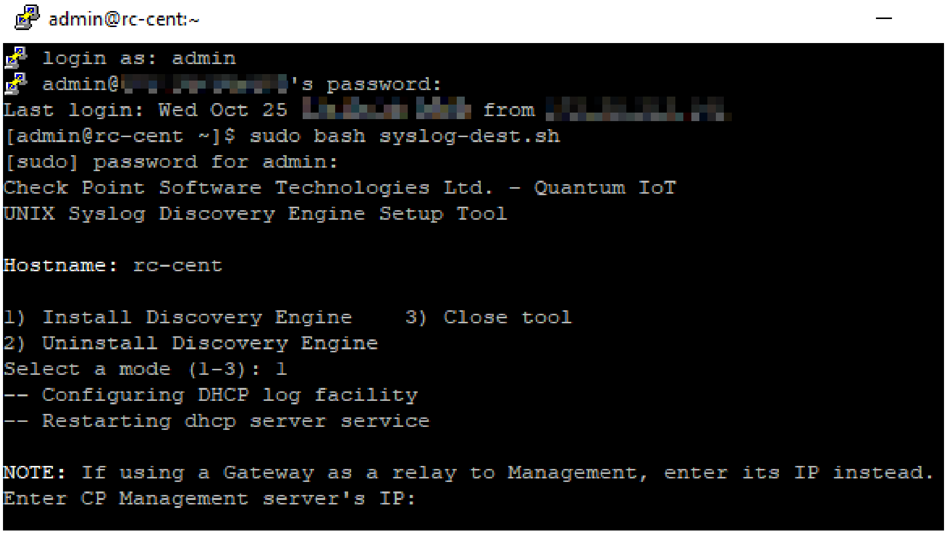
Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX Syslog Discovery Engine Setup Tool

Hostname: rc-cent

1) Install Discovery Engine     3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3):
```

g. To install the discovery engine, enter **1** and press **Enter**.

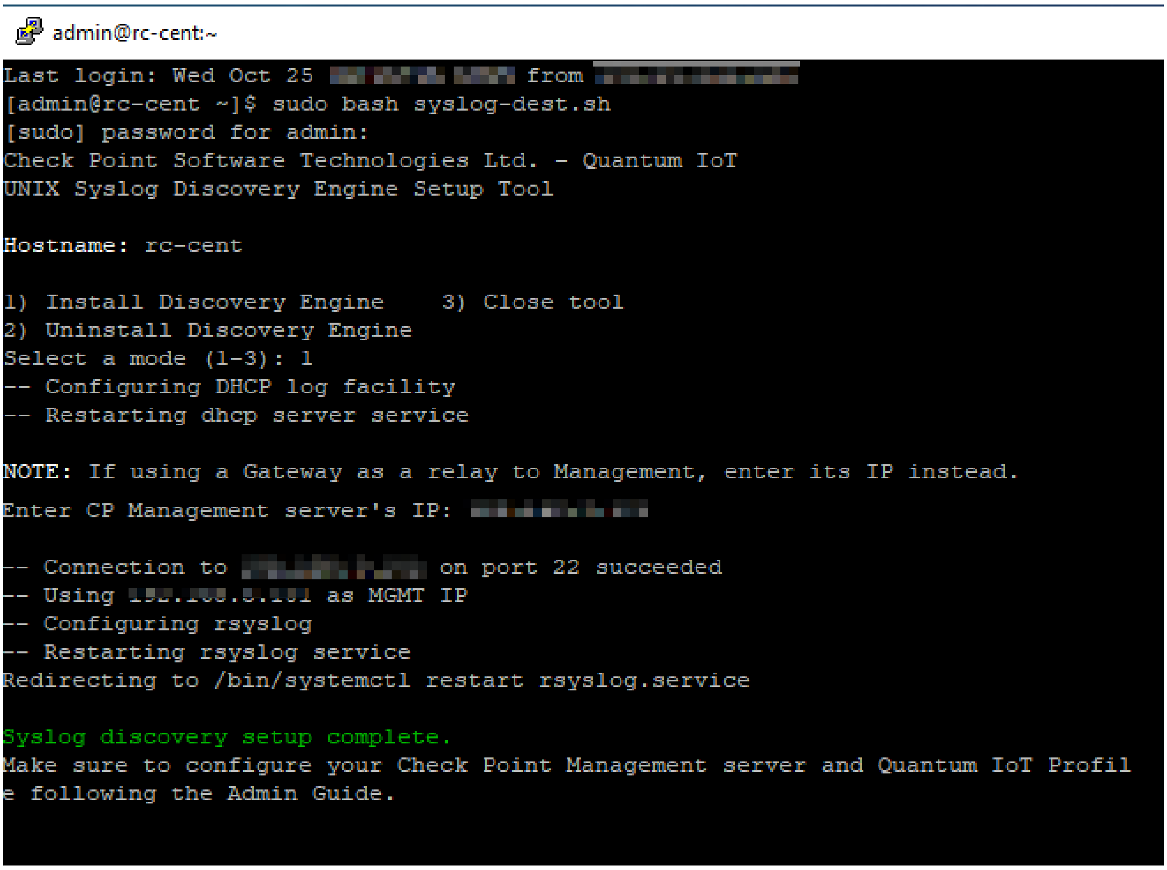
Output:



```
admin@rc-cent:~
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX Syslog Discovery Engine Setup Tool

Hostname: rc-cent

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 1
-- Configuring DHCP log facility
-- Restarting dhcp server service

NOTE: If using a Gateway as a relay to Management, enter its IP instead.
Enter CP Management server's IP:
```

h. Enter the IP address of your Check Point Management Server, and press **Enter**.

Output:



```
admin@rc-cent:~
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX Syslog Discovery Engine Setup Tool

Hostname: rc-cent

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 1
-- Configuring DHCP log facility
-- Restarting dhcp server service

NOTE: If using a Gateway as a relay to Management, enter its IP instead.
Enter CP Management server's IP: [redacted]

-- Connection to [redacted] on port 22 succeeded
-- Using [redacted] as MGMT IP
-- Configuring rsyslog
-- Restarting rsyslog service
Redirecting to /bin/systemctl restart rsyslog.service

Syslog discovery setup complete.
Make sure to configure your Check Point Management server and Quantum IoT Profil
e following the Admin Guide.
```

i. To close the setup tool, type **exit**.

After the installation, the system copies the Syslog logs to your Check Point Management Server at one-minute intervals.

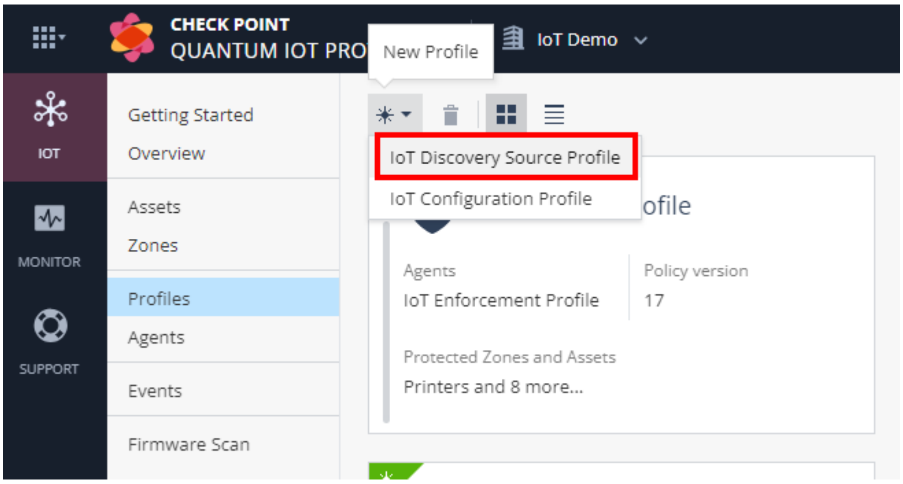
2. Configure **Unix DHCP - Syslog** as the IoT discovery engine in Quantum IoT Protect.

Notes:
- When you install the Unix DHCP - Syslog built-in discovery engine, it modifies the configuration of the Check Point Management Server on which it is installed and enables it to receive Syslog messages.
- Make sure no other user is logged in to **SmartConsole**.

a. Log in to the *Check Point Infinity Portal*.

b. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.

c. Click ✳ and select **IoT Discovery Source Profile**.

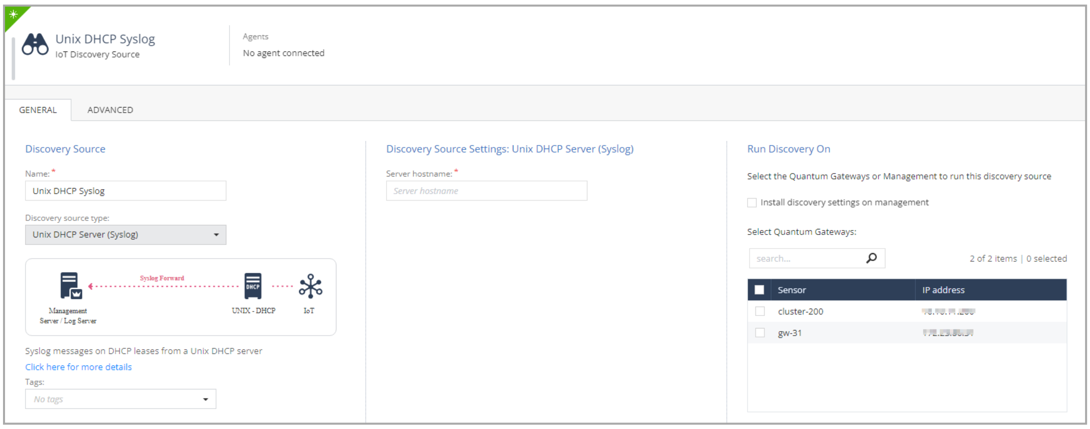


d. Enter these:

   i. In the **Discovery Source** section, from the **Discovery source type** list, select **Unix DHCP Server (Syslog)**.

   ii. In the **Discovery Source Settings** section, in the **Server hostname** field, enter the hostname of the Unix DHCP server.

   iii. In the **Run Discovery On** section, select your Check Point Management Server.



Unix DHCP Syslog
IoT Discovery Source

Agents
No agent connected

GENERAL | ADVANCED

Discovery Source

Name: *
Unix DHCP Syslog

Discovery source type:
Unix DHCP Server (Syslog)

Syslog messages on DHCP leases from a Unix DHCP server
Click here for more details

Tags:
No tags

Discovery Source Settings: Unix DHCP Server (Syslog)

Server hostname: *
Server hostname

Run Discovery On

Select the Quantum Gateways or Management to run this discovery source

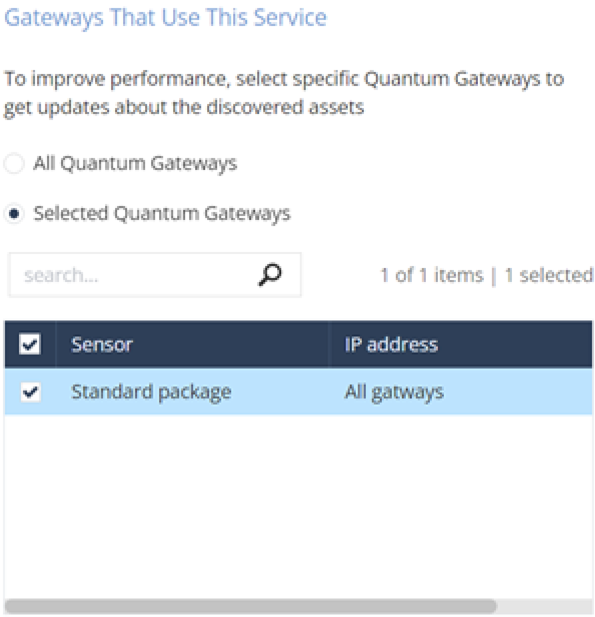
□ Install discovery settings on management

Select Quantum Gateways:

search... 2 of 2 items | 0 selected

□	Sensor	IP address
□	cluster-200	[redacted]
□	gw-31	[redacted]

   iv. In the **Gateways That Use This Service** section, select the gateways relevant to your discovered assets, or select the policy-package for all gateways.



Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways

● Selected Quantum Gateways

search... 1 of 1 items | 1 selected

☑	Sensor	IP address
☑	Standard package	All gatways

e. Click **Enforce**.

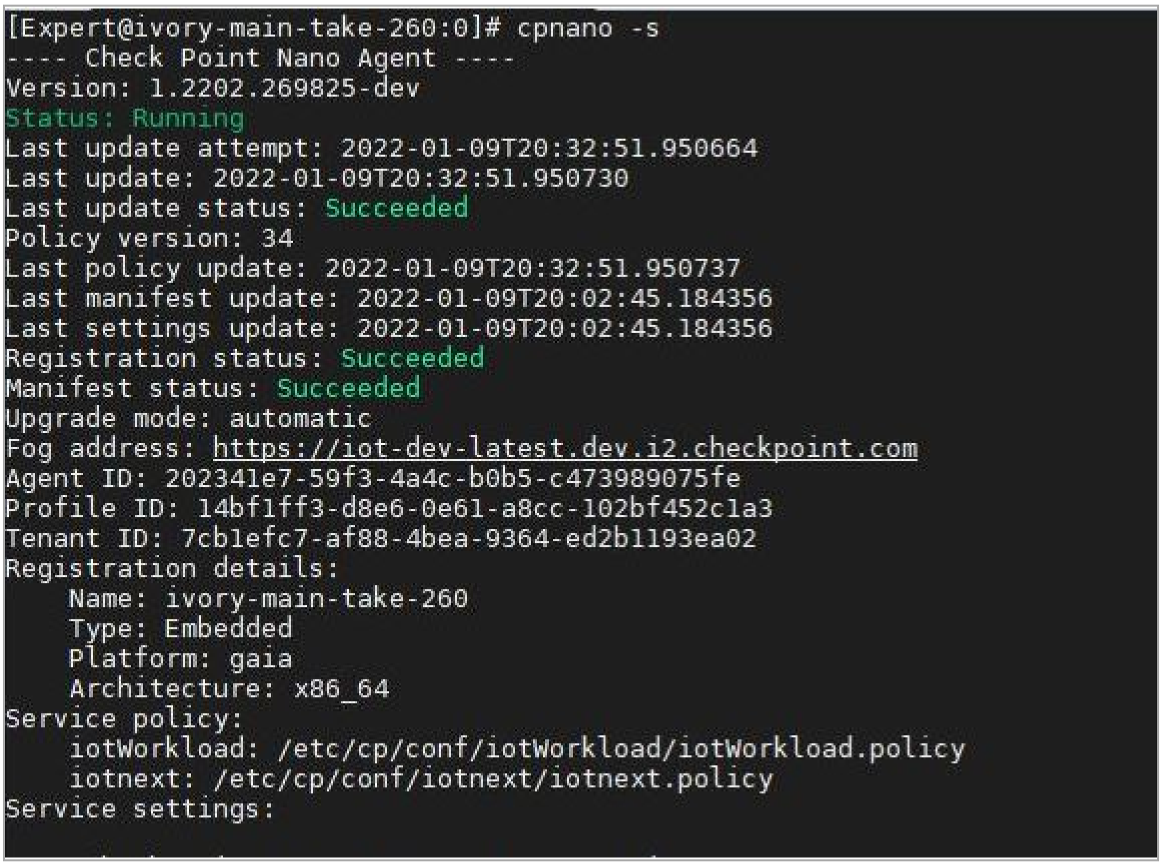
   The system installs the Unix DHCP - Syslog discovery engine and starts running on the Check Point Management Server.

Testing the Unix DHCP - Syslog IoT Discovery Engine

1. Connect to the command line on the Check Point Management Server (over SSH or console).
2. Log in to the Expert mode.
3. Run:

   ```
   cpnano -s
   ```

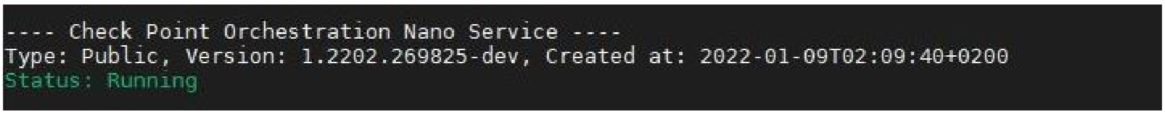
   Output:



```
[Expert@ivory-main-take-260:0]# cpnano -s
---- Check Point Nano Agent ----
Version: 1.2202.269825-dev
Status: Running
Last update attempt: 2022-01-09T20:32:51.950664
Last update: 2022-01-09T20:32:51.950730
Last update status: Succeeded
Policy version: 34
Last policy update: 2022-01-09T20:32:51.950737
Last manifest update: 2022-01-09T20:02:45.184356
Last settings update: 2022-01-09T20:02:45.184356
Registration status: Succeeded
Manifest status: Succeeded
Upgrade mode: automatic
Fog address: https://iot-dev-latest.dev.i2.checkpoint.com
Agent ID: 202341e7-59f3-4a4c-b0b5-c473989075fe
Profile ID: 14bf1ff3-d8e6-0e61-a8cc-102bf452c1a3
Tenant ID: 7cb1efc7-af88-4bea-9364-ed2b1193ea02
Registration details:
    Name: ivory-main-take-260
    Type: Embedded
    Platform: gaia
    Architecture: x86_64
Service policy:
    iotWorkload: /etc/cp/conf/iotWorkload/iotWorkload.policy
    iotnext: /etc/cp/conf/iotnext/iotnext.policy
Service settings:
```

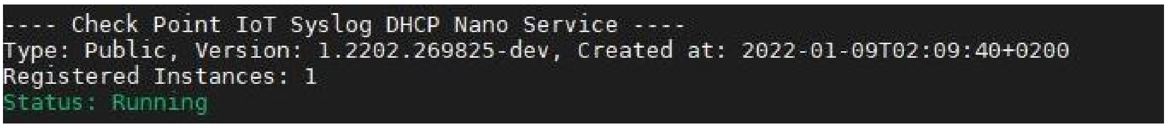
4. These nano services must be running:

   a. `Check Point Orchestration`



```
---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2202.269825-dev, Created at: 2022-01-09T02:09:40+0200
Status: Running
```

   b. `Check Point IoT Syslog DHCP`



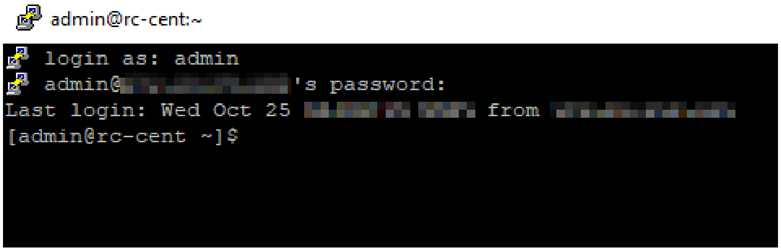
```
---- Check Point IoT Syslog DHCP Nano Service ----
Type: Public, Version: 1.2202.269825-dev, Created at: 2022-01-09T02:09:40+0200
Registered Instances: 1
Status: Running
```

Removing Unix DHCP - Syslog as the IoT Discovery Engine

To remove Unix DHCP - Syslog as the IoT discovery engine from the Unix DHCP server:

1. Connect to the command line on your Unix DHCP server (over SSH or console).
2. Log in with your administrator credentials.

   Output:

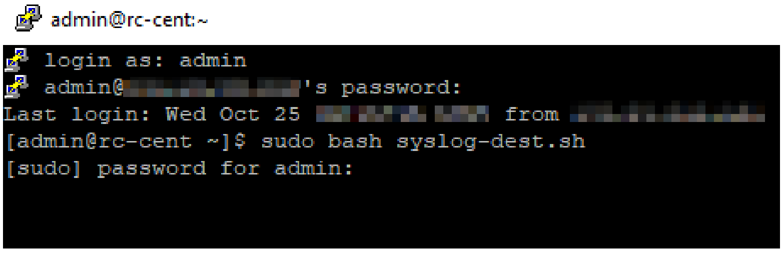


```
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$
```

3. Run:

   `sudo bash syslog-dest.sh`

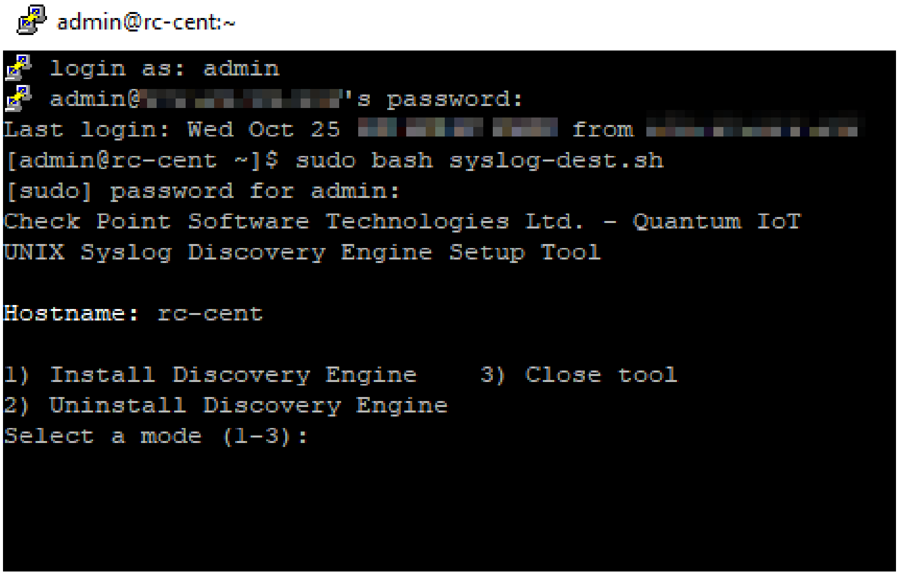
   Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
```

4. Enter the administrator password.

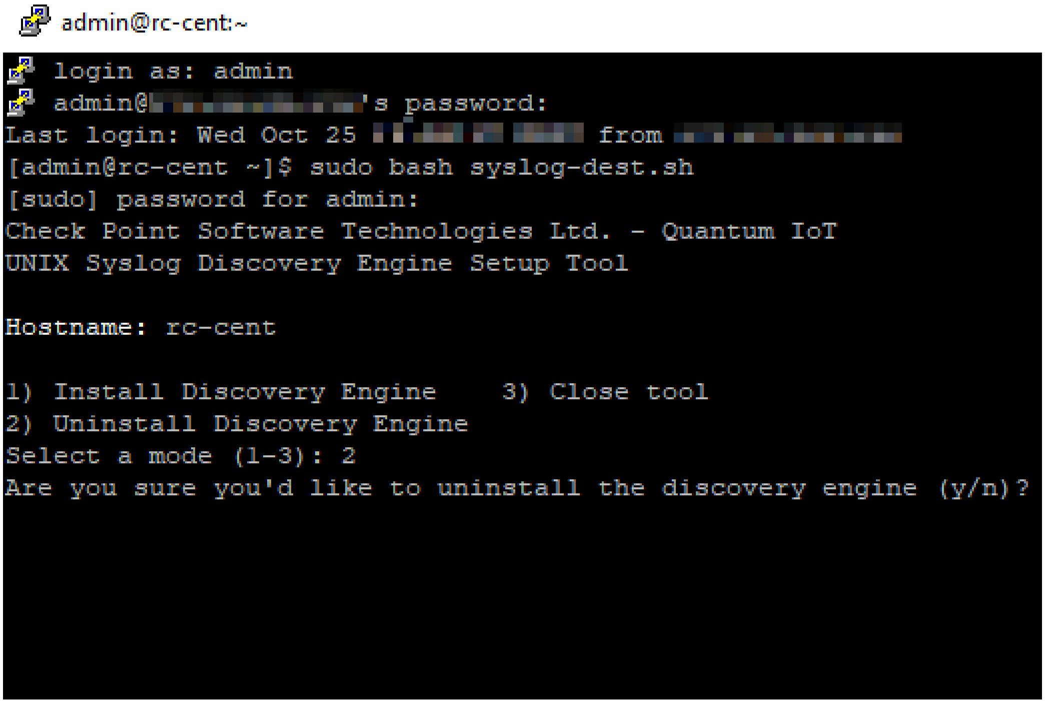
   Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX Syslog Discovery Engine Setup Tool

