QUANTUM

02 July 2025

QUANTUM SMART-1 CLOUD

Administration Guide

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.

Check Point Quantum Smart-1 Cloud Administration Guide

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.

Table of Contents

Smart-1 Cloud Overview

Check Point introduces the Quantum Smart-1 Cloud, an innovative, all-encompassing security management solution hosted entirely in the cloud. This solution simplifies security management across all environments, including on-premise firewalls, networks, cloud services, mobile devices, and IoT systems.

Quantum Smart-1 Cloud provides a centralized cloud-based management console that helps you monitor and mitigate evolving threats across multiple devices and workloads. This solution scales automatically as the number of Security Gateways increases, eliminating concerns about physical storage constraints or log capacity limitations.

With Quantum Smart-1 Cloud, you can automate essential tasks such as Security Gateways onboarding, device monitoring, facility power management, and software updates, saving valuable time and resources.

Quantum Smart-1 Cloud makes sure you always have access to the latest features and security capabilities through automatic updates to your unified management platform, keeping you current with the newest security advancements.

Key Benefits

- **Always the Latest Security Management** - The newest features are automatically updated in your unified management platform.
- **Zero Maintenance** - No need to monitor or perform backup operations on your Security Management Server.
- **On-demand Expansion** - Seamlessly increase capacity to support more Security Gateways and additional storage needs.

Use Case

A typical use case is a company seeking to improve operational efficiency and reduce the complexity of their Security Management platform. With Smart-1 Cloud, companies can focus more on managing their core security rather than the underlying infrastructure.

Tasks like maintenance, software updates, security patches, backups, and system health monitoring - all consume significant time and resources. Additionally, as companies grow, they need to effectively scale their security solutions, often requiring new hardware purchases and complex migration processes. By shifting these IT management responsibilities to Smart-1 Cloud, companies can significantly enhance their security management while concentrating on their core business priorities.

Deploying a new Management Service in Smart-1 Cloud takes just one minute. Once deployment completes, you get a new Security Management Server instance running the latest version - immediately ready to connect with Security Gateways. Existing customers can easily migrate from their on-premises environment to Smart-1 Cloud. After migration, you can resume work precisely where you left off with your on-premises Security Management Server (see *"Migrate" on page 43* for more information).

Important - Migration to Smart-1 Cloud is only supported from the Security Management Server version R81.10 and higher.

Supported Gateways and Versions

Category	Appliance Models	Software Version
Quantum Spark Security Gateways	2000	R81.10.X and higher
	1900	R81.10.X and higher
	1800 1600	R81.10.X and higher R81.10.X and higher
	1500	R81.10.X and higher
	CloudGuard Edge	R81.10.X and higher
Quantum Security Gateways	23000 21000 16000 15000 13000 12000 9000 7000 6000 5000 4000 3000	R81.10 and higher
CloudGuard Network	CloudGuard Network Security Gateway	R81.10 and higher
	Auto Scaling solutions	▪ Azure VMSS ▪ AWS ASG ▪ GCP MIG
Security Gateways	Open Servers	R81.10 and higher
Quantum Maestro	All Maestro-supported appliances	R81.10 and R81.20
VSNext	All VSNext-supported platforms	See sk166056 - Smart-1 Cloud Release Updates for more information.

Note - Smart-1 Cloud supports SecureXL in User Space mode (UPPAK - User Space Performance Pack) starting from R81.20 Jumbo Hotfix Accumulator Take 53.

Important - The `insights` CLI tool, which provides monitoring for the entire Scalable Platform cluster in Expert mode and Gaia gClish, can display an error indicating a mismatch in the IP address for the MaaS tunnel interface under a specific context ID. This is a cosmetic issue and does not affect the functionality.

Getting Started with Smart-1 Cloud

The *Check Point Infinity Portal* hosts the Smart-1 Cloud application. Before using the application, you must create an account in the portal.

To start working with Smart-1 Cloud, follow these steps:

1. *"Step 1: Create an Account in the Infinity Portal" below*
2. *"Step 2: Access the Infinity Smart-1 Cloud Portal" on the next page*
3. *"Creating and Deploying a New Smart-1 Cloud" on page 16*
4. Log in to Streamed SmartConsole (see *"Log in to SmartConsole from Smart-1 Cloud" on page 38* for more information).
5. Connect Security Gateways (see *"Connecting Gateways and Clusters in Smart-1 Cloud" on page 18* for more information).

Step 1: Create an Account in the Infinity Portal

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

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

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

Step 2: Access the Infinity Smart-1 Cloud Portal

Start a free trial if you don't want to associate Smart-1 Cloud with a user account. This option allows you to use Smart-1 Cloud for a 30-day period.