Hostname: rc-cent

1) Install Discovery Engine     3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3):
```

5. To uninstall the discovery engine, enter **2** and press **Enter**.

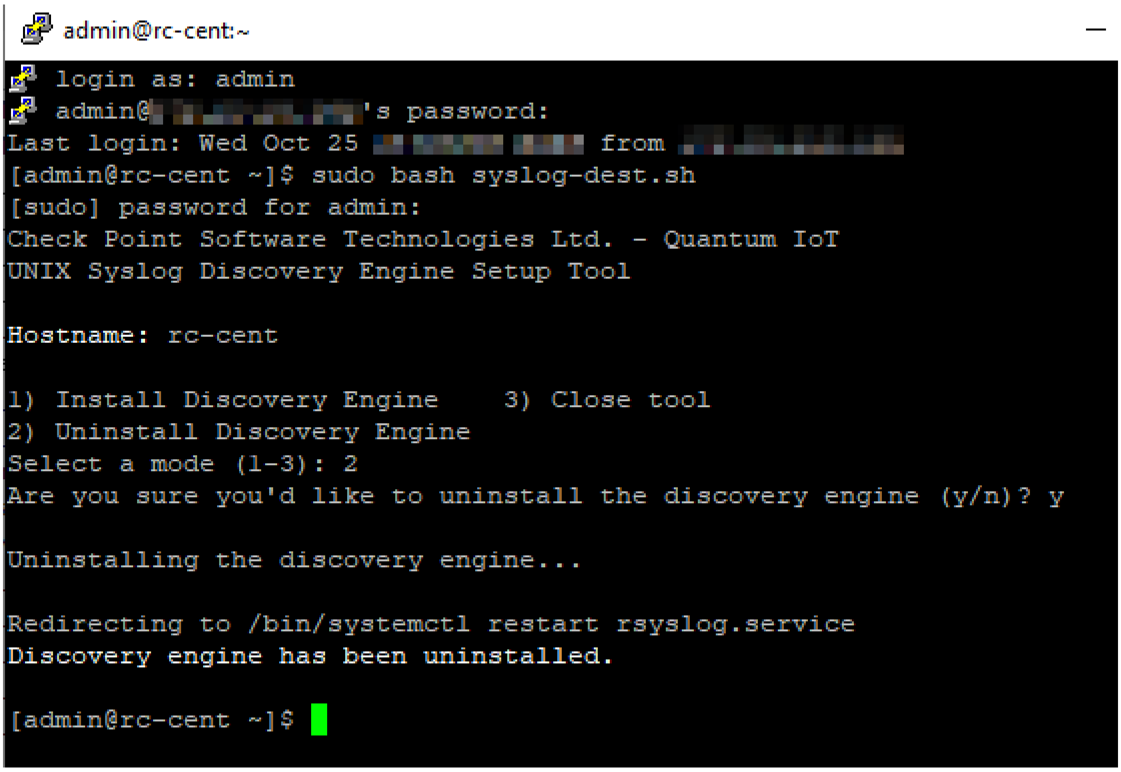
   Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX Syslog Discovery Engine Setup Tool

Hostname: rc-cent

1) Install Discovery Engine     3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 2
Are you sure you'd like to uninstall the discovery engine (y/n)?
```

6. Enter **y** and press **Enter**.

   Output:



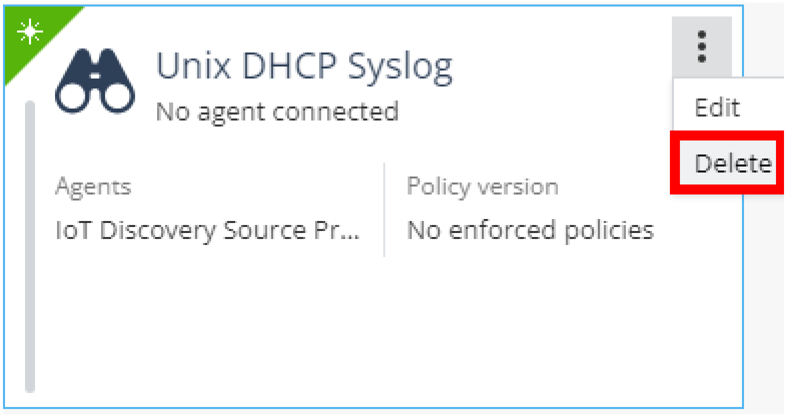
```
admin@rc-cent:~
login as: admin
admin@[redacted]'s password:
Last login: Wed Oct 25 [redacted] from [redacted]
[admin@rc-cent ~]$ sudo bash syslog-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX Syslog Discovery Engine Setup Tool

Hostname: rc-cent

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 2
Are you sure you'd like to uninstall the discovery engine (y/n)? y

Uninstalling the discovery engine...

Redirecting to /bin/systemctl restart rsyslog.service
Discovery engine has been uninstalled.

[admin@rc-cent ~]$
```

7. To close the setup tool, type **exit**.

   The system uninstalls the Unix DHCP - Syslog discovery engine. DHCP logs are no longer copied to the Check Point Management Server.

To remove the IoT Discovery Source Profile in Quantum IoT Protect:

1. Log in to *Check Point Infinity Portal*.
2. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.
3. On the **Unix DHCP Syslog** discovery engine profile, click ⋮ and then **Delete**.

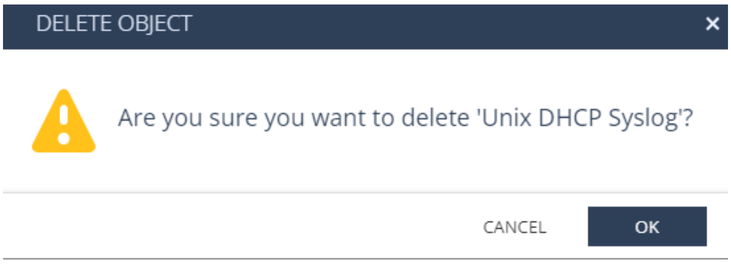


Unix DHCP Syslog
No agent connected

Agents
IoT Discovery Source Pr...

Policy version
No enforced policies

4. Click **OK**.



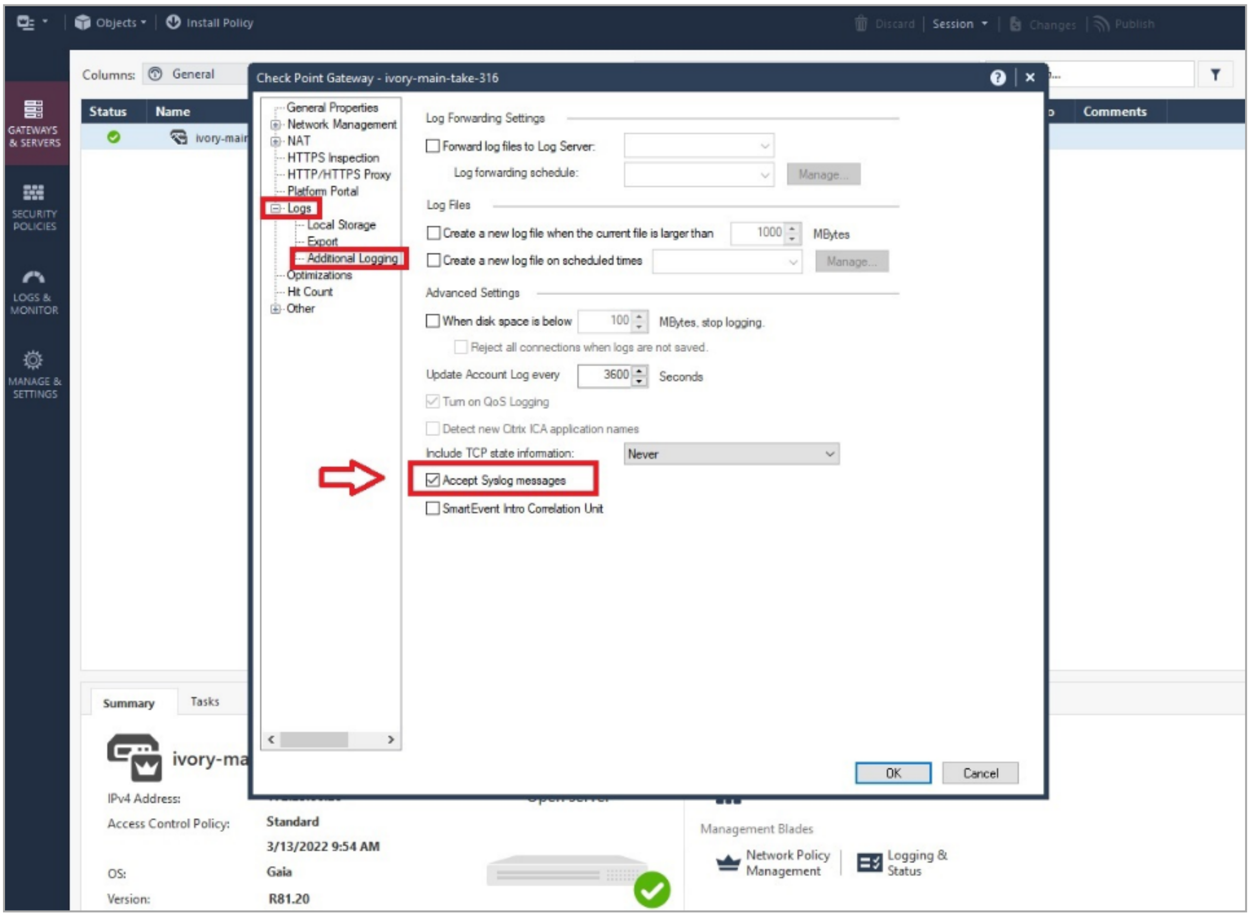
DELETE OBJECT

Are you sure you want to delete 'Unix DHCP Syslog'?

5. Click **Enforce**.

Troubleshooting the Unix DHCP - Syslog IoT Discovery Engine

1. Connect with SmartConsole to the Check Point Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Management Server object.
4. Expand **Logs** > click **Additional Logging**.



Check Point Gateway - ivory-main-take-316

Log Forwarding Settings

☐ Forward log files to Log Server:

Log forwarding schedule:

Log Files

☐ Create a new log file when the current file is larger than 1000 MBytes

☐ Create a new log file on scheduled times

Advanced Settings

☐ When disk space is below 100 MBytes, stop logging.

☐ Reject all connections when logs are not saved.

Update Account Log every 3600 Seconds

☑ Turn on QoS Logging

☐ Detect new Citrix ICA application names

Include TCP state information: Never

☑ Accept Syslog messages

☐ SmartEvent Intro Correlation Unit

IPv4 Address:

Access Control Policy: Standard

3/13/2022 9:54 AM

OS: Gaia

Version: R81.20

5. Select **Accept Syslog messages**.

6. Click **OK**.

7. Install the Access Control policy.

8. Enable Syslog traffic from the Unix DHCP server to the Check Point Management Server:

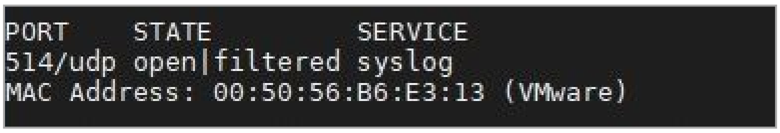
   a. Connect to the command line on your Unix DHCP server (over SSH or console).

   b. Log in with your administrator credentials.

   c. Run:

      i. `nmap -sU -p 514 <IP Address of Management Server>`

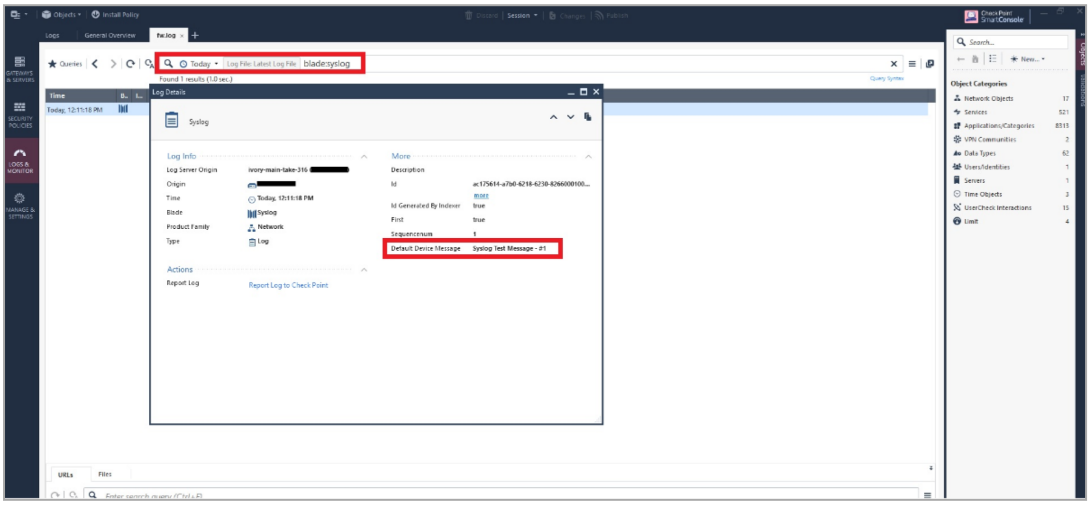
      Expected output:



```
PORT     STATE         SERVICE
514/udp  open|filtered syslog
MAC Address: 00:50:56:B6:E3:13 (VMware)
```

      ii. `echo "Syslog Test Message - #1" | nc -u <IP Address of Management Server> 514`

      Expected output in SmartConsole > **Logs & Monitor** view > **Logs**.



Today ▾ | Log File: Latest Log File | blade:syslog

Found 1 results (1.0 sec.)

Time	B..
Today, 12:11:18 PM	

Log Details

Syslog

Log Info

Log Server Origin	ivory-main-take-316 [redacted]
Origin	[redacted]
Time	Today, 12:11:18 PM
Blade	Syslog
Product Family	Network
Type	Log

Actions

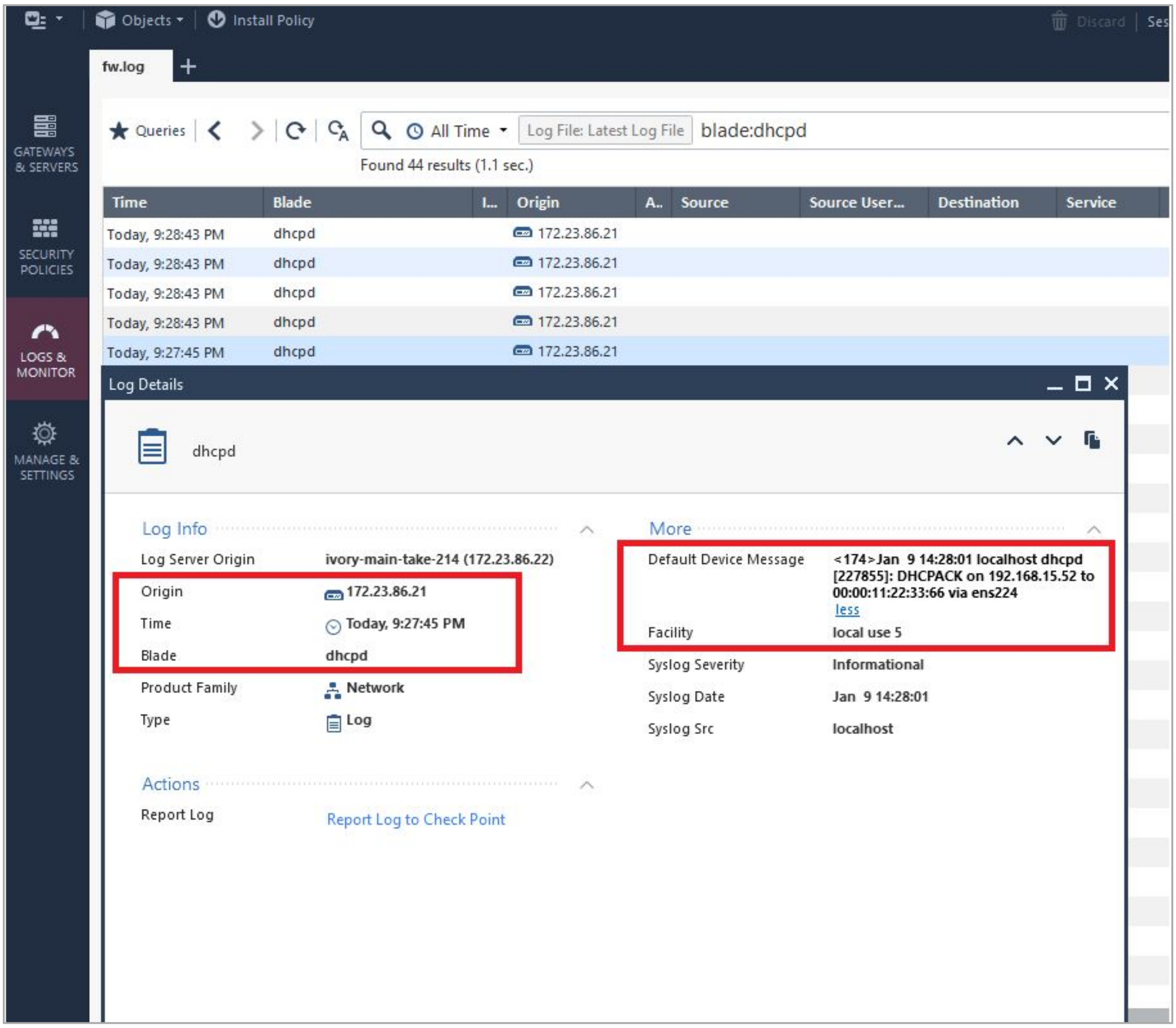
Report Log	Report Log to Check Point

More

Description	
Id	ac175614-a7b0-6218-6230-8266000100... more
Id Generated By Indexer	true
First	true
Sequencenum	1
Default Device Message	Syslog Test Message - #1

9. Filter the logs with this query:

   blade: dhcpd or blade: syslog



blade:dhcpd

Found 44 results (1.1 sec.)

Time	Blade	I...	Origin	A...	Source	Source User...	Destination	Service
Today, 9:28:43 PM	dhcpd		172.23.86.21					
Today, 9:28:43 PM	dhcpd		172.23.86.21					
Today, 9:28:43 PM	dhcpd		172.23.86.21					
Today, 9:28:43 PM	dhcpd		172.23.86.21					
Today, 9:27:45 PM	dhcpd		172.23.86.21					

Log Details

dhcpd

Log Info

Log Server Origin	ivory-main-take-214 (172.23.86.22)
Origin	172.23.86.21
Time	Today, 9:27:45 PM
Blade	dhcpd
Product Family	Network
Type	Log

Actions

Report Log	Report Log to Check Point

More

Default Device Message	<174>Jan 9 14:28:01 localhost dhcpd [227855]: DHCPACK on 192.168.15.52 to 00:00:11:22:33:66 via ens224 less
Facility	local use 5
Syslog Severity	Informational
Syslog Date	Jan 9 14:28:01
Syslog Src	localhost

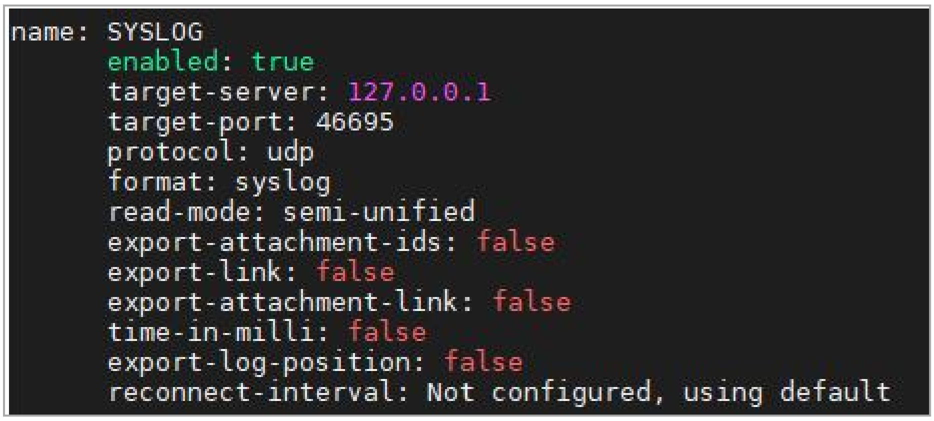
10. Connect to the command line on the Check Point Management Server(over SSH or console).

11. Log in to the Expert mode.

12. Run:

    ```
    cp_log_export show
    ```

    Expected output:



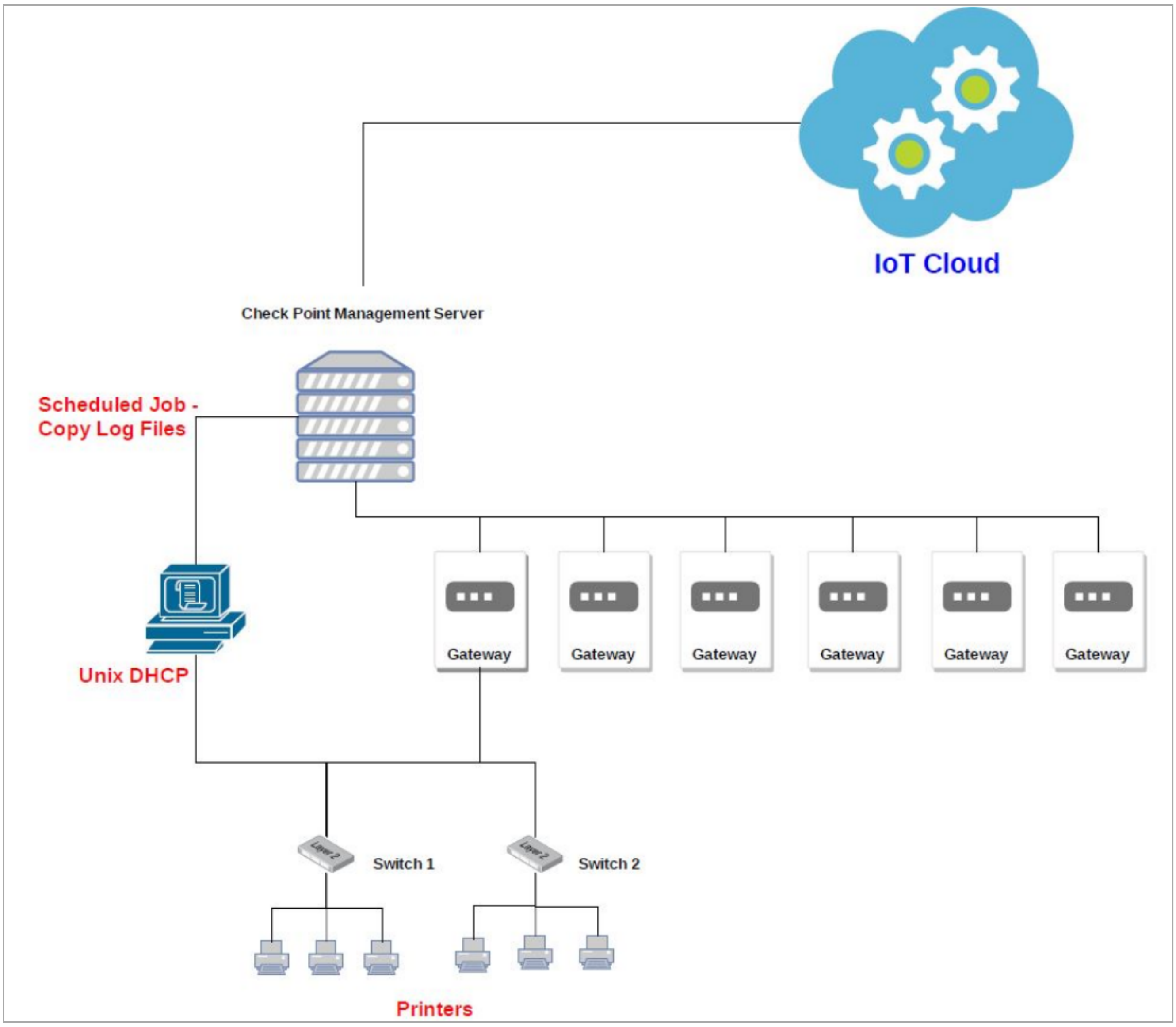
```
name: SYSLOG
      enabled: true
      target-server: 127.0.0.1
      target-port: 46695
      protocol: udp
      format: syslog
      read-mode: semi-unified
      export-attachment-ids: false
      export-link: false
      export-attachment-link: false
      time-in-milli: false
      export-log-position: false
      reconnect-interval: Not configured, using default
```

Appendix F - Using Unix DHCP as the IoT Discovery Engine

You can set up an IoT discovery engine on the Check Point Security Gateway or Management Server to discover IoT assets in your network. The IoT discovery engine uses the network devices in the network, such as switches, routers, gateways, or Network Access Control (NAC) devices to discover IoT assets.

You can use Unix DHCP server as an IoT discovery engine. It maintains a pool of IP addresses and provides an IP address to every new DHCP-enabled client.

Unix DHCP integration is based on log files for events which are created by Unix DHCP server. Such events may include the MAC address of the device and the leased IP address. Unix DHCP integration reads the actual log files from a local directory to which these files are copied.



Prerequisites

- Unix DHCP server with Cron installed. If Cron is not installed, install it using the package manager for your Linux distribution.
- IP address and login credentials of your Check Point Security Gateway / Management Server that is used to discover IoT assets in your network.
- On your Check Point Security Gateway / Management Server, the default shell must be the Expert mode (`/bin/bash`).

  To change the default user shell:

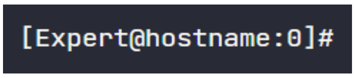
  a. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console).

b. Next step depends on the current configuration:

- If you default shell is the Expert mode, then the prompt shows the word "`Expert`" in front of the hostname.

  There is nothing else to configure.

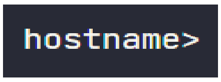
  Example:

  ```
  [Expert@hostname:0]#
  ```

- If you default shell is Gaia Clish, then the prompt shows only the hostname.

  Example:

  ```
  hostname>
  ```

  You can change the default shell in **one** of these ways:

  - In Gaia Portal, configure:

    a. Go to **User Management** > **Users**.

    b. Select and edit the **admin** user.

    c. In the **Shell** field, select **/bin/bash**.

    d. Click **OK**.

  - In Gaia Clish, run:

    a. `set user admin shell /bin/bash`

    b. `save config`

c. Restart your SSH session and check if you are in Expert mode by default.

If you are still in Clish mode, make sure you have entered the correct commands and restart the SSH session.

d. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console) again.

e. The prompt must show the word "`Expert`" in front of the hostname.

Setting Up Unix DHCP as the IoT Discovery Engine

To set up Unix DHCP as the IoT Discovery Engine:

1. Create a Cron task to copy the log files from the Unix DHCP server to the Check Point Security Gateway server / Management Server:

   a. Download the `unix-dest.sh` file.

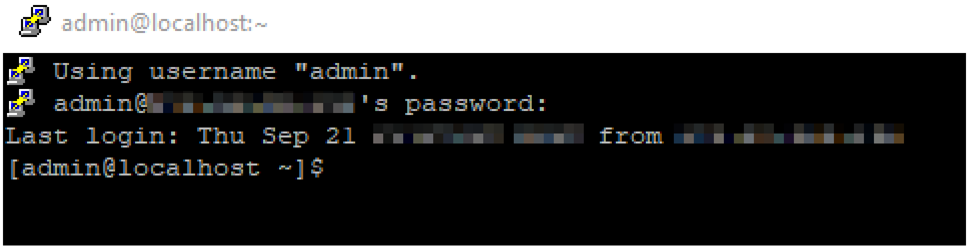
      The system downloads the file.

   b. Transfer the file to the Unix DHCP server.

   c. Connect to the command line on your Unix DHCP server (over SSH or console).

   d. Log in with your administrator credentials.

      Output:

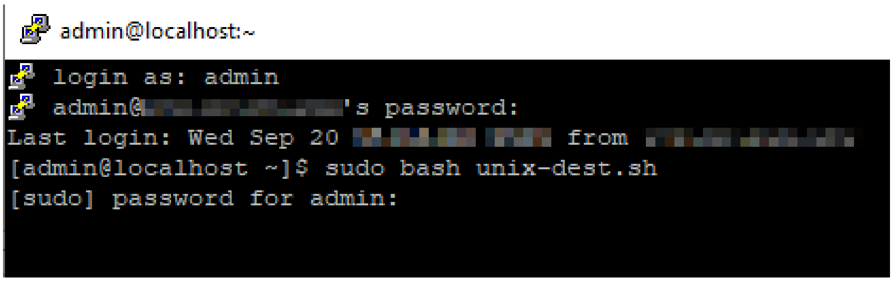
      

```
admin@localhost:~
Using username "admin".
admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] from [redacted]
[admin@localhost ~]$
```

   e. Run:

```
sudo bash unix-dest.sh
```

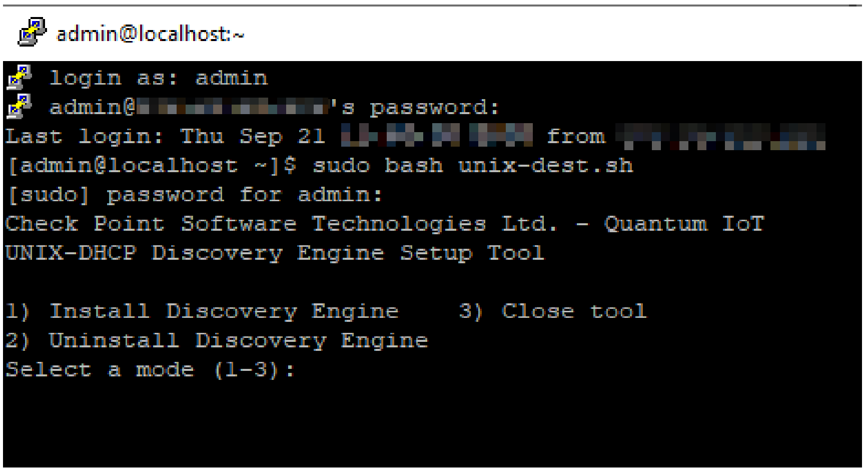
      Output:

```
admin@localhost:~
login as: admin
admin@[redacted]'s password:
Last login: Wed Sep 20 [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
```

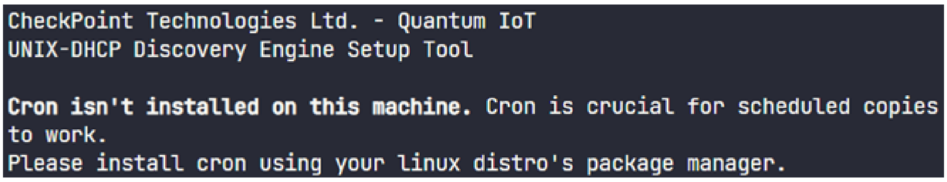
f. Enter the administrator password.

Output:



```
 login as: admin
 admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3):
```

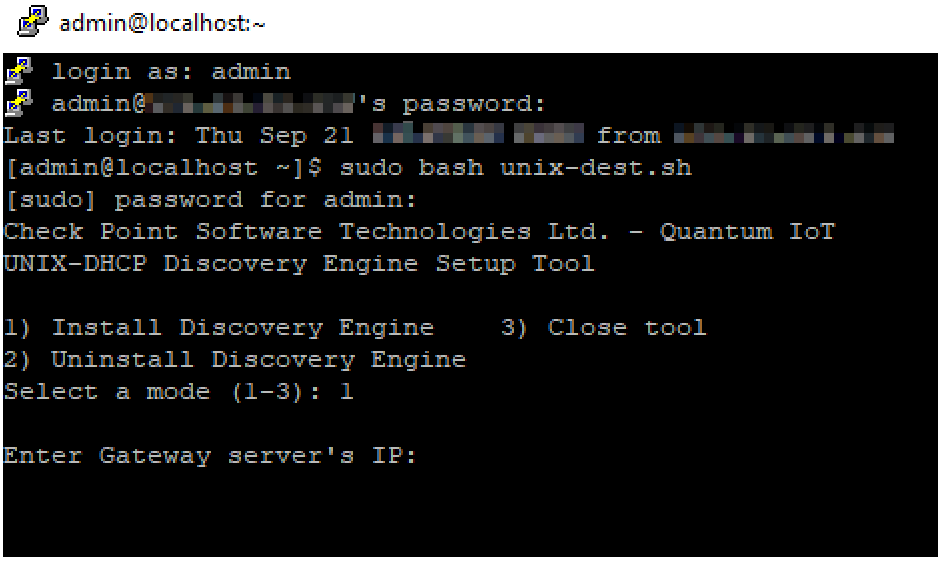
Note - If the following output appears, you must install Cron. See *"Prerequisites" on page 130*.



```
CheckPoint Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

Cron isn't installed on this machine. Cron is crucial for scheduled copies
to work.
Please install cron using your linux distro's package manager.
```

g. To install the discovery engine, enter **1** and press **Enter**.

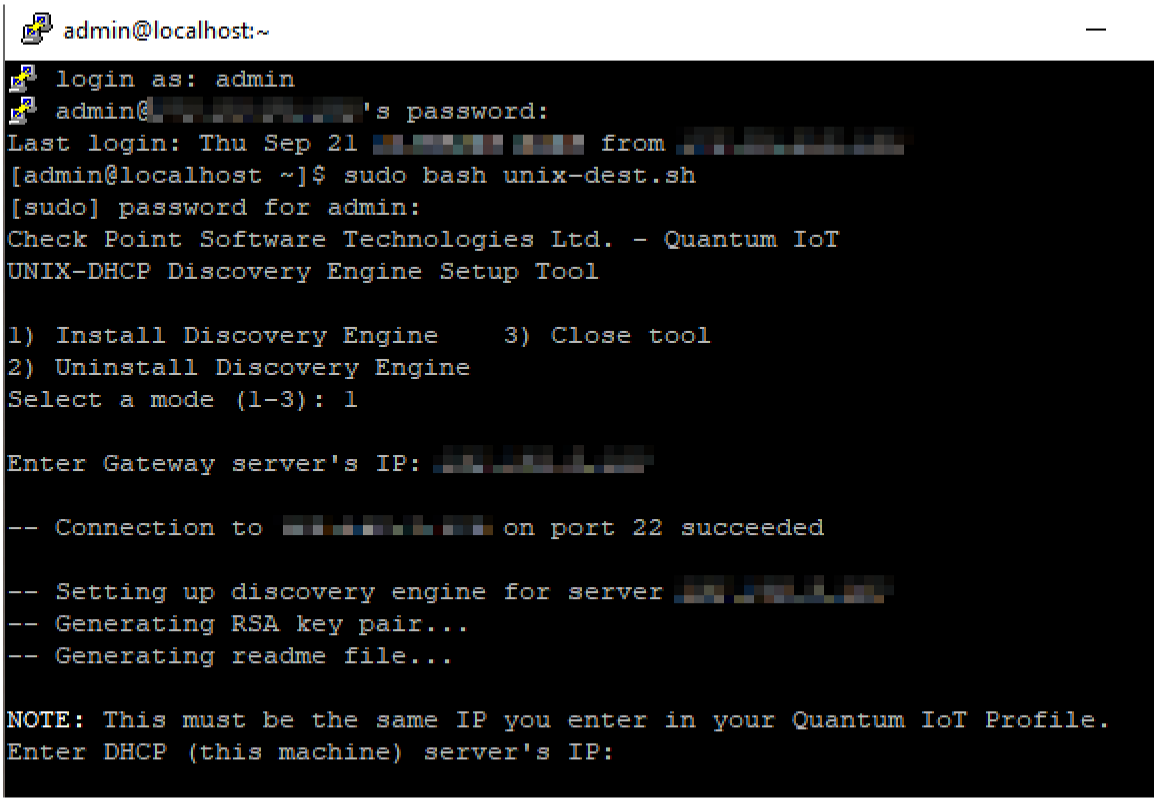
Output:



```
 login as: admin
 admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 1

Enter Gateway server's IP:
```

h. Enter the IP address of your Check Point Security Gateway server / Management Server, and press **Enter**.

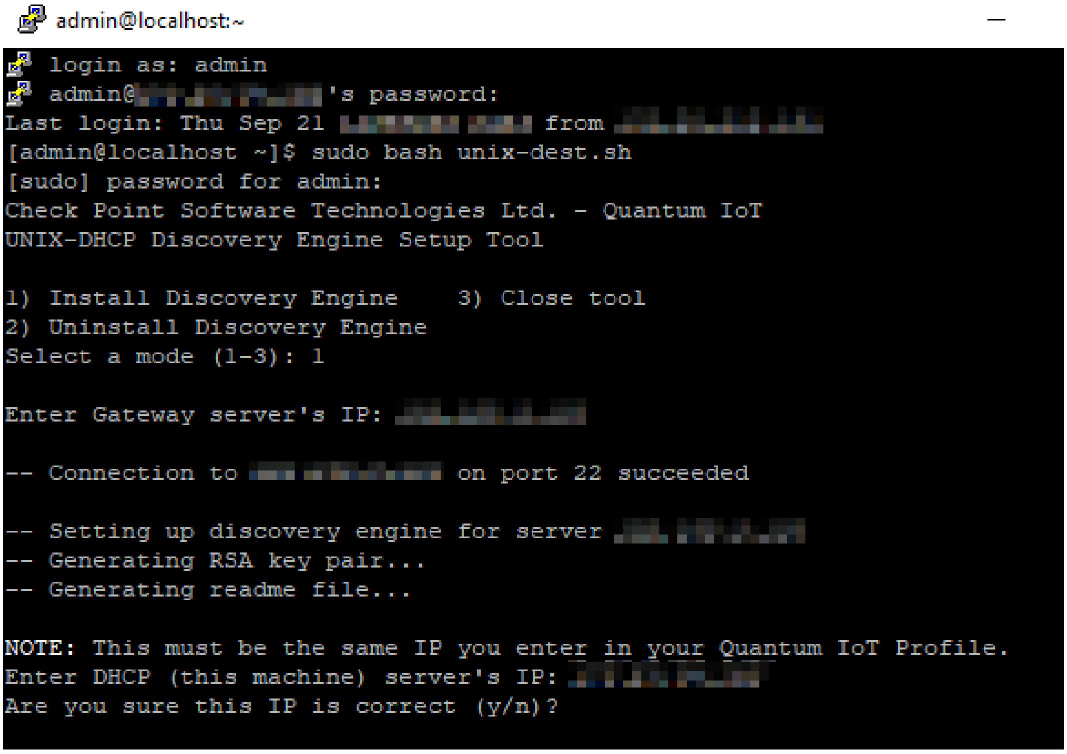
Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 1

Enter Gateway server's IP: [redacted]

-- Connection to [redacted] on port 22 succeeded

-- Setting up discovery engine for server [redacted]
-- Generating RSA key pair...
-- Generating readme file...

NOTE: This must be the same IP you enter in your Quantum IoT Profile.
Enter DHCP (this machine) server's IP:
```

i. Enter the IP address of the Unix DHCP server.

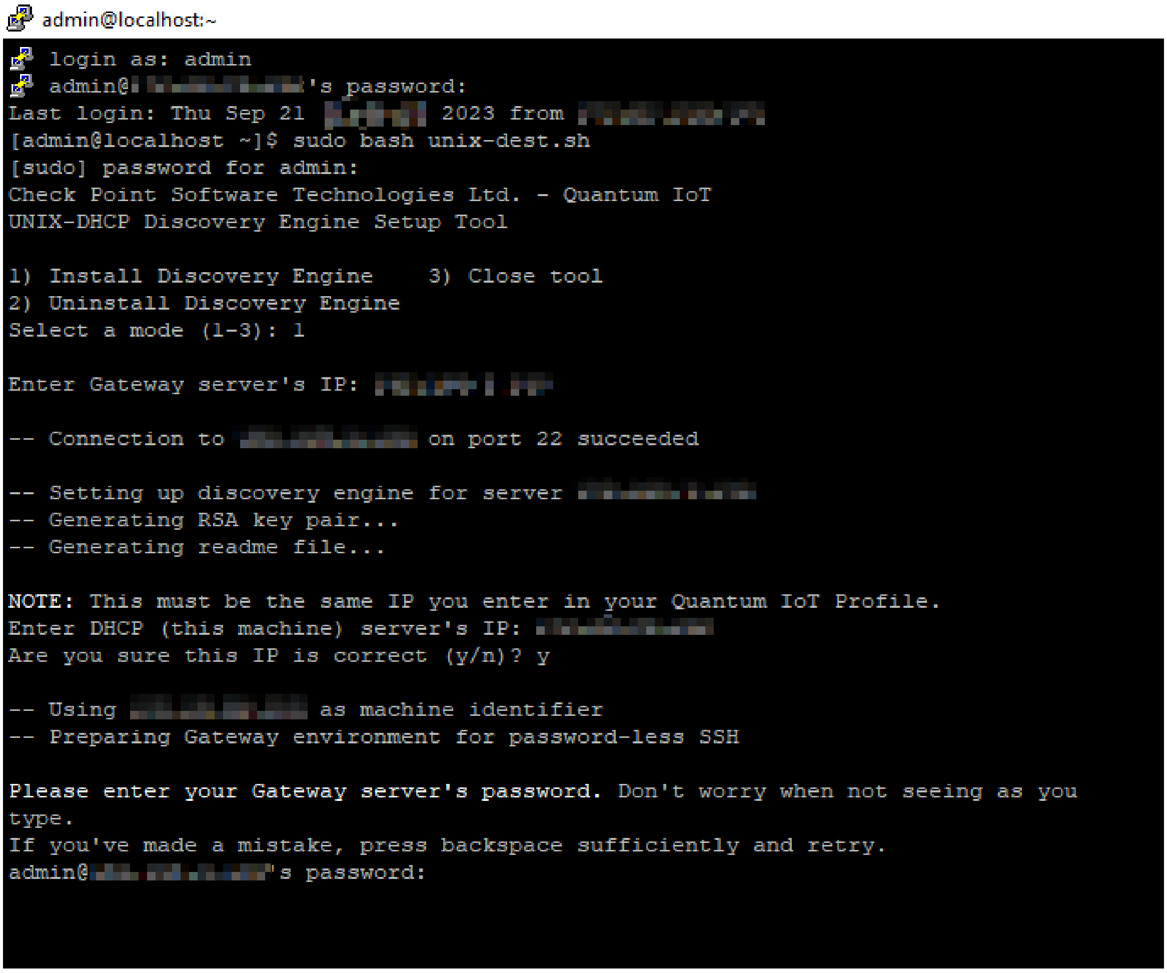
   Output:



```
 login as: admin
 admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine     3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 1

Enter Gateway server's IP: [redacted]

-- Connection to [redacted] on port 22 succeeded

-- Setting up discovery engine for server [redacted]
-- Generating RSA key pair...
-- Generating readme file...

NOTE: This must be the same IP you enter in your Quantum IoT Profile.
Enter DHCP (this machine) server's IP: [redacted]
Are you sure this IP is correct (y/n)?
```

j. Enter **y** and press **Enter**.

Output:



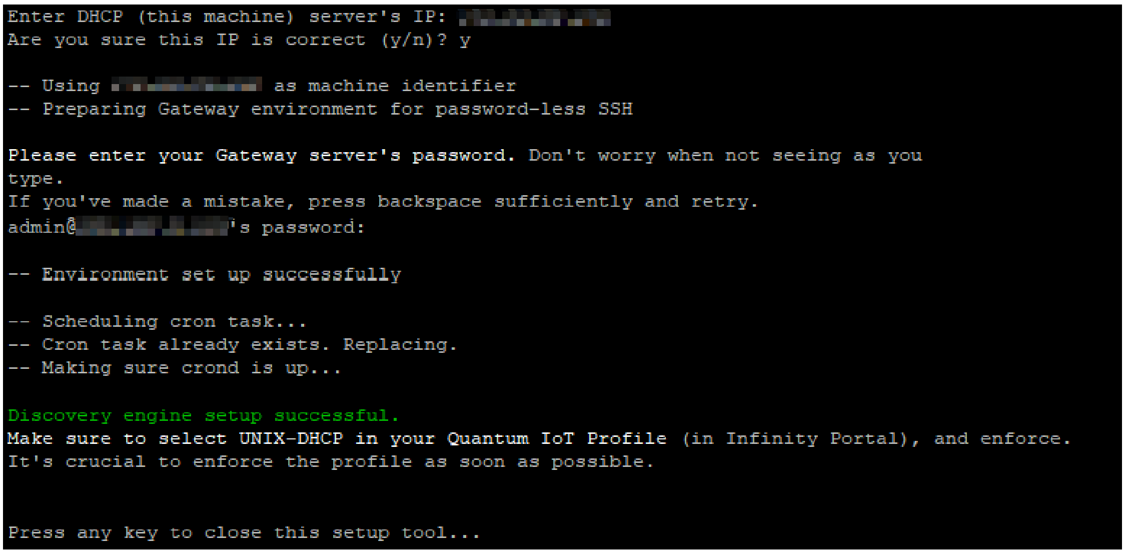
```
login as: admin
admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] 2023 from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 1

Enter Gateway server's IP: [redacted]

-- Connection to [redacted] on port 22 succeeded

-- Setting up discovery engine for server [redacted]
-- Generating RSA key pair...
-- Generating readme file...

NOTE: This must be the same IP you enter in your Quantum IoT Profile.
Enter DHCP (this machine) server's IP: [redacted]
Are you sure this IP is correct (y/n)? y

-- Using [redacted] as machine identifier
-- Preparing Gateway environment for password-less SSH

Please enter your Gateway server's password. Don't worry when not seeing as you
type.
If you've made a mistake, press backspace sufficiently and retry.
admin@[redacted]'s password:
```

Note - If this output appears, make sure that the Unix DHCP server is up and running, and enter the correct IP address.
Resolve the issue and repeat step i.

```
Connection could not be made to the server.
Make sure the Gateway server is up and configured, or try inputting the
correct IP address.
```

k. Enter the Expert mode password of your Check Point Security Gateway server / Management Server, and press **Enter**.

Output:



```
Enter DHCP (this machine) server's IP: [redacted]
Are you sure this IP is correct (y/n)? y

-- Using [redacted] as machine identifier
-- Preparing Gateway environment for password-less SSH

Please enter your Gateway server's password. Don't worry when not seeing as you
type.
If you've made a mistake, press backspace sufficiently and retry.
admin@[redacted]'s password:

-- Environment set up successfully

-- Scheduling cron task...
-- Cron task already exists. Replacing.
-- Making sure crond is up...

Discovery engine setup successful.
Make sure to select UNIX-DHCP in your Quantum IoT Profile (in Infinity Portal), and enforce.
It's crucial to enforce the profile as soon as possible.