After selecting Start free trial, the welcome page offers two options:

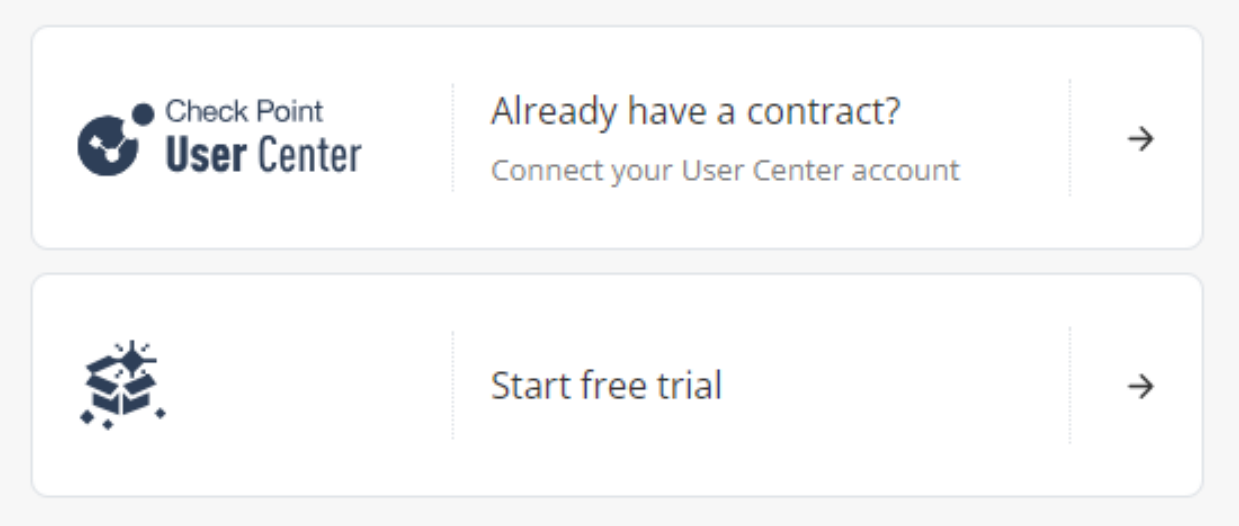
Create a new Smart-1 Cloud Management

Connect an existing Self-Hosted (on-premises) Management

For information on connecting existing Self-Hosted Management Servers to the Infinity Portal, refer to the R81.20 Quantum Security Management Administration Guide > Connecting On-Premises Management Servers and Security Gateways to the Infinity Portal.

1. Log in to the Infinity Portal.
2. Click the **Menu** icon in the top left corner of the Infinity Portal window.
3. From the Quantum group, select **Security Management**.

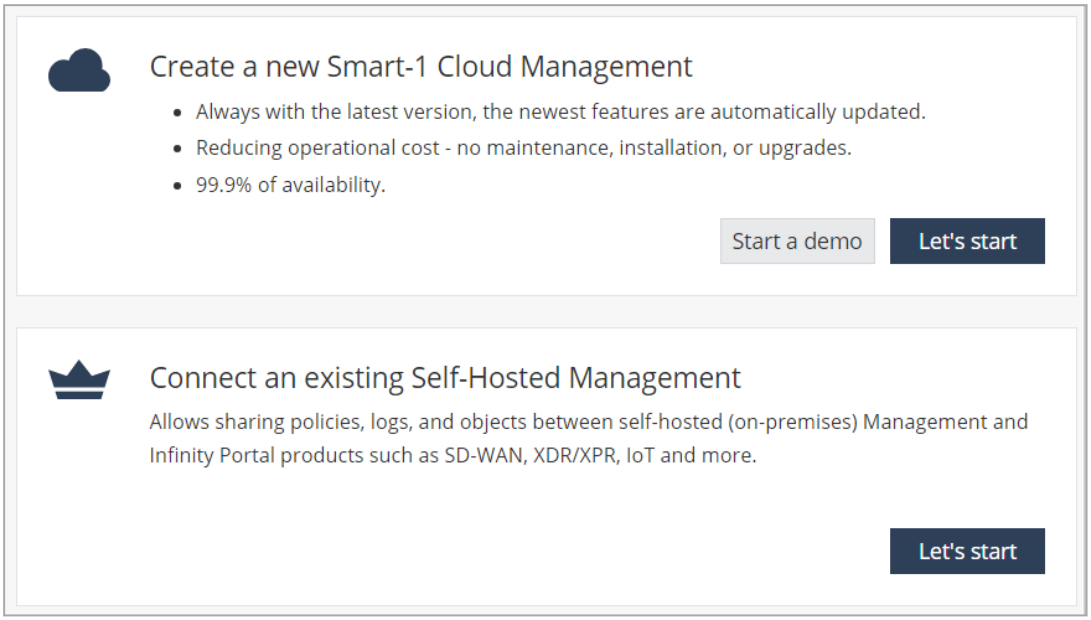
   Note - Security Management provides a unified experience for all your Quantum Management solutions.
   You can connect multiple self-hosted (on-premises) Security Management Servers and manage one Smart-1 Cloud environment in a single Infinity Portal tenant.
4. If you access the Smart-1 Cloud portal for the first time, select one of these options:



   - Connect your User Center account if you already have a Check Point contract. When you select this option, the **Attach Account** window opens. For more information, see **Associated Accounts** in the Infinity Portal Administration Guide.

     After selecting **existing account**, the main screen shows a dashboard (a Security Policies dashboard by default) of your environment.