Press any key to close this setup tool...
```

The discovery engine setup is complete.

l. To close the setup tool, press any key.

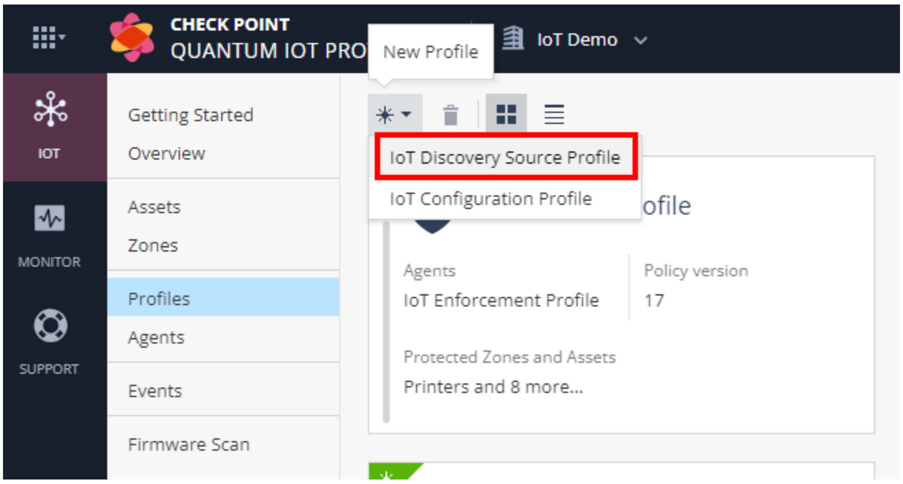
After the installation, the system copies the DHCP logs to your Security Gateway / Management Server at one-minute intervals.

2. Configure Unix-DHCP as the discovery engine in Quantum IoT Protect:

a. Log in to *Check Point Infinity Portal*.

b. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.

c. Click ✳ and select **IoT Discovery Source Profile**.



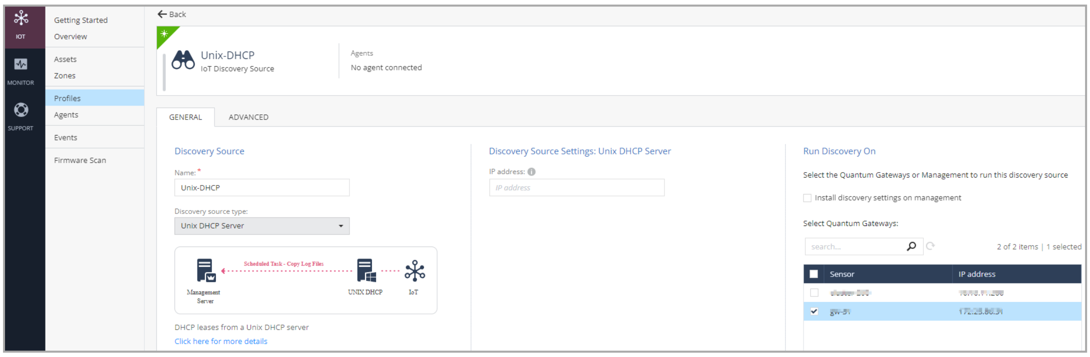
d. Enter these:

i. In the **Discovery Source** section, from the **Discovery source type** list, select **Unix DHCP Server**.

ii. In the **Discovery Source Settings** section, in the **IP address** field, enter the IP address of the Unix DHCP server.

iii. In the **Run Discovery On** section, select the Security Gateway from the list.

If you use a Standalone or Management Server, select **Install discovery settings on management**.



Unix-DHCP
IoT Discovery Source

Agents
No agent connected

Discovery Source

Name: *
Unix-DHCP

Discovery source type:
Unix DHCP Server

DHCP leases from a Unix DHCP server
Click here for more details

Discovery Source Settings: Unix DHCP Server

IP address:
IP address

Run Discovery On

Select the Quantum Gateways or Management to run this discovery source

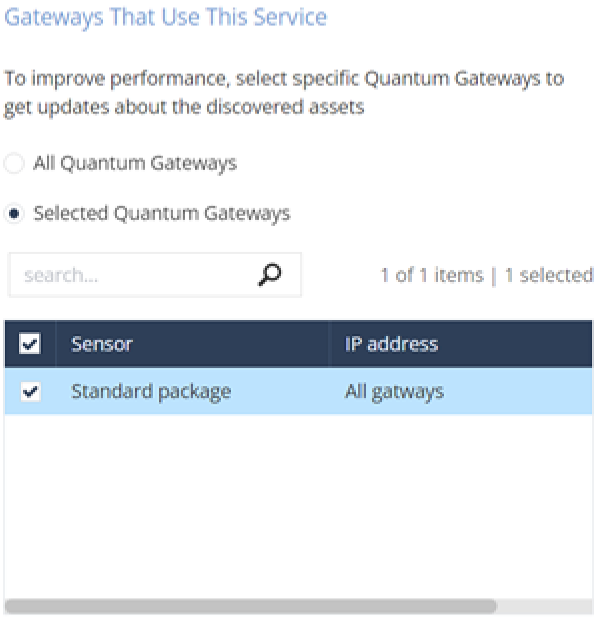
□ Install discovery settings on management

Select Quantum Gateways:

search...   2 of 2 items | 1 selected

■	Sensor	IP address
□	[redacted]	[redacted]
☑	[redacted]	[redacted]

iv. In the **Gateways That Use This Service** section, select the gateways relevant to your discovered assets, or select the policy-package for all gateways.



Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways

● Selected Quantum Gateways

search...   1 of 1 items | 1 selected

☑	Sensor	IP address
☑	Standard package	All gatways

e. Click **Enforce**.

The system installs the Unix-DHCP discovery engine and starts running on the Check Point Security Gateway / Management Server.

Testing the Unix DHCP IoT Discovery Engine

1. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console).

2. Log in to the Expert mode.

3. Run:

   ```
   cpnano -s
   ```

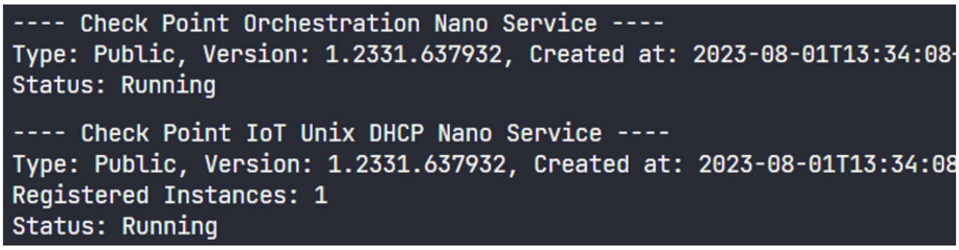
   Note - The output for this command may take time to appear depending on how long the system takes to enforce the profile. If you do not see the output, then verify whether you have selected the correct Security Gateway in the Profiles setting.

4. These nano services must be running:

   a. `Check Point Orchestration`

   b. `Check Point IoT Unix DHCP`

   Output:



```
---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2331.637932, Created at: 2023-08-01T13:34:08-
Status: Running

---- Check Point IoT Unix DHCP Nano Service ----
Type: Public, Version: 1.2331.637932, Created at: 2023-08-01T13:34:08
Registered Instances: 1
Status: Running
```

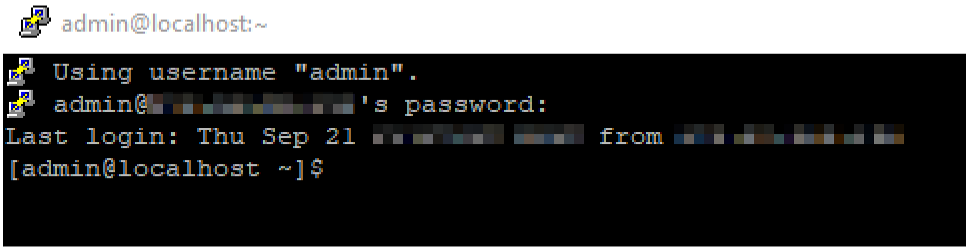
Removing Unix DHCP as the IoT Discovery Engine

To remove Unix DHCP as the IoT discovery engine from the Unix DHCP server:

1. Connect to the command line on your Unix DHCP server (over SSH or console).

2. Log in with administrator credentials.

   Output:

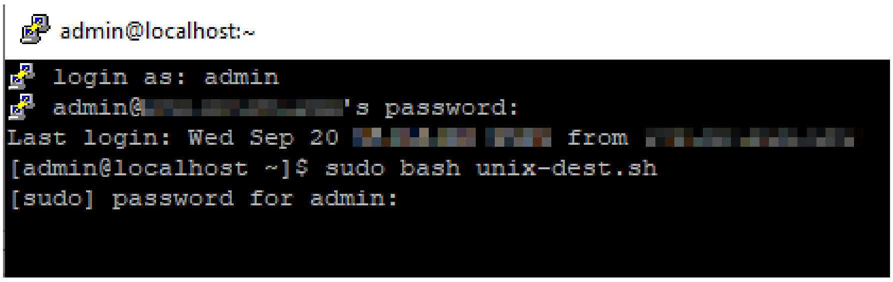


```
Using username "admin".
admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] from [redacted]
[admin@localhost ~]$
```

3. Run:

   ```
   sudo bash unix-dest.sh
   ```

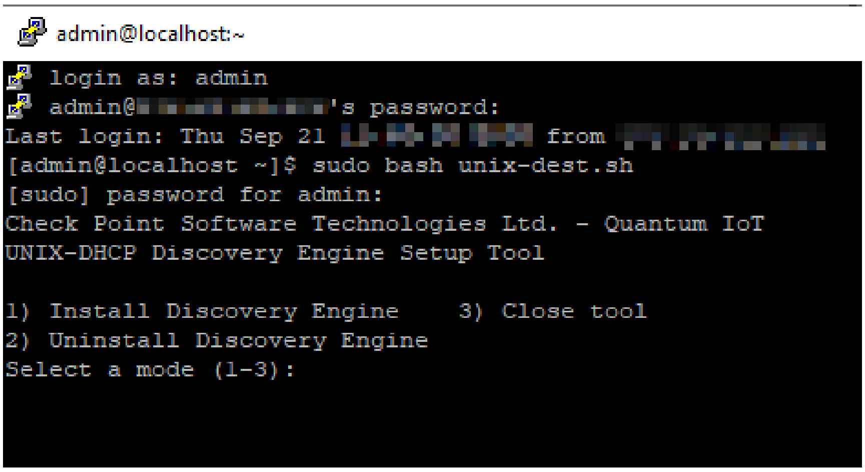
   Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Wed Sep 20 [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
```

4. Enter the administrator password.

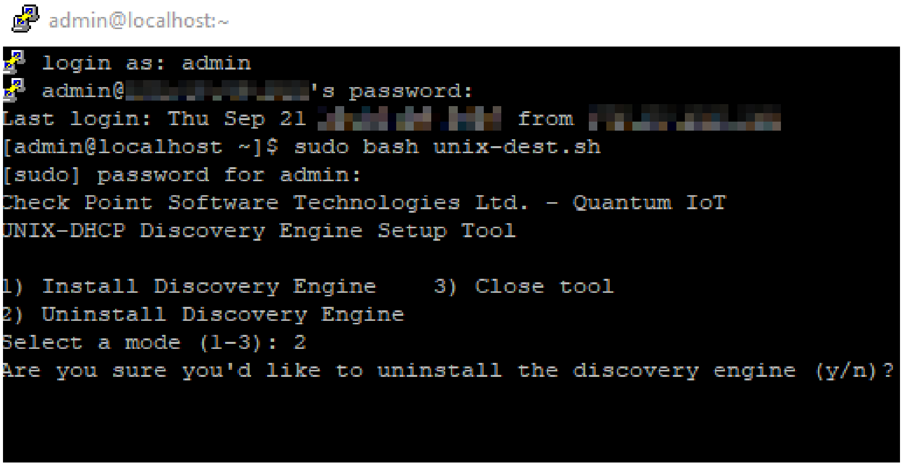
   Output:



```
login as: admin
admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3):
```

5. To uninstall the discovery engine, enter **2** and press **Enter**.

   Output:

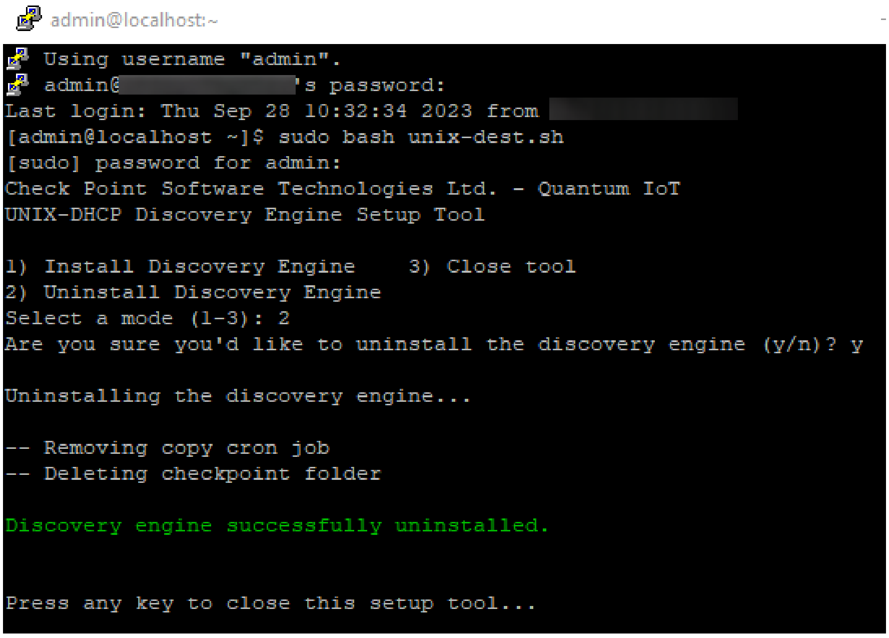


```
login as: admin
admin@[redacted]'s password:
Last login: Thu Sep 21 [redacted] from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 2
Are you sure you'd like to uninstall the discovery engine (y/n)?
```

6. To confirm, enter **y** and press **Enter**.

   The system removes the scheduled copy task and uninstalls the Unix DHCP server as the discovery engine.

   Output:



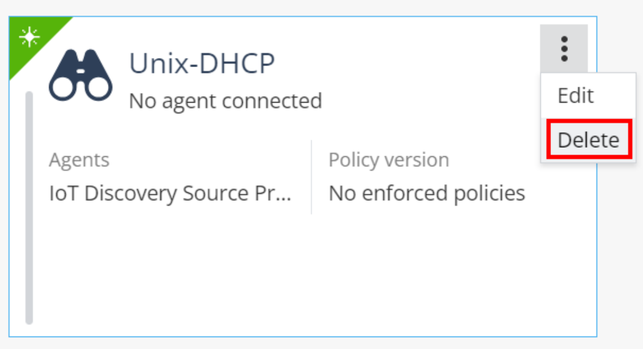
```
Using username "admin".
admin@[redacted]'s password:
Last login: Thu Sep 28 10:32:34 2023 from [redacted]
[admin@localhost ~]$ sudo bash unix-dest.sh
[sudo] password for admin:
Check Point Software Technologies Ltd. - Quantum IoT
UNIX-DHCP Discovery Engine Setup Tool

1) Install Discovery Engine    3) Close tool
2) Uninstall Discovery Engine
Select a mode (1-3): 2
Are you sure you'd like to uninstall the discovery engine (y/n)? y

Uninstalling the discovery engine...

-- Removing copy cron job
-- Deleting checkpoint folder

Discovery engine successfully uninstalled.


Press any key to close this setup tool...
```

7. To close the tool, press any key.

   DHCP logs are no longer copied to the Check Point Security Gateway / Management Server.

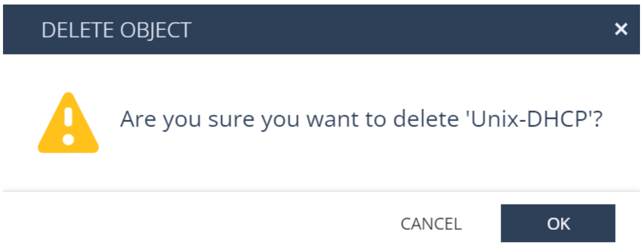
To remove the IoT Discovery Source Profile in Quantum IoT Protect:

1. Log in to *Check Point Infinity Portal*.
2. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.
3. On the **Unix-DHCP** discovery engine profile, click ⋮ and then **Delete**.



Unix-DHCP
No agent connected
Agents
IoT Discovery Source Pr...
Policy version
No enforced policies

4. Click **OK**.



DELETE OBJECT

Are you sure you want to delete 'Unix-DHCP'?

5. Click **Enforce**.

Troubleshooting the Unix DHCP IoT Discovery Engine

1. Connect to the command line on the Check Point Security Gateway / Management Server (over SSH or console).
2. Log in to the Expert mode.
3. The DHCP logs files are available in this location:

   /var/log/iot-discovery/unix-dhcp-logs

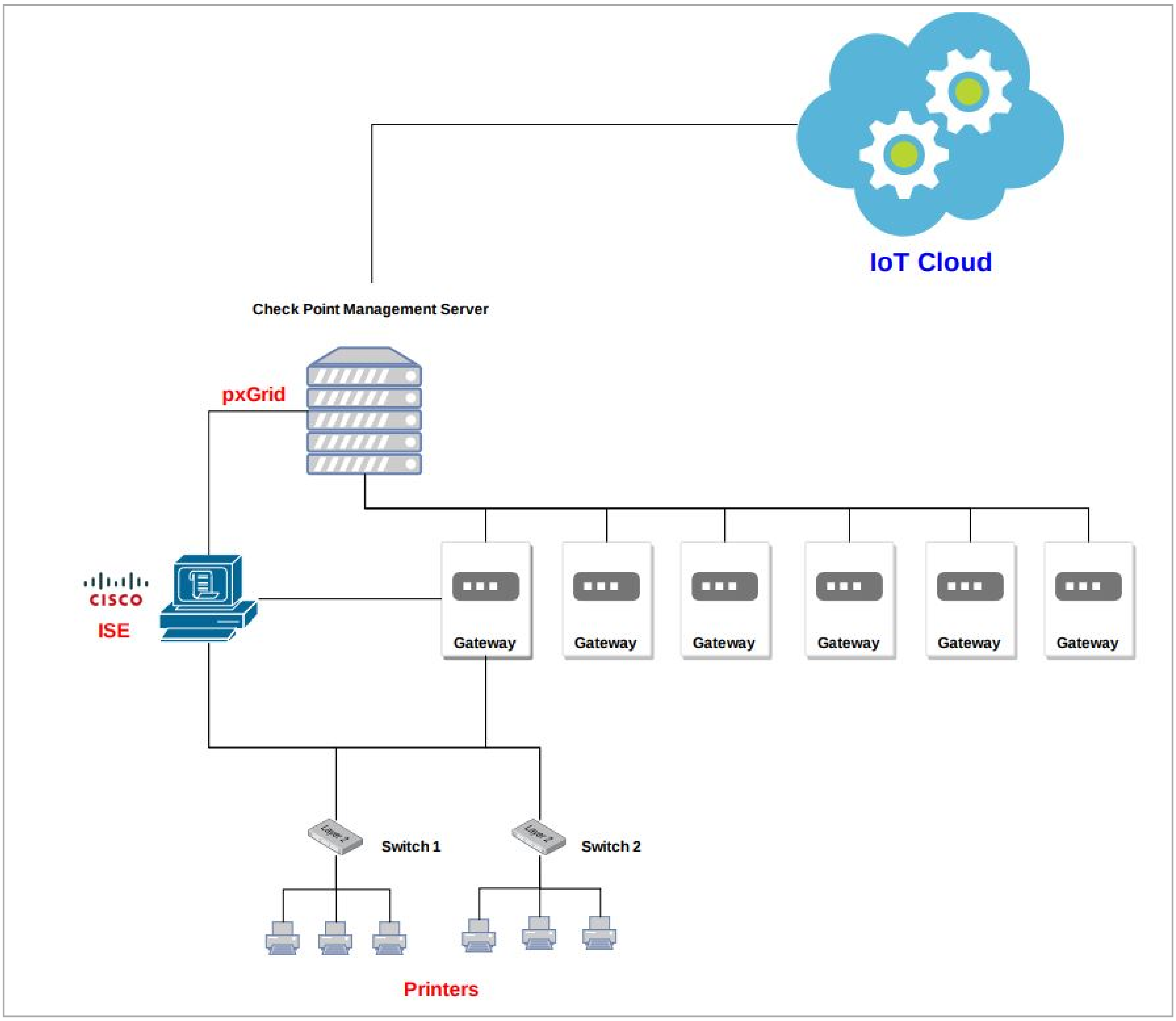
Appendix G - Using Cisco ISE as the IoT Discovery Engine

You can set up an IoT discovery engine on the Check Point Security Gateway or Management Server to discover IoT assets in your network. The IoT discovery engine uses the network devices in the network, such as switches, routers, gateways, or Network Access Control (NAC) devices to discover IoT assets.

You can use Cisco Identity Services Engine (ISE) as an IoT discovery engine. It is a NAC device that:

- Allows organizations to provide highly secure network access to users and devices.
- Uses a proprietary WebSocket-based protocol called Platform Exchange Grid (pxGrid) to share vital contextual data with integrated solutions. For pxGrid- related REST and WebSocket communication, pxGrid uses port 8910 over TCP on Cisco ISE.
- Subscribes to Cisco ISE's session events. With this subscription, IoT Protect is notified of any event in which a network device is authenticated by Cisco ISE. The notification includes the MAC address and IP address of the device.

This network diagram shows the setup to use Cisco ISE as the IoT discovery engine.



Note - Our integration with Cisco ISE is based on pxGrid - Platform Exchange Grid 2.0, which is officially supported starting from ISE 2.4. The procedures described in this appendix are tested on Cisco ISE versions 2.6 and 2.7.0.356, on a virtual machine.

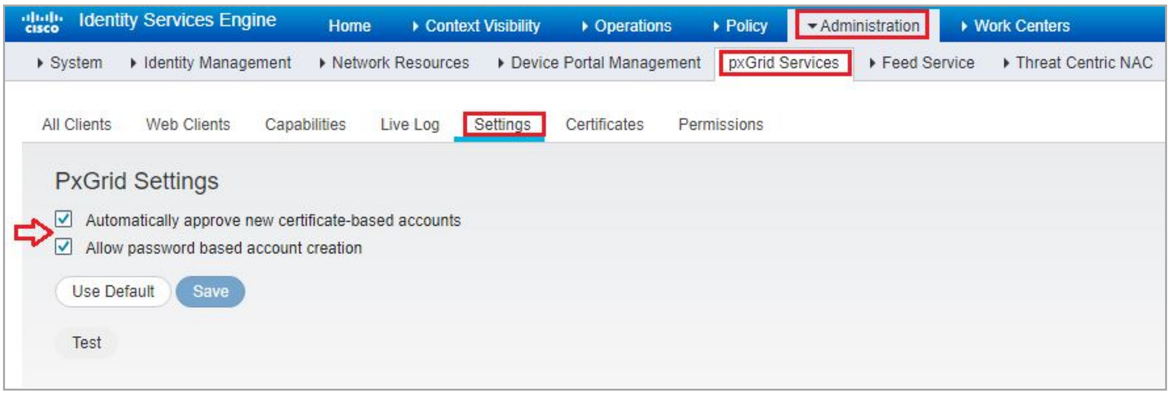
Prerequisites

1. Set the relevant rules in the Access Control policy to allow pxGrid traffic between the Check Point Management Server and the Cisco ISE server.

2. Configure pxGrid services on Cisco ISE:

a. Log in to Cisco ISE Web Management portal.

b. Go to **Administration** > **pxGrid Services** > **Settings**.



PxGrid Settings

☑ Automatically approve new certificate-based accounts

☑ Allow password based account creation

c. Select these checkboxes:

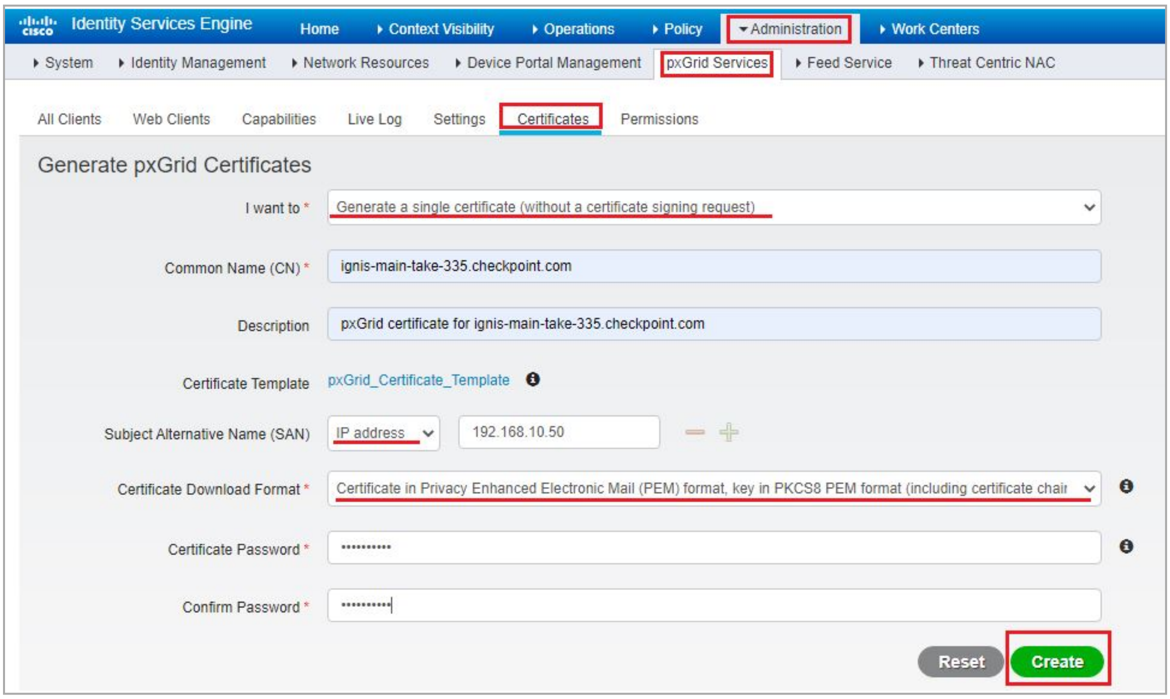
- **Automatically approve new certificate-based accounts**
- **Allow password based account creation**

d. Click **Save**.

Setting Up Cisco ISE as the IoT Discovery Engine

To set up Cisco ISE as the IoT Discovery Engine:

1. Issue pxGrid certificates:
   a. Log in to Cisco ISE Web Management portal.
   b. Go to **Administration** > **pxGrid Services** > **Certificates**.



Generate pxGrid Certificates

I want to * Generate a single certificate (without a certificate signing request)

Common Name (CN) * ignis-main-take-335.checkpoint.com

Description pxGrid certificate for ignis-main-take-335.checkpoint.com

Certificate Template pxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.10.50

Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chair

Certificate Password * ••••••••••

Confirm Password * ••••••••••

c. Enter these:

   i. **I want to** - Select **Generate a single certificate (without a certificate signing request)**.

   ii. **Common name (CN)** - FQDN [Host.Domain] of the pxGrid client, the subscriber of Cisco ISE server's sessions (the Management Server on which the integration is installed).

   iii. **Subject Alternative Name (SAN)** - Select **IP Address** and enter the IP Address of the pxGrid client, the subscriber of the Cisco ISE server's sessions (the Management Server on which the integration is installed).

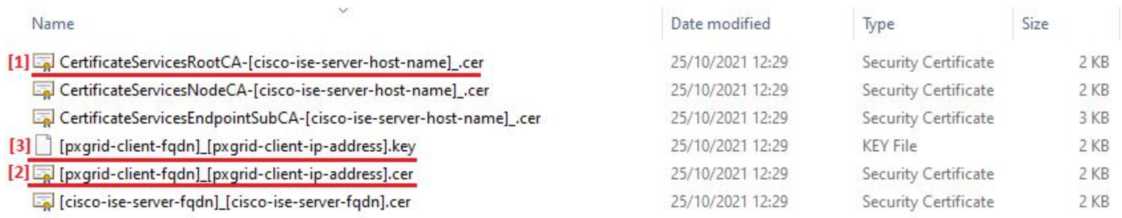
   iv. **Certificate Download Format** - Select **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**.

   v. **Certificate Password** - Enter the certificate password of the pxGrid client.

   vi. Click **Create**.

   The system creates a zip file of the certificates and downloads it to the path selected in the Windows Explorer dialog box.

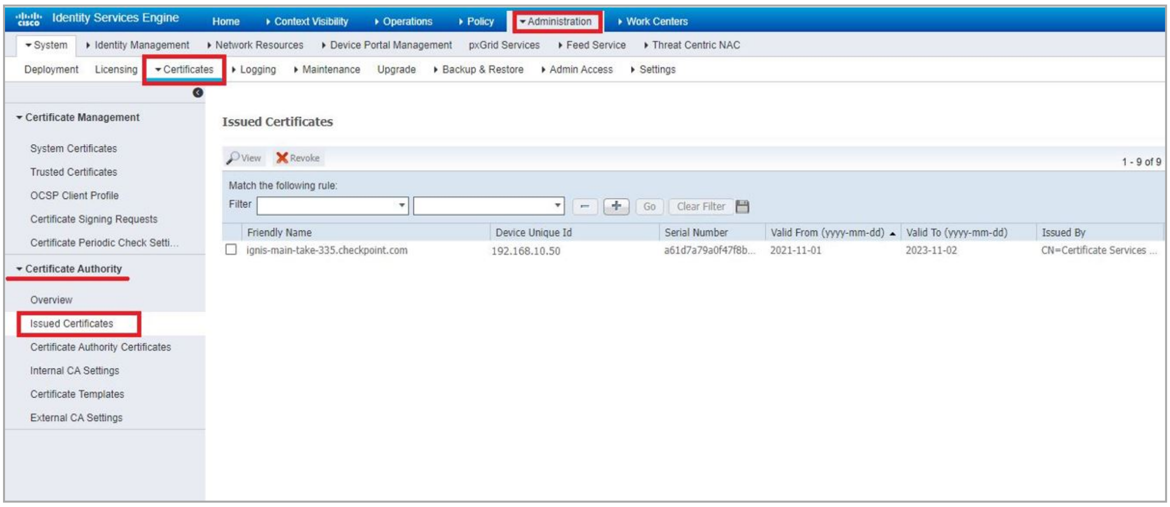
d. Extract the zip file and download the three certificate files.



	Name	Date modified	Type	Size
[1]	CertificateServicesRootCA-[cisco-ise-server-host-name]_.cer	25/10/2021 12:29	Security Certificate	2 KB
	CertificateServicesNodeCA-[cisco-ise-server-host-name]_.cer	25/10/2021 12:29	Security Certificate	2 KB
	CertificateServicesEndpointSubCA-[cisco-ise-server-host-name]_.cer	25/10/2021 12:29	Security Certificate	3 KB
[3]	[pxgrid-client-fqdn]_[pxgrid-client-ip-address].key	25/10/2021 12:29	KEY File	2 KB
[2]	[pxgrid-client-fqdn]_[pxgrid-client-ip-address].cer	25/10/2021 12:29	Security Certificate	2 KB
	[cisco-ise-server-fqdn]_[cisco-ise-server-fqdn].cer	25/10/2021 12:29	Security Certificate	2 KB

- [1] - pxGrid Server certificate - Root CA (Cisco ISE server)
- [2] - pxGrid Client certificate (Management Server)
- [3] - pxGrid Client Key (Management Server)

e. To view the certificates issued by the Cisco ISE server, go to **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**.



Issued Certificates

1 - 9 of 9

Match the following rule:

Filter

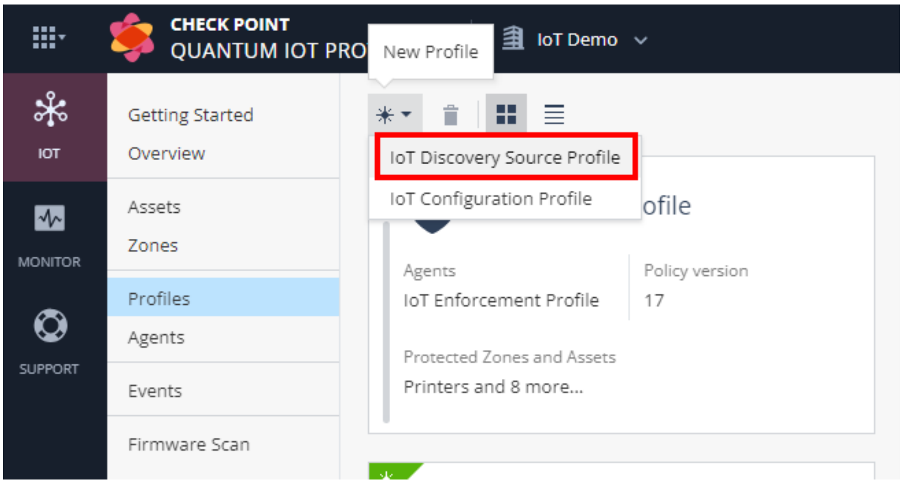
	Friendly Name	Device Unique Id	Serial Number	Valid From (yyyy-mm-dd)	Valid To (yyyy-mm-dd)	Issued By
☐	ignis-main-take-335.checkpoint.com	192.168.10.50	a61d7a79a0f47f8b...	2021-11-01	2023-11-02	CN=Certificate Services ...

2. Set Cisco ISE as the discovery engine in Quantum IoT Protect:

a. Log in to *Check Point Infinity Portal*.

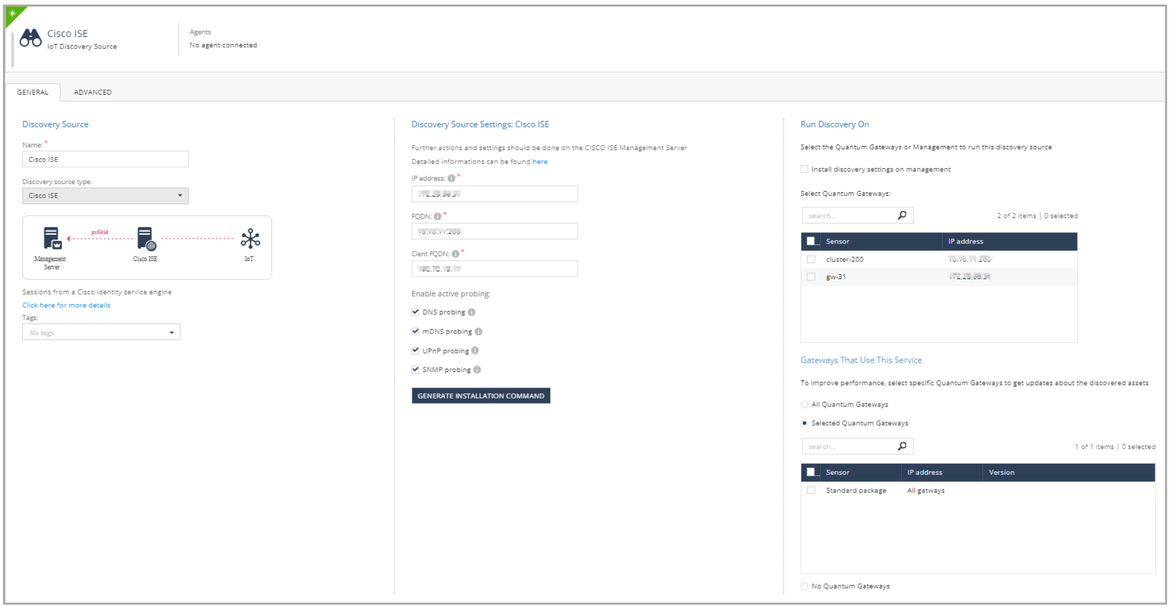
b. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.

c. Click ✳ and select **IoT Discovery Source Profile**.



d. In the **Discovery Source** section, from the **Discovery source type** list, select **Cisco ISE**.

e. In the **Discovery Source Settings** section:



Cisco ISE
IoT Discovery Source

Agents
No agent connected

GENERAL | ADVANCED

Discovery Source

Name: *
Cisco ISE

Discovery source type:
Cisco ISE

Sessions from a Cisco identity service engine

Click here for more details

Tags:
No tags

Discovery Source Settings: Cisco ISE

Further actions and settings should be done on the CISCO ISE Management Server

Detailed informations can be found here

IP address: *
[redacted]

FQDN: *
[redacted]

Cient FQDN: *
[redacted]

Enable active probing:

☑ DNS probing

☑ mDNS probing

☑ UPnP probing

☑ SNMP probing

GENERATE INSTALLATION COMMAND

Run Discovery On

Select the Quantum Gateways or Management to run this discovery source

□ Install discovery settings on management

Select Quantum Gateways:

search... 2 of 2 items | 0 selected

□	Sensor	IP address
□	cluster-200	[redacted]
□	gw-31	[redacted]

Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways

● Selected Quantum Gateways

search... 1 of 1 items | 0 selected

□	Sensor	IP address	Version
□	Standard package	All gatways	

○ No Quantum Gateways

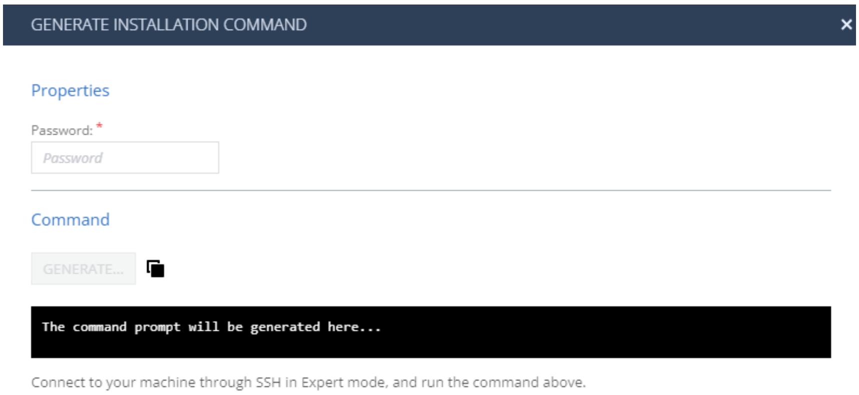
i. In the **IP address** field, enter the IP address of the Cisco ISE Server.

ii. In the **FQDN** field, enter the Full Qualified Domain (FQDN) of the Cisco ISE Server.

iii. In the **Client FQDN** field, enter the FQDN of the client connected to the Cisco ISE Server.

f. Click **Generate Installation Command**.

The **Generate Installation Command** window appears.



GENERATE INSTALLATION COMMAND ✕

Properties

Password: *
Password

Command

GENERATE...

```
The command prompt will be generated here...
```

Connect to your machine through SSH in Expert mode, and run the command above.

g. In the **Properties** section, enter the pxGrid client certificate password.

Note - Cisco ISE discovery engine uses pxGrid certificates issued by the Cisco ISE server. See Issue pxGrid certificates in Prerequisites.

h. In the **Command** section, click **Generate**.

   The system generates the command to configure the Cisco ISE discovery engine on the Check Point Security Gateway / Management Server.

i. Copy the generated command.

j. Access your Check Point Security Gateway / Management Server through SSH, for example using PuTTY.

k. Log in to Expert mode.

l. Paste the generated command.

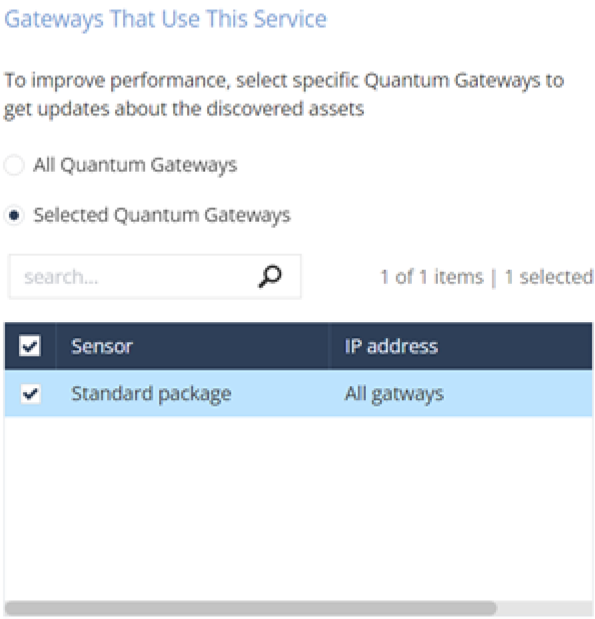
m. If the integration is installed on a cluster gateway or Management Server with High Availability (HA) or Multi-Domain Server (MDS) with HA:

   i. Access each member through SSH and log in to Expert mode.

   ii. Paste the generated command.

n. In the **Run Discovery On** section, select the Management Server on which the integration should be installed.

o. In the **Gateways That Use This Service** section, select the gateways relevant to your discovered assets, or select the policy-package for all gateways.



Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways

● Selected Quantum Gateways

1 of 1 items | 1 selected

☑	Sensor	IP address
✓	Standard package	All gatways

p. Click **Enforce**.

3. Copy the pxGrid certificates to your Check Point Security Gateway / Management Server:

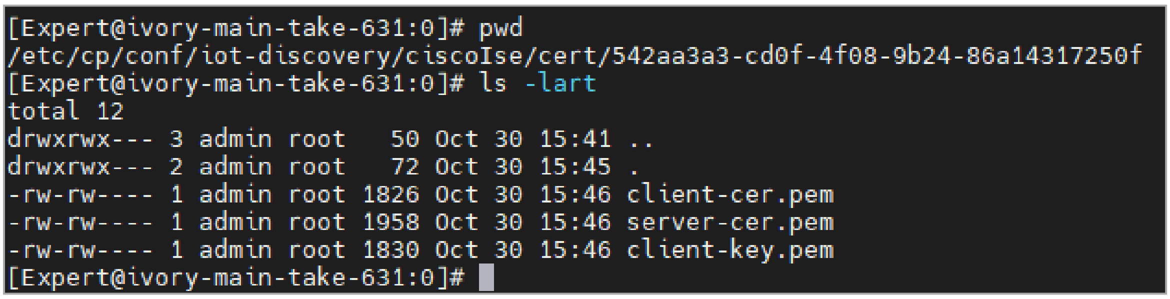
a. Before you copy, rename the pxGrid certificate file names as per the table below.

File Type	File Name
pxGrid server certificate (Cisco ISE)	*server-cer.pem*
pxGrid client certificate (Management Server)	*client-cer.pem*
pxGrid client key (Management Server)	*client-key.pem*

b. Use a file transfer application, such as WinSCP to copy the pxGrid certificate files to your Check Point Security Gateway / Management Server:

Copy the pxGrid certificates to the following path:

```
/etc/cp/conf/iot-discovery/ciscoIse/cert/${cisco_ise_
integration_id}
```



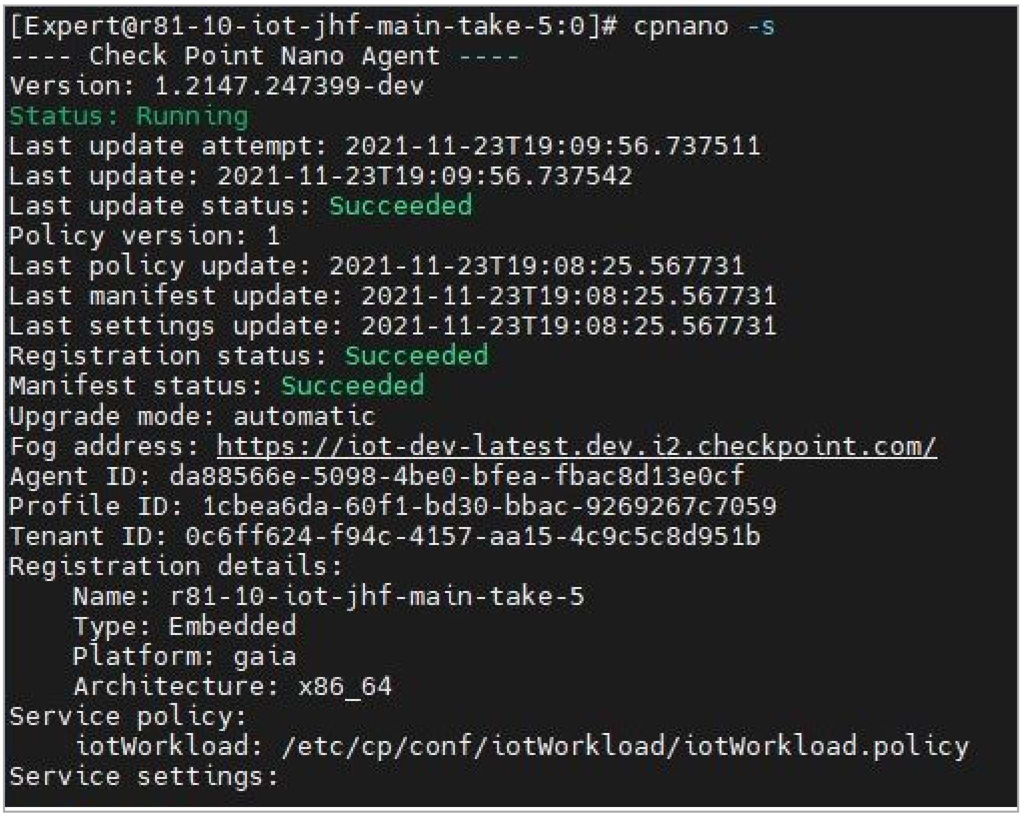
```
[Expert@ivory-main-take-631:0]# pwd
/etc/cp/conf/iot-discovery/ciscoIse/cert/542aa3a3-cd0f-4f08-9b24-86a14317250f
[Expert@ivory-main-take-631:0]# ls -lart
total 12
drwxrwx--- 3 admin root   50 Oct 30 15:41 ..
drwxrwx--- 2 admin root   72 Oct 30 15:45 .
-rw-rw---- 1 admin root 1826 Oct 30 15:46 client-cer.pem
-rw-rw---- 1 admin root 1958 Oct 30 15:46 server-cer.pem
-rw-rw---- 1 admin root 1830 Oct 30 15:46 client-key.pem
[Expert@ivory-main-take-631:0]#
```

Testing the Cisco ISE IoT Discovery Engine

1. Access the Check Point Security Gateway / Management Server through SSH and run:

   ```
   cpnano -s
   ```

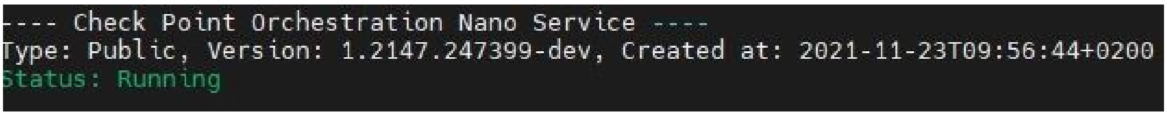
   Sample output:



```
[Expert@r81-10-iot-jhf-main-take-5:0]# cpnano -s
---- Check Point Nano Agent ----
Version: 1.2147.247399-dev
Status: Running
Last update attempt: 2021-11-23T19:09:56.737511
Last update: 2021-11-23T19:09:56.737542
Last update status: Succeeded
Policy version: 1
Last policy update: 2021-11-23T19:08:25.567731
Last manifest update: 2021-11-23T19:08:25.567731
Last settings update: 2021-11-23T19:08:25.567731
Registration status: Succeeded
Manifest status: Succeeded
Upgrade mode: automatic
Fog address: https://iot-dev-latest.dev.i2.checkpoint.com/
Agent ID: da88566e-5098-4be0-bfea-fbac8d13e0cf
Profile ID: 1cbea6da-60f1-bd30-bbac-9269267c7059
Tenant ID: 0c6ff624-f94c-4157-aa15-4c9c5c8d951b
Registration details:
    Name: r81-10-iot-jhf-main-take-5
    Type: Embedded
    Platform: gaia
    Architecture: x86_64
Service policy:
    iotWorkload: /etc/cp/conf/iotWorkload/iotWorkload.policy
Service settings:
```

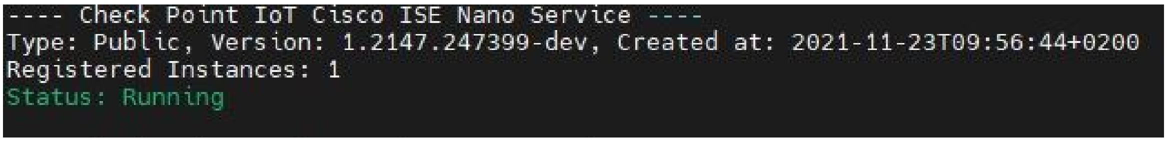
2. Make sure these nano services are running:

   a. Check Point Orchestration



```
---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2147.247399-dev, Created at: 2021-11-23T09:56:44+0200
Status: Running
```

   b. Check Point IoT Cisco ISE



```
---- Check Point IoT Cisco ISE Nano Service ----
Type: Public, Version: 1.2147.247399-dev, Created at: 2021-11-23T09:56:44+0200
Registered Instances: 1
Status: Running
```

Troubleshooting the Cisco ISE IoT Discovery Engine

1. Access the Check Point Security Gateway / Management Server through SSH.
2. To ensure that the network and access rules have enabled pxGrid traffic between the Security Gateway / Management Server(pxGrid client) and Cisco ISE (pxGrid) server, run:

- `ping <Cisco ISE's IP Address>`
- `ping <Cisco ISE's FQDN>`
- `telnet <Cisco ISE's FQDN> 8910`

3. Make sure that the certificate files are copied and named correctly:

File Type	File Name
pxGrid server certificate (Cisco ISE)	*server-cer.pem*
pxGrid client certificate (Management Server)	*client-cer.pem*
pxGrid client key (Management Server)	*client-key.pem*

4. If the certificate files are not copied, repeat these procedures:
   a. Create pxGrid certificate files in Cisco ISE. See *"Issue pxGrid certificates:" on page 146*.
   b. Copy pxGrid certificate files to the Management server. See *"Copy the pxGrid certificates to your Check Point Security Gateway / Management Server:" on page 150*.
5. Check whether the log file exists:

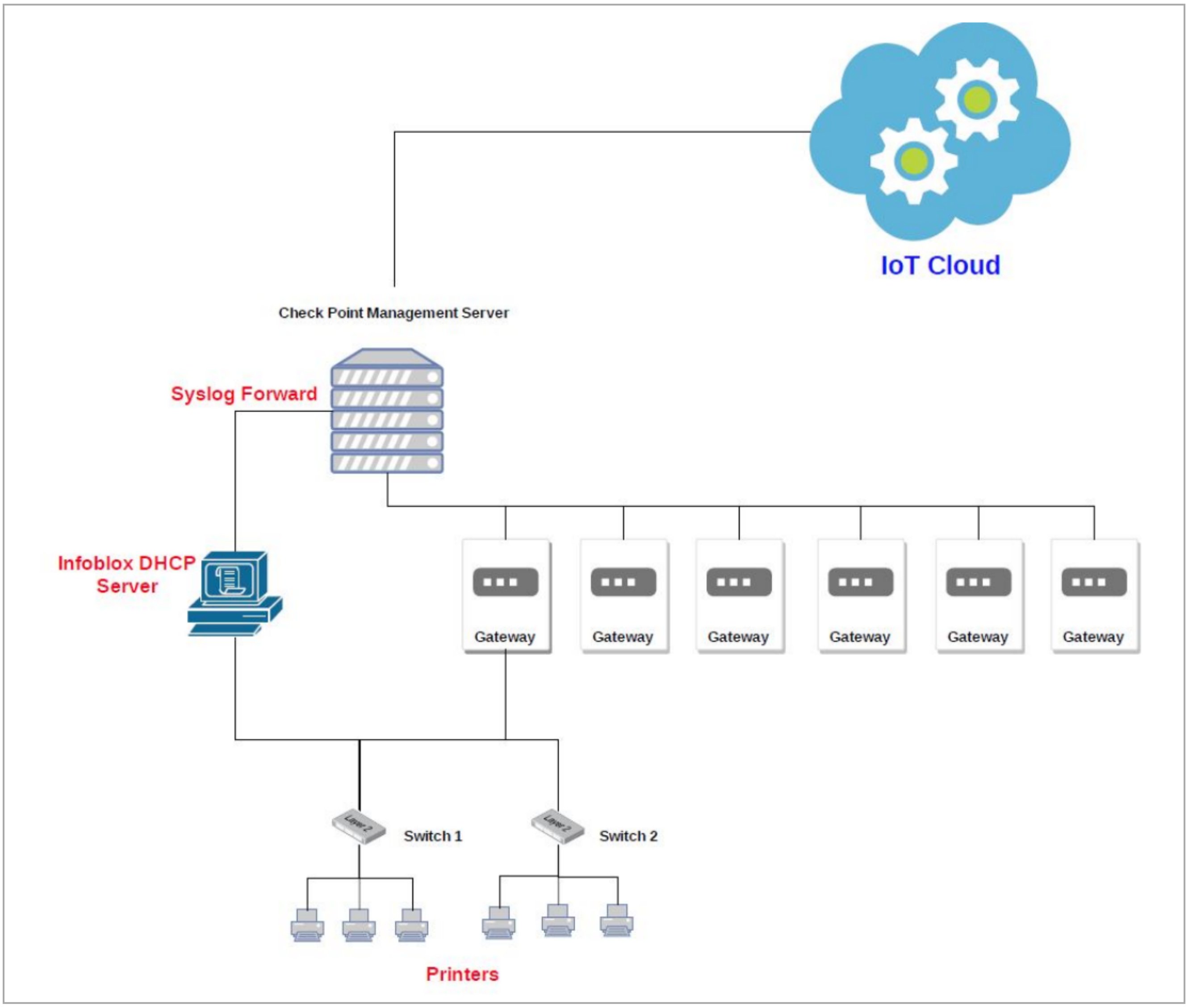
```
/etc/cp/scripts/iot/ciscoIse/cisco_ise.log
```

Appendix H - Using Infoblox DHCP - Syslog as the IoT Discovery Engine

You can set up an IoT discovery engine on the Check Point Management Server to discover IoT assets in your network. The IoT discovery engine uses the network devices in the network, such as switches, routers, gateways, or Network Access Control (NAC) devices to discover IoT assets.

You can use the Infoblox DHCP server as an IoT discovery engine. It maintains a pool of IP addresses and leases an IP address to every new DHCP-enabled client.

Infoblox DHCP - Syslog integration is based on Syslog messages generated by Infoblox DHCP server. Such Syslog message includes the MAC address of the device and the leased IP address. Syslog uses port 514 to send log messages over TCP or UDP.



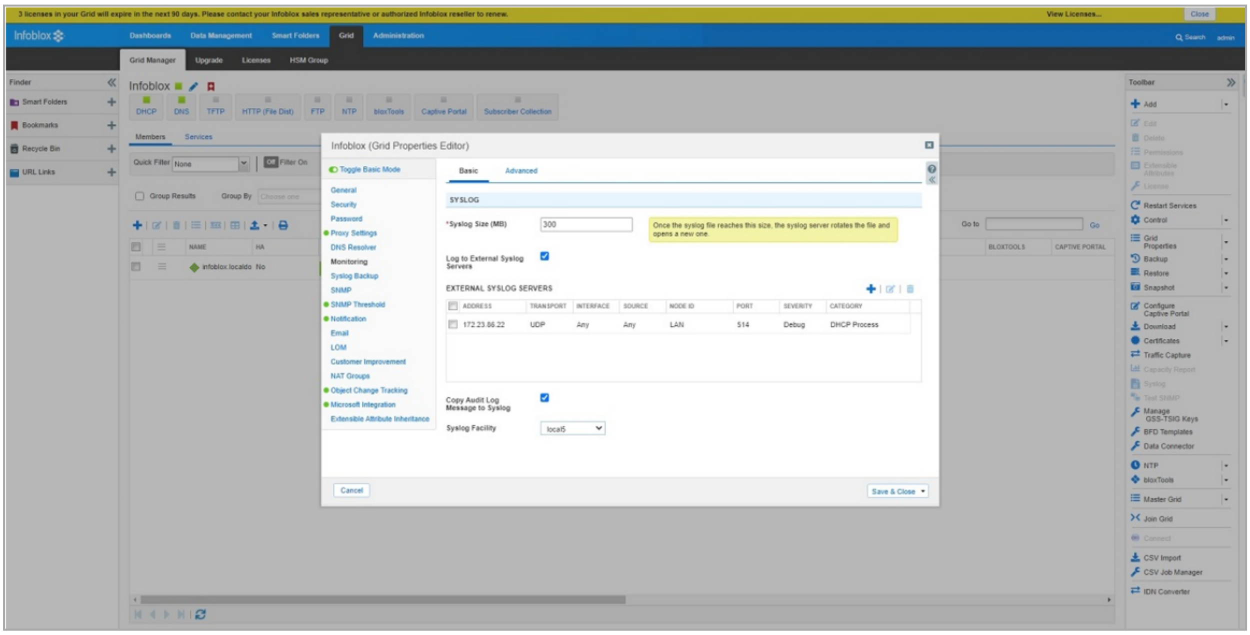
Prerequisites

1. Add the Check Point Management Server on which the integration is installed as an external log server.

   a. Log in to **Infoblox**.

   b. Go to **Grid** > **Grid Manager** > **Members**.

   c. Go to **Grid Properties** > **Monitoring** > **Basic**.



Infoblox (Grid Properties Editor)

SYSLOG

*Syslog Size (MB): 300

Once the syslog file reaches this size, the syslog server rotates the file and opens a new one.

Log to External Syslog Servers: ☑

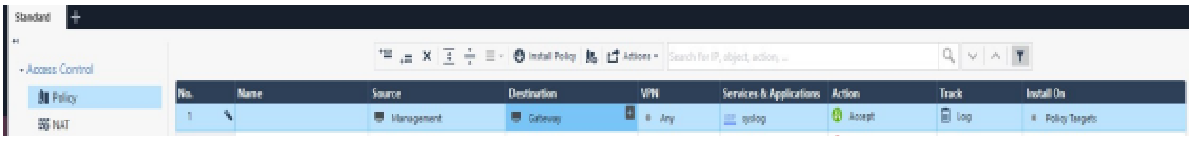
EXTERNAL SYSLOG SERVERS

ADDRESS	TRANSPORT	INTERFACE	SOURCE	NODE ID	PORT	SEVERITY	CATEGORY
172.23.86.22	UDP	Any	Any	LAN	514	Debug	DHCP Process

Copy Audit Log Message to Syslog: ☑

Syslog Facility: local5

2. Set the relevant Access Control rules on the relevant gateway, to allow Syslog traffic between the Infoblox DHCP server and the Check Point Management Server.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Management	Gateway	Any	syslog	Accept	Log	Policy Targets

Setting Up Infoblox DHCP - Syslog as the IoT Discovery Engine

To set up Infoblox DHCP - Syslog as the IoT Discovery Engine:

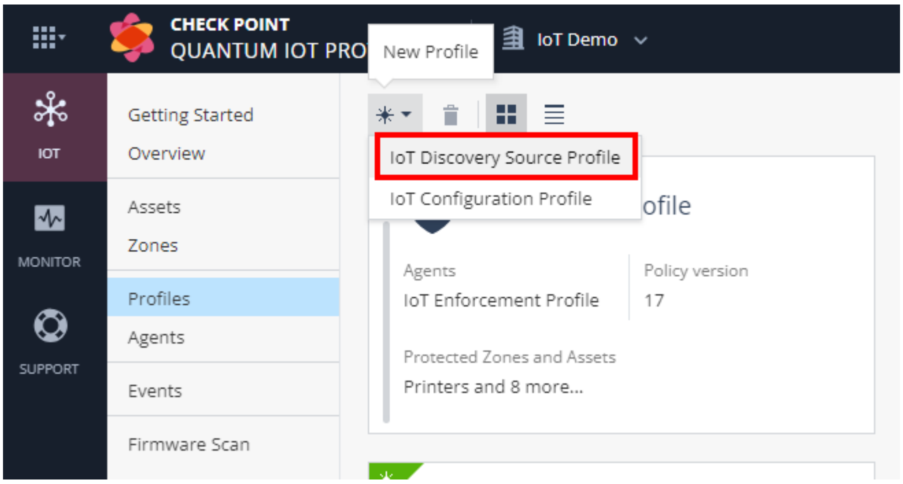
1. Enable Infoblox DHCP - Syslog as the IoT discovery engine in Quantum IoT Protect.

   Notes:
   - When you install the Infoblox DHCP - Syslog built-in discovery engine, it modifies the configuration of the Check Point Management Server on which it is installed and enables it to receive Syslog messages.
   - Make sure no other user is logged in to **SmartConsole**.

   a. Log in to the *Check Point Infinity Portal*.

   b. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.

   c. Click ✳ and select **IoT Discovery Source Profile**.

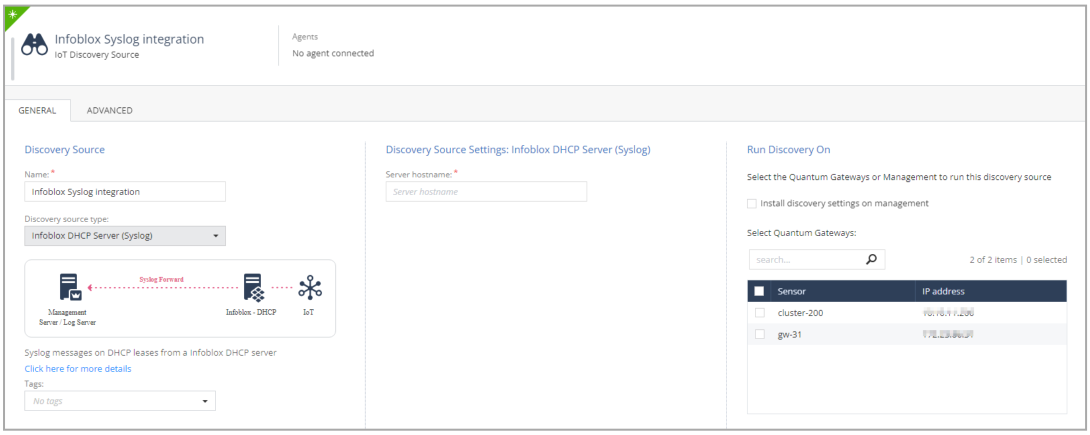


d. Enter these:

   i. In the **Discovery Source** section, from the **Discovery source type** list, select **Infoblox DHCP Server (Syslog)**.

   ii. In the **Discovery Source Settings** section, in the **Server hostname** field, enter the hostname of the Infoblox DHCP server.

   iii. In the **Run Discovery On** section, select your Check Point Management Server.



Infoblox Syslog integration
IoT Discovery Source

Agents
No agent connected

GENERAL | ADVANCED

Discovery Source

Name: *
Infoblox Syslog integration

Discovery source type:
Infoblox DHCP Server (Syslog)

Syslog messages on DHCP leases from a Infoblox DHCP server
Click here for more details

Tags:
No tags

Discovery Source Settings: Infoblox DHCP Server (Syslog)

Server hostname: *
Server hostname

Run Discovery On

Select the Quantum Gateways or Management to run this discovery source

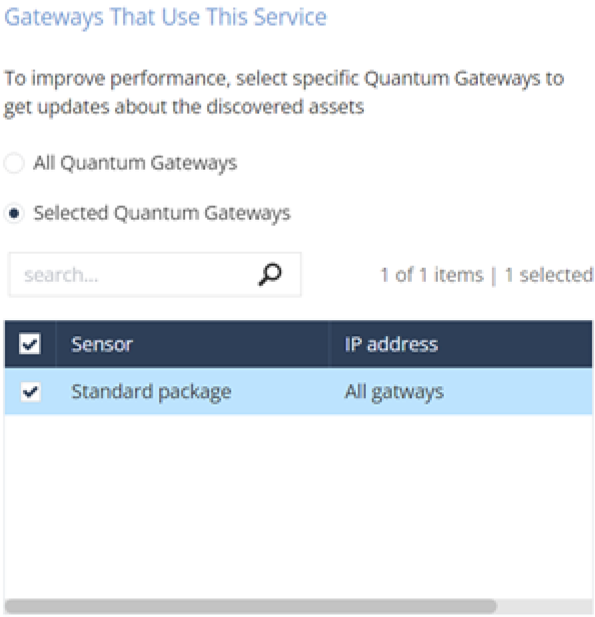
□ Install discovery settings on management

Select Quantum Gateways:

search... 2 of 2 items | 0 selected

□	Sensor	IP address
□	cluster-200	[redacted]
□	gw-31	[redacted]

   iv. In the **Gateways That Use This Service** section, select the gateways relevant to your discovered assets, or select the policy-package for all gateways.



Gateways That Use This Service

To improve performance, select specific Quantum Gateways to get updates about the discovered assets

○ All Quantum Gateways

● Selected Quantum Gateways

search... 1 of 1 items | 1 selected

☑	Sensor	IP address
☑	Standard package	All gatways

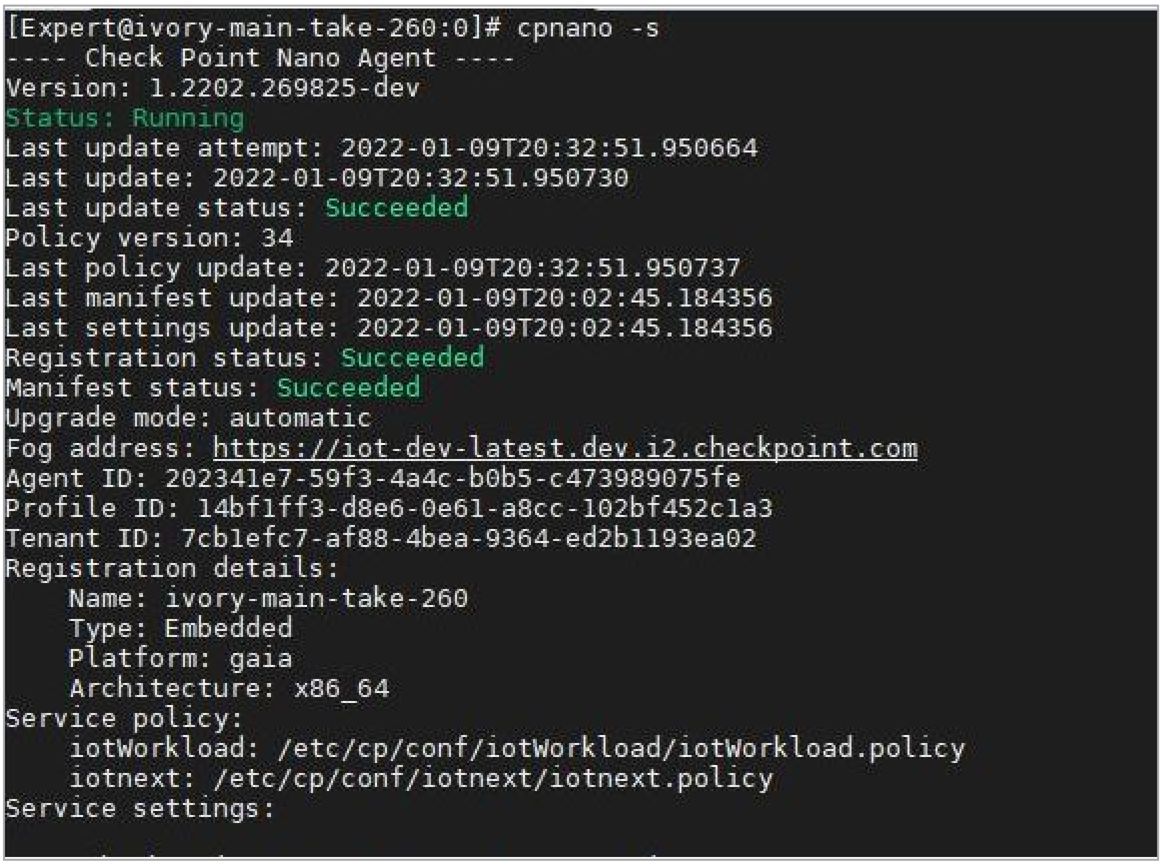
e. Click **Enforce**.

   The system installs the Infoblox DHCP - Syslog discovery engine and starts running on the Check Point Management Server.

Testing the Infoblox DHCP - Syslog IoT Discovery Engine

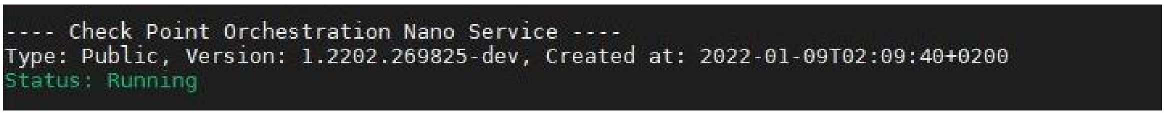
1. Access the Check Point Management Server through SSH, for example using PuTTY.
2. Run:

   ```
   cpnano -s
   ```



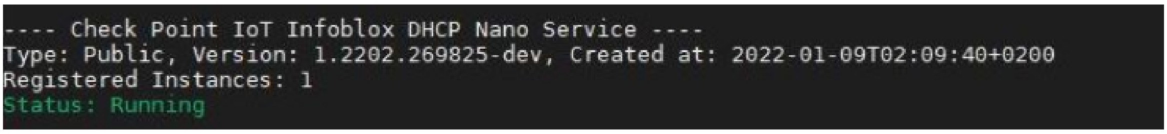
```
[Expert@ivory-main-take-260:0]# cpnano -s
---- Check Point Nano Agent ----
Version: 1.2202.269825-dev
Status: Running
Last update attempt: 2022-01-09T20:32:51.950664
Last update: 2022-01-09T20:32:51.950730
Last update status: Succeeded
Policy version: 34
Last policy update: 2022-01-09T20:32:51.950737
Last manifest update: 2022-01-09T20:02:45.184356
Last settings update: 2022-01-09T20:02:45.184356
Registration status: Succeeded
Manifest status: Succeeded
Upgrade mode: automatic
Fog address: https://iot-dev-latest.dev.i2.checkpoint.com
Agent ID: 202341e7-59f3-4a4c-b0b5-c473989075fe
Profile ID: 14bf1ff3-d8e6-0e61-a8cc-102bf452c1a3
Tenant ID: 7cb1efc7-af88-4bea-9364-ed2b1193ea02
Registration details:
    Name: ivory-main-take-260
    Type: Embedded
    Platform: gaia
    Architecture: x86_64
Service policy:
    iotWorkload: /etc/cp/conf/iotWorkload/iotWorkload.policy
    iotnext: /etc/cp/conf/iotnext/iotnext.policy
Service settings:
```

3. Make sure that these nano services are running:
   a. Check Point Orchestration



```
---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2202.269825-dev, Created at: 2022-01-09T02:09:40+0200
Status: Running
```

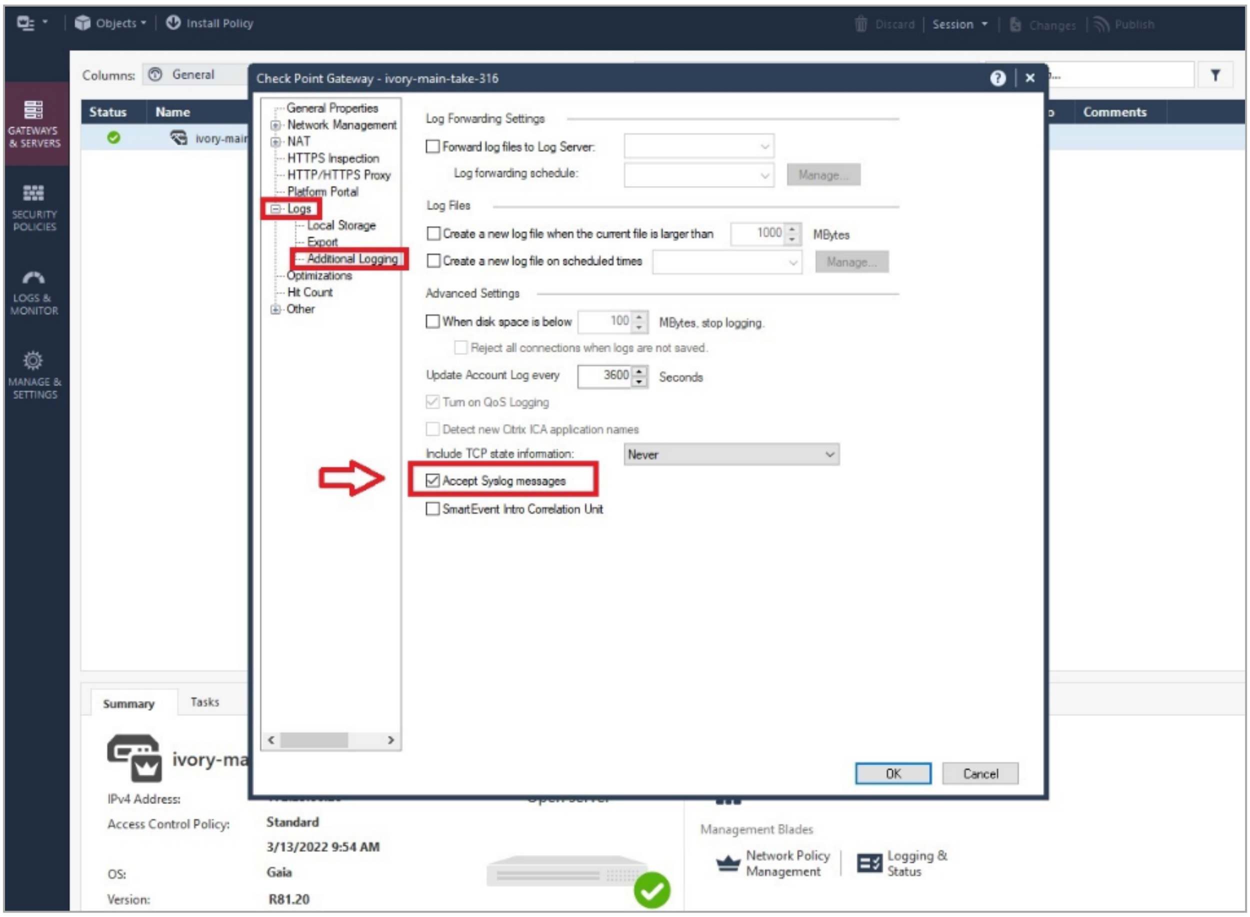
   b. Check Point IoT Infoblox DHCP



```
---- Check Point IoT Infoblox DHCP Nano Service ----
Type: Public, Version: 1.2202.269825-dev, Created at: 2022-01-09T02:09:40+0200
Registered Instances: 1
Status: Running
```

Troubleshooting the Infoblox DHCP - Syslog IoT Discovery Engine

1. Log in to **SmartConsole**.
2. Go to **Gateway & Services** > **Check Point** > **Management Server**.
3. Expand **Logs** > **Additional Logging**.



Check Point Gateway - ivory-main-take-316

Log Forwarding Settings

□ Forward log files to Log Server:

Log forwarding schedule:

Log Files

□ Create a new log file when the current file is larger than 1000 MBytes

□ Create a new log file on scheduled times

Advanced Settings

□ When disk space is below 100 MBytes, stop logging.

□ Reject all connections when logs are not saved.

Update Account Log every 3600 Seconds

☑ Turn on QoS Logging

□ Detect new Citrix ICA application names

Include TCP state information: Never

☑ Accept Syslog messages

□ SmartEvent Intro Correlation Unit

IPv4 Address:

Access Control Policy: Standard

3/13/2022 9:54 AM

OS: Gaia

Version: R81.20

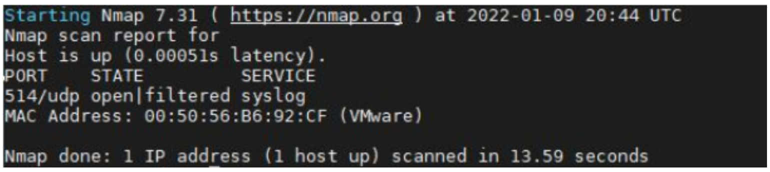
4. Select **Accept Syslog messages**.
5. Click **OK**.
6. Enable Syslog traffic from the Infoblox DHCP server to the Check Point Management Server.

   To enable, access the Infoblox DHCP server through SSH, and run:

   ```
   Infoblox > set maintenancemode
   ```

   ```
   Maintenance Mode > show network_connectivity proto udp <IP
   Address of Management Server> 514
   ```

Expected output:

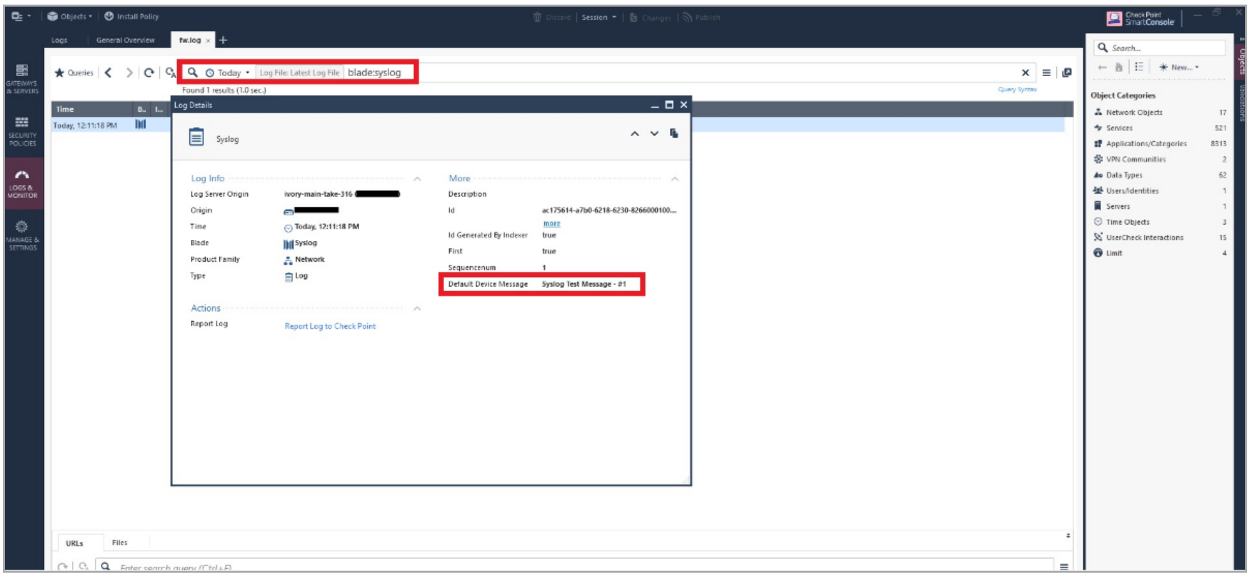


```
Starting Nmap 7.31 ( https://nmap.org ) at 2022-01-09 20:44 UTC
Nmap scan report for
Host is up (0.00051s latency).
PORT     STATE         SERVICE
514/udp open|filtered syslog
MAC Address: 00:50:56:B6:92:CF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

7. To access any Unix terminal through SSH hosted in the same network on which the Check Point Management Server is hosted, run:

   ```
   echo "Syslog Test Message - #1" | nc -u <IP Address of
   Management Server> 514
   ```

   Expected output: in **SmartConsole** > **Logs & Monitor** view:



Today | Log File: Latest Log File | blade:syslog

Found 1 results (1.0 sec.)

Time: Today, 12:11:18 PM

Log Details

Syslog

Log Info

Log Server Origin ivory-main-take-316 [redacted]

Origin [redacted]

Time Today, 12:11:18 PM

Blade Syslog

Product Family Network

Type Log

Actions

Report Log Report Log to Check Point

More

Description

Id ac175614-a7b0-6218-6230-8266000100... more

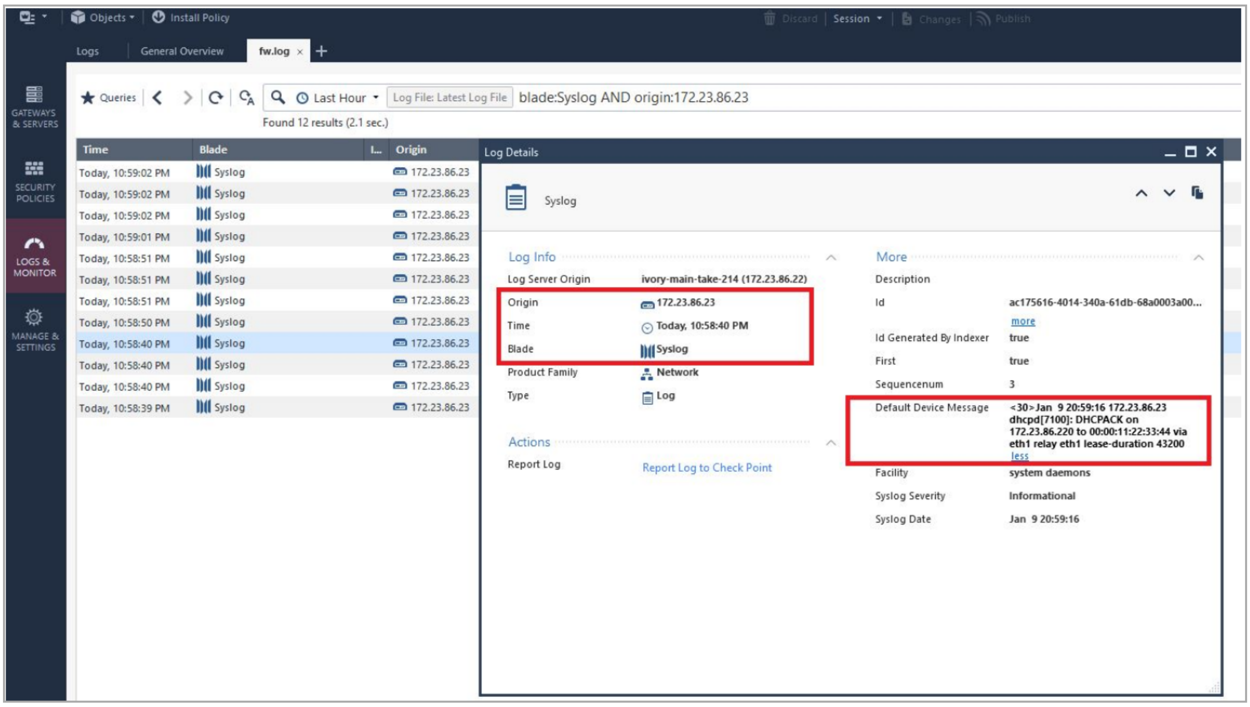
Id Generated By Indexer true

First true

Sequencenum 1

Default Device Message Syslog Test Message - #1

8. Filter by: **blade: syslog**



blade:Syslog AND origin:172.23.86.23

Found 12 results (2.1 sec.)

Time	Blade	I...	Origin
Today, 10:59:02 PM	Syslog		172.23.86.23
Today, 10:59:02 PM	Syslog		172.23.86.23
Today, 10:59:02 PM	Syslog		172.23.86.23
Today, 10:59:01 PM	Syslog		172.23.86.23
Today, 10:58:51 PM	Syslog		172.23.86.23
Today, 10:58:51 PM	Syslog		172.23.86.23
Today, 10:58:51 PM	Syslog		172.23.86.23
Today, 10:58:50 PM	Syslog		172.23.86.23
Today, 10:58:40 PM	Syslog		172.23.86.23
Today, 10:58:40 PM	Syslog		172.23.86.23
Today, 10:58:40 PM	Syslog		172.23.86.23
Today, 10:58:39 PM	Syslog		172.23.86.23

Log Details

Syslog

Log Info

Log Server Origin	ivory-main-take-214 (172.23.86.22)
Origin	172.23.86.23
Time	Today, 10:58:40 PM
Blade	Syslog
Product Family	Network
Type	Log

Actions

Report Log	Report Log to Check Point

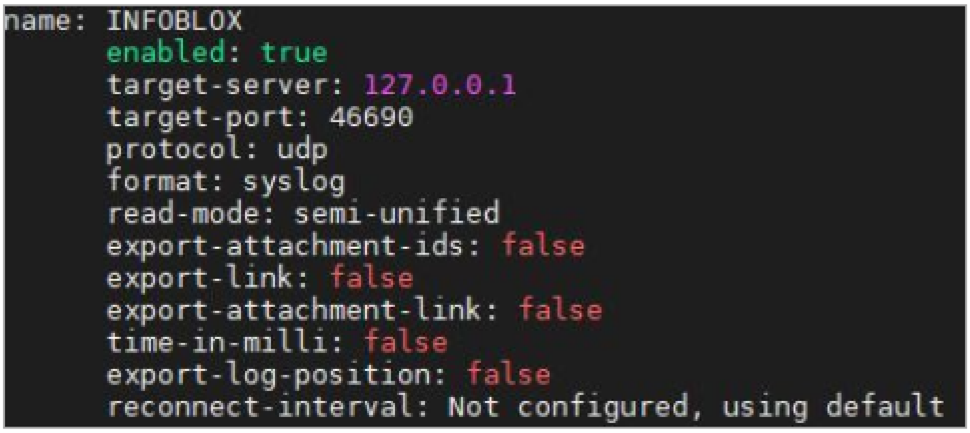
More

Description	
Id	ac175616-4014-340a-61db-68a0003a00... more
Id Generated By Indexer	true
First	true
Sequencenum	3
Default Device Message	<30>Jan 9 20:59:16 172.23.86.23 dhcpd[7100]: DHCPACK on 172.23.86.220 to 00:00:11:22:33:44 via eth1 relay eth1 lease-duration 43200 less
Facility	system daemons
Syslog Severity	Informational
Syslog Date	Jan 9 20:59:16

9. To access the Check Point Management Server through SSH, run:

   ```
   cp_log_export show
   ```

   Expected output:



```
name: INFOBLOX
      enabled: true
      target-server: 127.0.0.1
      target-port: 46690
      protocol: udp
      format: syslog
      read-mode: semi-unified
      export-attachment-ids: false
      export-link: false
      export-attachment-link: false
      time-in-milli: false
      export-log-position: false
      reconnect-interval: Not configured, using default
```

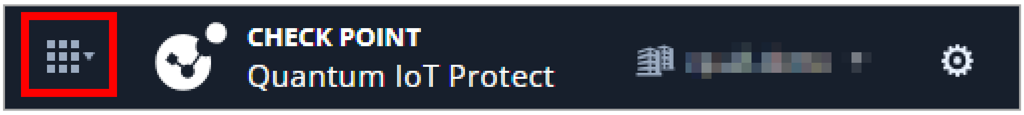
Appendix I - Integrating IoT Assets using Third-Party Discovery Engines through APIs

Quantum IoT Protect allows external vendors to act as third-party discovery engines by adding their IoT assets to the system through APIs. The supported vendors are:

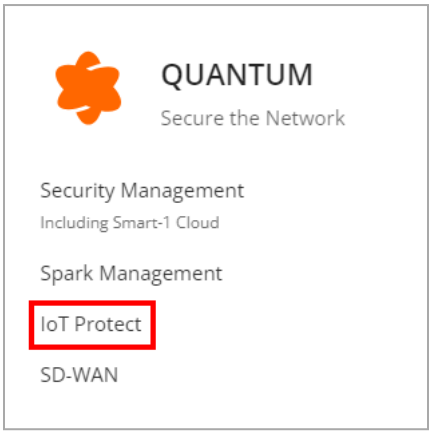
- Claroty
- Cynerio
- Ordr
- Phosphorus
- Saiflow
- Sapphire

Step 1 - Creating a Profile for Third-Party Discovery Engine in the Quantum IoT Protect Administrator Portal

1. Log in to *Check Point Infinity Portal*.
2. Click the **Menu** icon in the top left corner.

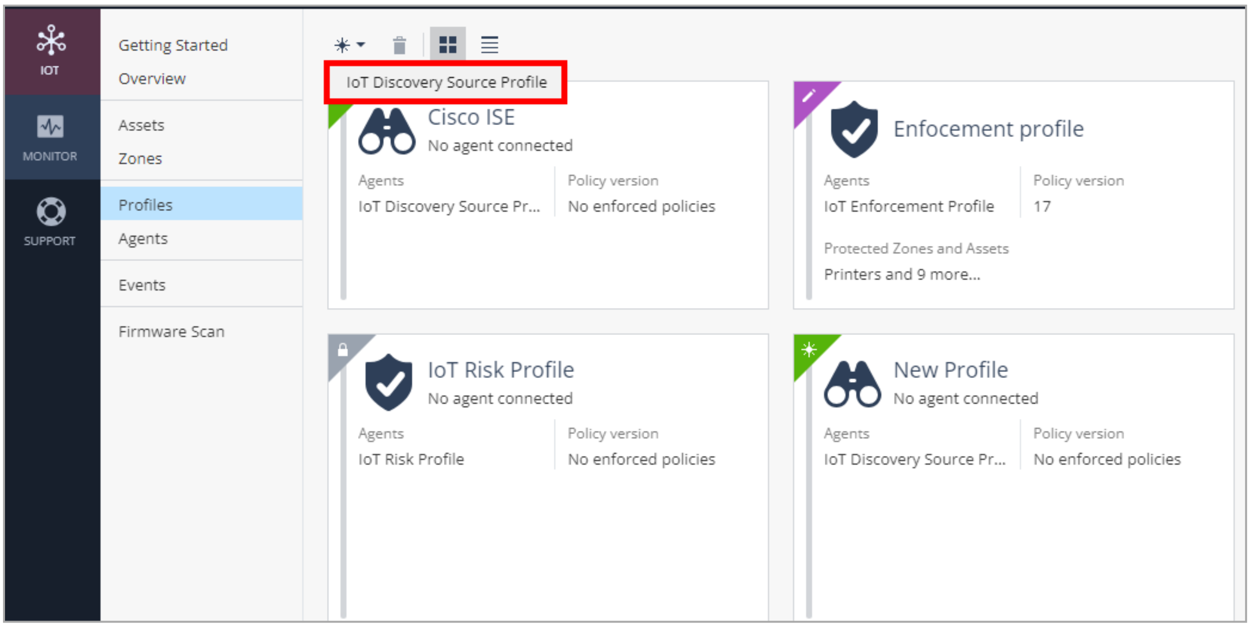


3. In the **Quantum** section, click **IoT Protect**.



4. Go to **IoT** > **Profiles**.

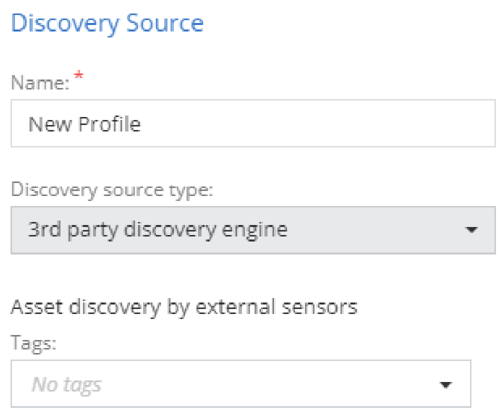
5. To create a new profile, click ✳ and select **IoT Discovery Source Profile**.



6. In the **Discovery Source** section:

a. Enter a name for the profile.

b. From the **Discovery source type** list, select **3rd party discovery engine**.



Discovery Source

Name: *

New Profile

Discovery source type:

3rd party discovery engine

Asset discovery by external sensors

Tags:

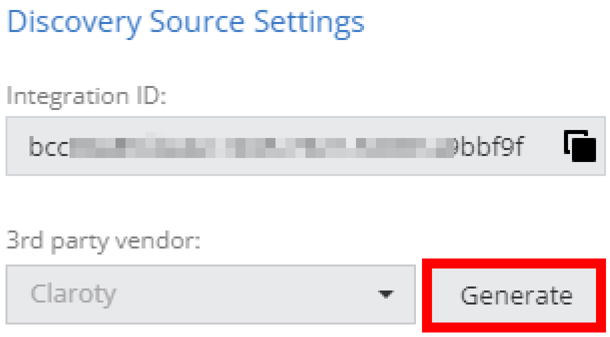
No tags

7. In the **Discovery Source Settings** section:

   a. Copy the **Integration ID**.

   b. From the **3rd party vendor** list, select the vendor.

c. To integrate the vendor with Infinity Portal service, you must generate an API key. To do that, click **Generate**.



Discovery Source Settings

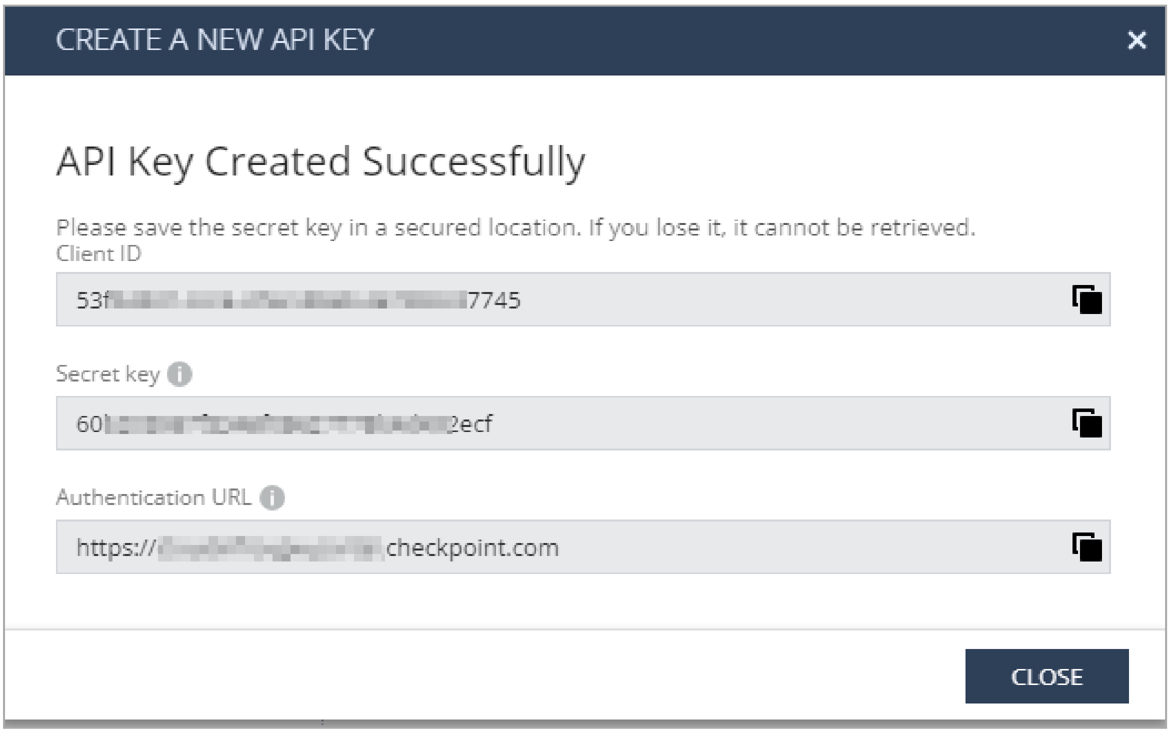
Integration ID:

bcc[redacted]bbf9f

3rd party vendor:

Claroty

The system generates a new API key.



CREATE A NEW API KEY

API Key Created Successfully

Please save the secret key in a secured location. If you lose it, it cannot be retrieved.

Client ID

53f[redacted]7745

Secret key

60[redacted]2ecf

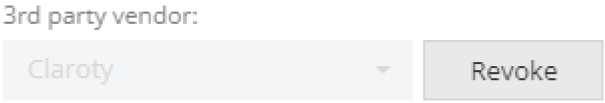
Authentication URL

https://[redacted]checkpoint.com

- **Client ID** - The identifier for the vendor's account and the client service that uses this API key.
- **Secret key** - The password to access the Check Point Infinity Portal.

- **Authentication URL** - The URL address used to authenticate API requests. In addition, it shows the specific gateway that uses this URL to authenticate the Client ID and Secret key.

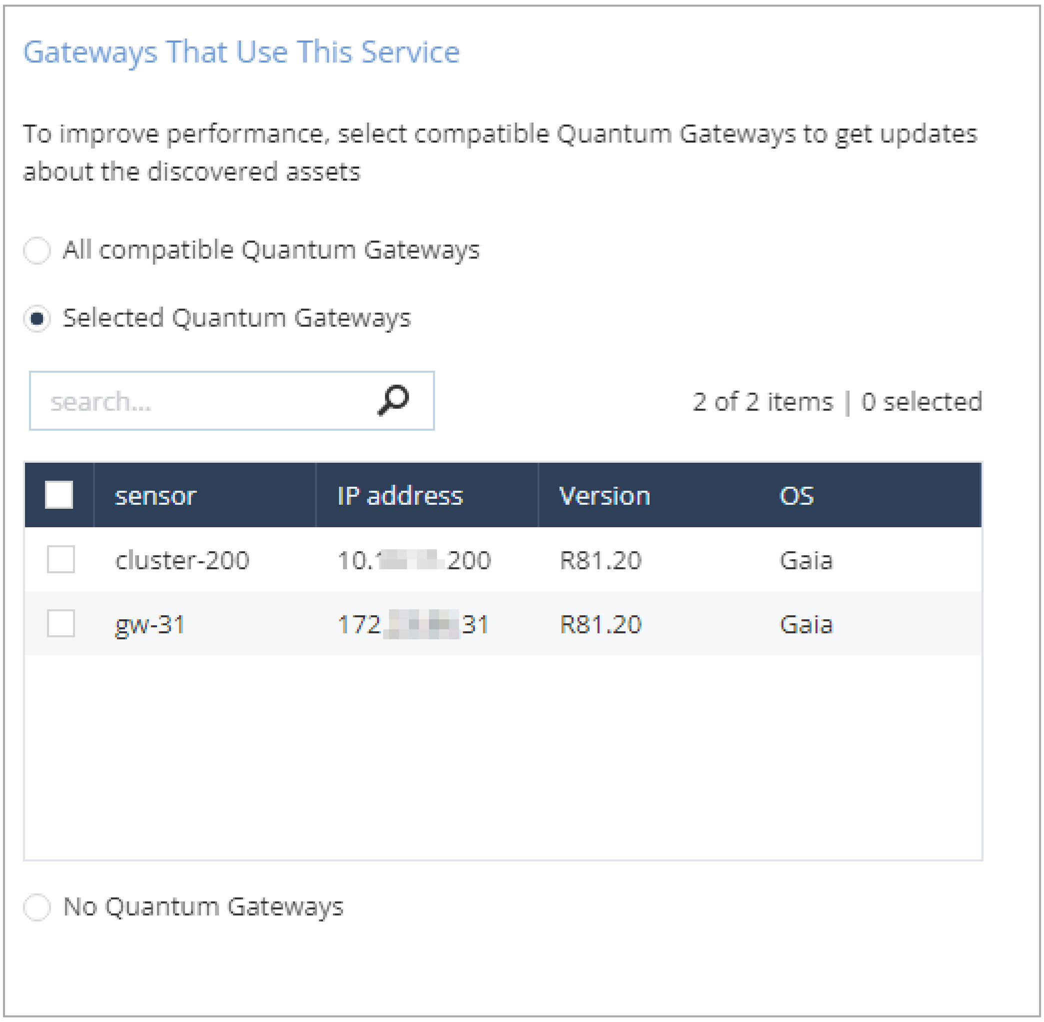
  Note - To revoke the generated API key, click **Revoke**.



3rd party vendor: Claroty

d. Copy and share the **Integration ID**, **Client ID**, **Secret key** and **Authentication URL** with the vendor.

8. In the **Gateways That Use This Service** section, select the gateway where you want to add the assets.



Gateways That Use This Service

To improve performance, select compatible Quantum Gateways to get updates about the discovered assets

○ All compatible Quantum Gateways

● Selected Quantum Gateways

search...

2 of 2 items | 0 selected

□	sensor	IP address	Version	OS
□	cluster-200	10.[redacted]200	R81.20	Gaia
□	gw-31	172[redacted]31	R81.20	Gaia

○ No Quantum Gateways

9. Click **Enforce**.

Step 2 - Adding Assets from Third-Party Discovery Engines (External Vendors)

Prerequisites

1. Make sure that the vendor has the following details:
   - Integration ID
   - Client ID
   - Secret key
   - Authentication URL
2. An API client or API testing tool to run API calls.
3. API Region URL:

Region	URL
Europe (EU)	*https://cloudinfra-gw.portal.checkpoint.com/app/iotprotect/api/v1/asset-gateway*
United States (US)	*https://cloudinfra-gw-us.portal.checkpoint.com/app/iotprotect/api/v1/asset-gateway*
Australia (AU)	*https://cloudinfra-gw.ap.portal.checkpoint.com/app/iotprotect/api/v1/asset-gateway*

For more information, see IoT External Asset API documentation.

Appendix J - Active Probing

Active probing queries the network for additional information on the IP addresses detected by these integrations:

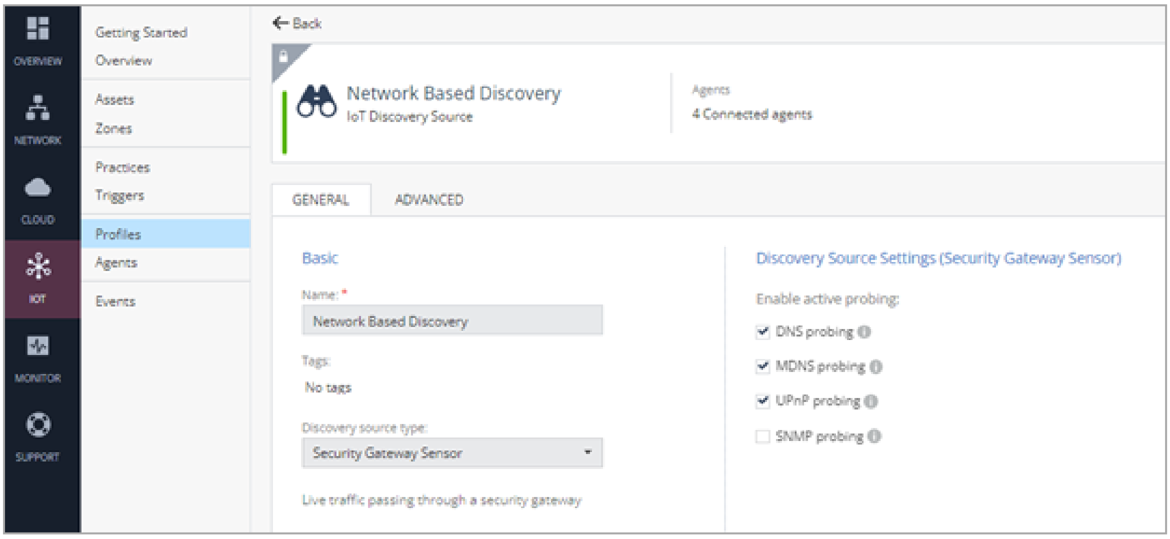
- Cisco ISE
- SNMP
- Network Sensor

All probes are enabled by default and can be configured. Active probing uses one of these protocols to query and retrieve the IP data:

1. DNS
2. Multi DNS (mDNS)
3. uPnP
4. SNMP

Configuring Active Probing

1. Log in to *Check Point Infinity Portal*.
2. Under **Quantum**, go to **IoT Protect** > **IoT** > **Profiles**.
3. Click the required profile to edit it.
4. Under **Discovery Source Settings**, select the probes that you want to enable.
   - **Network Based Discovery** integration:



Network Based Discovery
IoT Discovery Source

Agents
4 Connected agents

Basic

Name: * Network Based Discovery

Tags: No tags

Discovery source type: Security Gateway Sensor

Live traffic passing through a security gateway

Discovery Source Settings (Security Gateway Sensor)

Enable active probing:

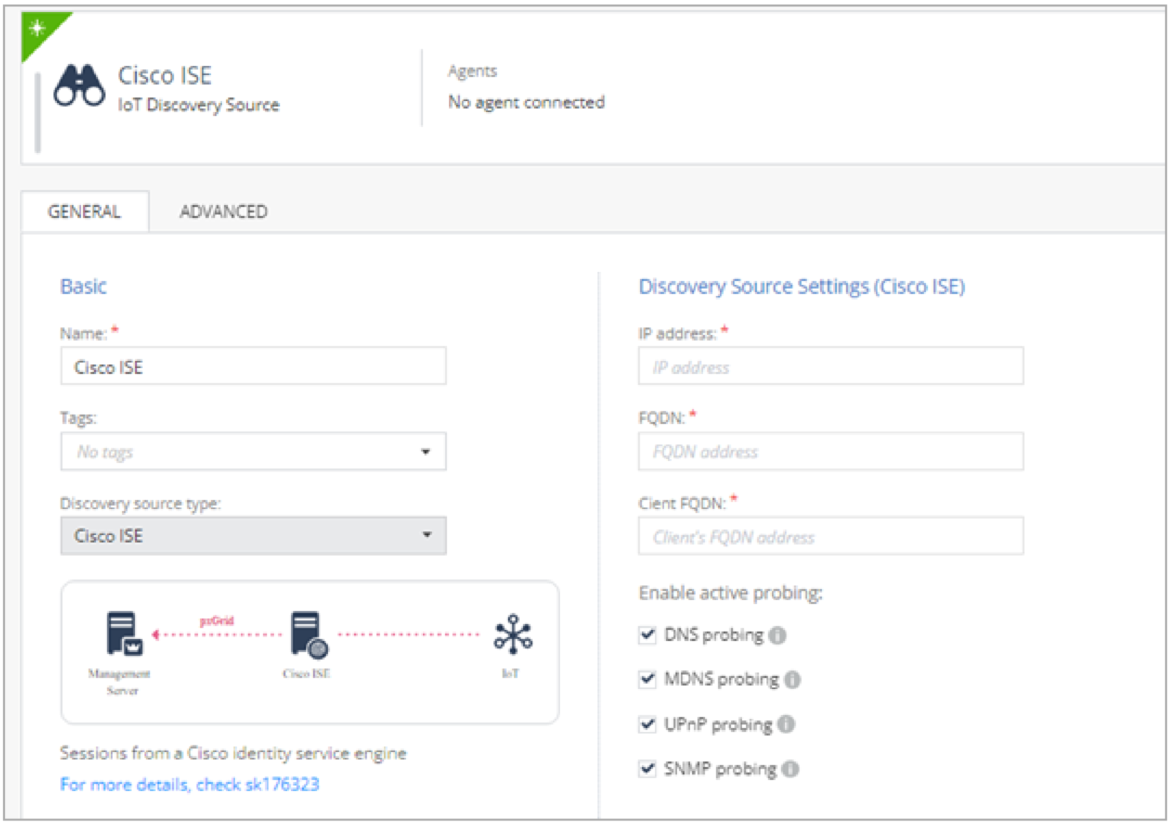
☑ DNS probing

☑ MDNS probing

☑ UPnP probing

☐ SNMP probing

- **Cisco ISE** integration:



Cisco ISE
IoT Discovery Source

Agents
No agent connected

GENERAL | ADVANCED

Basic

Name: *
Cisco ISE

Tags:
No tags

Discovery source type:
Cisco ISE

Sessions from a Cisco identity service engine
For more details, check sk176323

Discovery Source Settings (Cisco ISE)

IP address: *
IP address

FQDN: *
FQDN address

Cient FQDN: *
Client's FQDN address

Enable active probing:

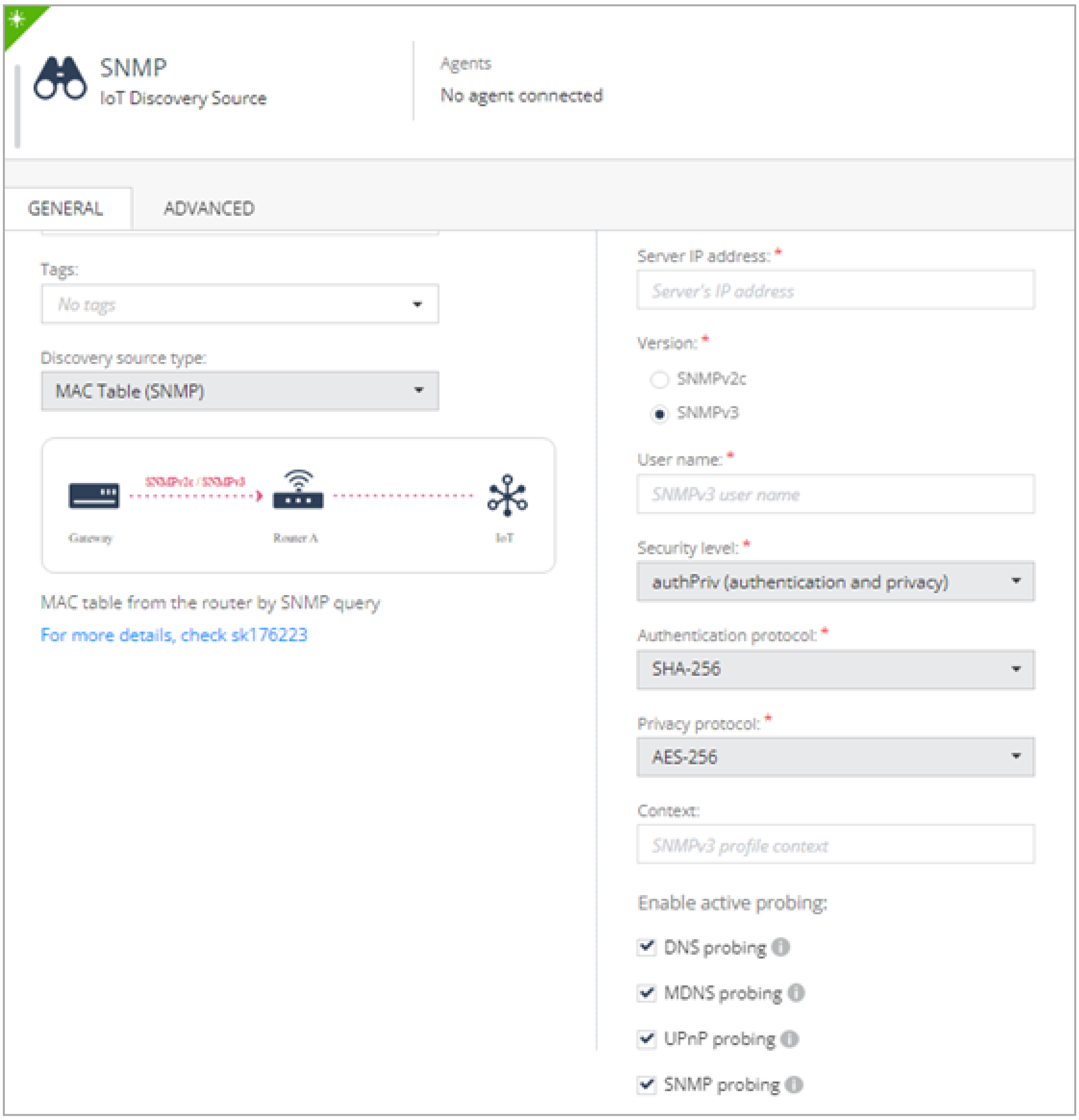
☑ DNS probing

☑ MDNS probing

☑ UPnP probing

☑ SNMP probing

- **SNMP** integration:



SNMP
IoT Discovery Source

Agents
No agent connected

GENERAL | ADVANCED

Tags:
No tags

Discovery source type:
MAC Table (SNMP)

MAC table from the router by SNMP query
For more details, check sk176223

Server IP address: *
Server's IP address

Version: *
○ SNMPv2c
● SNMPv3

User name: *
SNMPv3 user name

Security level: *
authPriv (authentication and privacy)

Authentication protocol: *
SHA-256

Privacy protocol: *
AES-256

Context:
SNMPv3 profile context

Enable active probing:
☑ DNS probing
☑ MDNS probing
☑ UPnP probing
☑ SNMP probing

Appendix K - Onboarding Quantum IoT Protect on Quantum Maestro Security Group

Prerequisites

- R81.20 Jumbo Hotfix Accumulator Latest Take.
- Disable the SMO Image Cloning on the Quantum Maestro Security Group:
  1. Connect to the command line on the Quantum Maestro Security Group.
  2. If your default shell is the Expert mode, run this command to go to Gaia gClish:

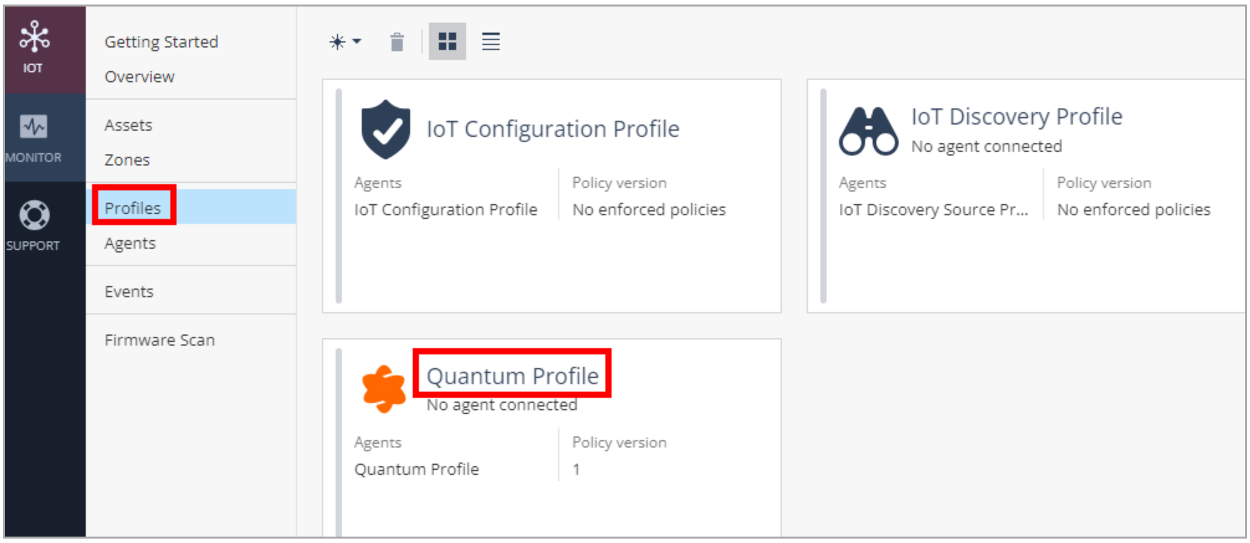
     ```
     gclish
     ```
  3. To disable the SMO Image Cloning, run:

     ```
     set smo image auto-clone state off
     ```

     For more information, see the *Maestro Administration Guide* for your version.

Installing Nano-Agent Manually on Quantum Maestro Security Group

1. Log in to *Check Point Infinity Portal*.
2. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Profiles**.
3. Click **Quantum Profile**.

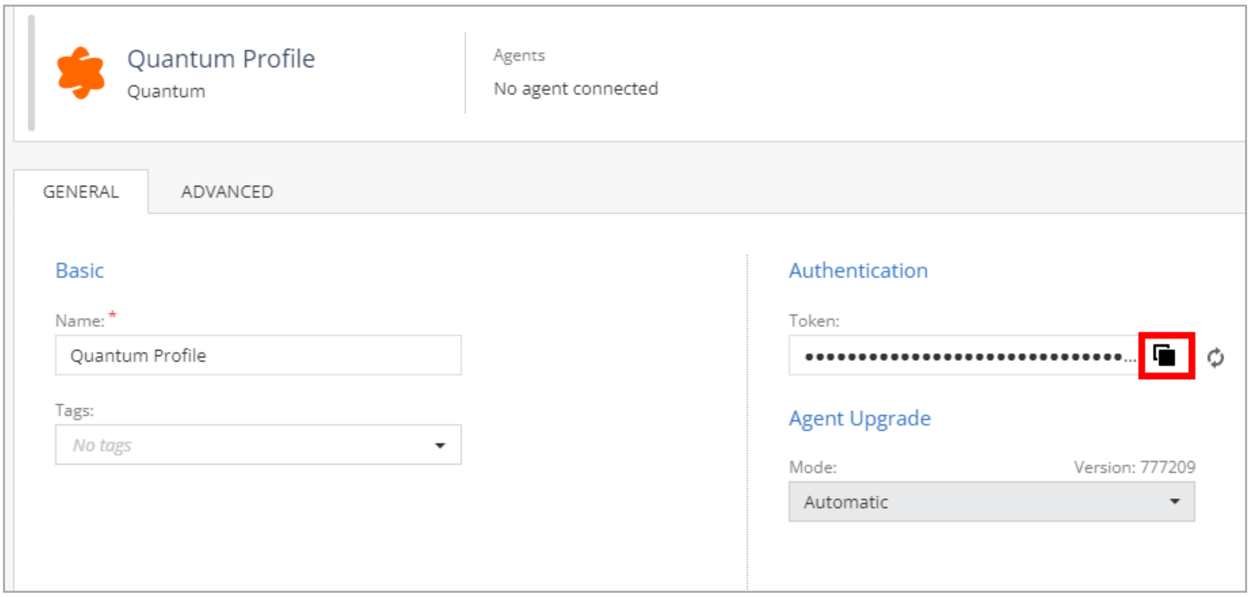


IoT Configuration Profile
Agents: IoT Configuration Profile
Policy version: No enforced policies

IoT Discovery Profile
No agent connected
Agents: IoT Discovery Source Pr...
Policy version: No enforced policies

Quantum Profile
No agent connected
Agents: Quantum Profile
Policy version: 1

4. In the **Authentication** section, click ⧉ to copy the token to your clipboard.



Quantum Profile
Quantum
Agents: No agent connected

Name: * Quantum Profile
Tags: No tags
Token: ••••••••••••••••••••••••••••••••...
Mode: Automatic
Version: 777209

5. Connect to the command line on the Quantum Maestro Security Group.

6. Log in to the Expert mode.

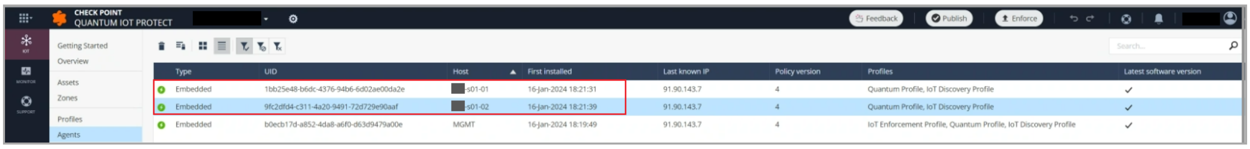
7. Run:

```
$MDS_FWDIR/bin/nano-egg --install --token <paste token from
clipboard> --run-all-members
```

Verifying the Installation

1. Log in to *Check Point Infinity Portal*.

2. In the **Quantum** section, go to **IoT Protect** > **IoT** > **Agents**.



	Type	UID	Host	First installed	Last known IP	Policy version	Profiles	Latest software version
●	Embedded	1bb25e48-b6dc-4376-94b6-6d02ae00da2e	[redacted]-s01-01	16-Jan-2024 18:21:31	91.90.143.7	4	Quantum Profile, IoT Discovery Profile	✓
●	Embedded	9fc2dfd4-c311-4a20-9491-72d729e90aaf	[redacted]-s01-02	16-Jan-2024 18:21:39	91.90.143.7	4	Quantum Profile, IoT Discovery Profile	✓
●	Embedded	b0ecb17d-a852-4da8-a6f0-d63d9479a00e	MGMT	16-Jan-2024 18:19:49	91.90.143.7	4	IoT Enforcement Profile, Quantum Profile, IoT Discovery Profile	✓

3. Locate the Quantum Maestro Security Group member in the **Host** column and verify that the agent is connected (●).

Known Limitations

Monitoring the nano-agent status on all Quantum Maestro security group members simultaneously using `cpnano` commands (such as gexec variants, asg) is not supported. However, you can monitor the nano-agent status on each member individually.