- Start a free trial if you do not want to associate Smart-1 Cloud with a user account. When you select this option, you can use Smart-1 Cloud for a 30-day period.
  - After you select **Start free trial**, the welcome page offers to **Create a new Smart-1 Cloud Management** or **Connect an existing Self-Hosted (on-premises) Management**.



  For information on connecting existing Self-Hosted Management Servers to the Infinity Portal, refer to the R81.20 Quantum Security Management Administration Guide > Connecting On-Premises Management Servers and Security Gateways to the Infinity Portal.

  - When selecting **Create a new Smart-1 Cloud Management**, you can:
    - **Start a demo**.
    - Click **Let's start**.

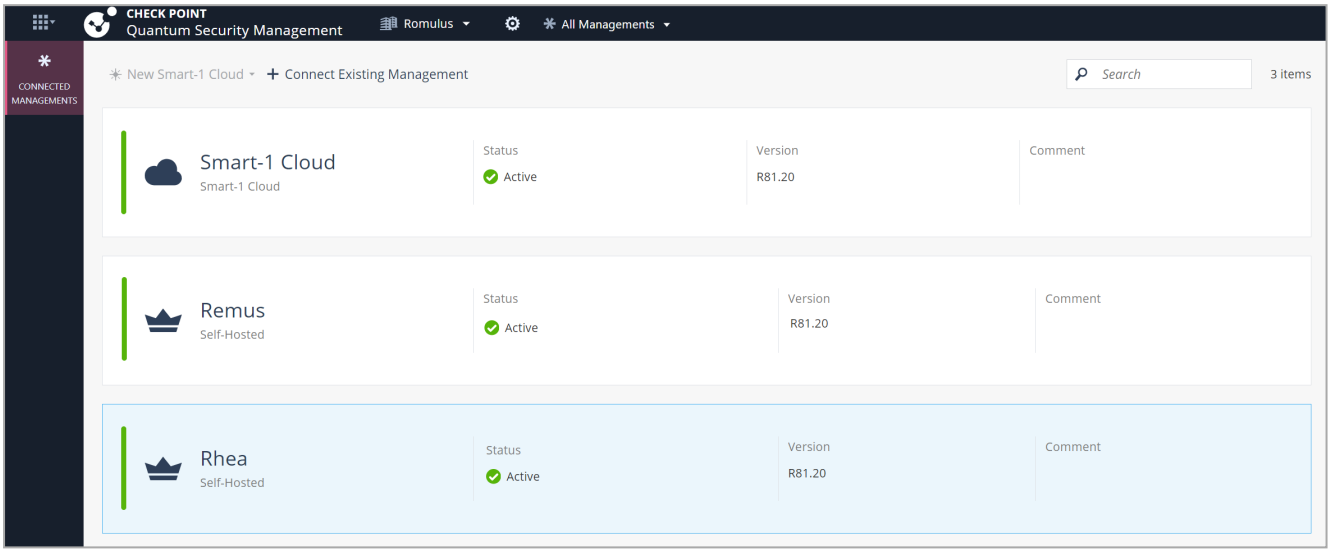
      An email confirmation of your registration will be sent to your email account.

      After approving your registration, the page automatically refreshes, and you can begin using the application.

Navigating the Smart-1 Cloud Portal

The management menu is located in the upper middle of the page. From this drop-down menu, select either **All Managements** or **Smart-1 Cloud**.

On the **All Managements** page, you can find all connected Security Management Servers.



Note - You can connect only one Smart-1 Cloud environment.

Common Smart-1 Cloud Tasks:

- Creating a new Smart-1 Cloud environment.
- Logging into SmartConsole.
- Connecting Security Gateways.
- Obtaining more information and running advanced options.

Additionally, you can:

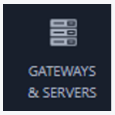
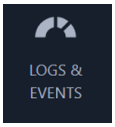
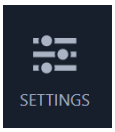
- Update and change Global Settings.

  The information in Global Settings and Profile contains the initial default values that affect the entire system.

- Access the latest Smart-1 Cloud news and online help.

For more information, see the *Infinity Portal Administration Guide*.

Overview of the Smart-1 Cloud Portal options:

To do this:	Click this:
■ Log in to Smart-1 Cloud. ■ Access Control, Threat Prevention, HTTPS Inspection, Manage Policies.	
■ Register and add new Security Gateways to your management service.	
■ See logs and monitor events.	
■ Infinity Services.	
■ General Smart-1 Cloud information. ■ Information about the use of APIs in your Smart-1 Cloud application. ■ SmartConsole: Web SmartConsole, Installed SmartConsole. ■ Migrate an existing management to the cloud. ■ Advanced configuration: Cloud Management Extension (CME) Configuration, Forward to SIEM, Inspect files (.def files).	

Creating and Deploying a New Smart-1 Cloud

After registering for the Smart-1 Cloud application, you can begin onboarding to a new Smart-1 Cloud.

To create a new Smart-1 Cloud:

Click **Let's Start**.

Note - There are two environment types:

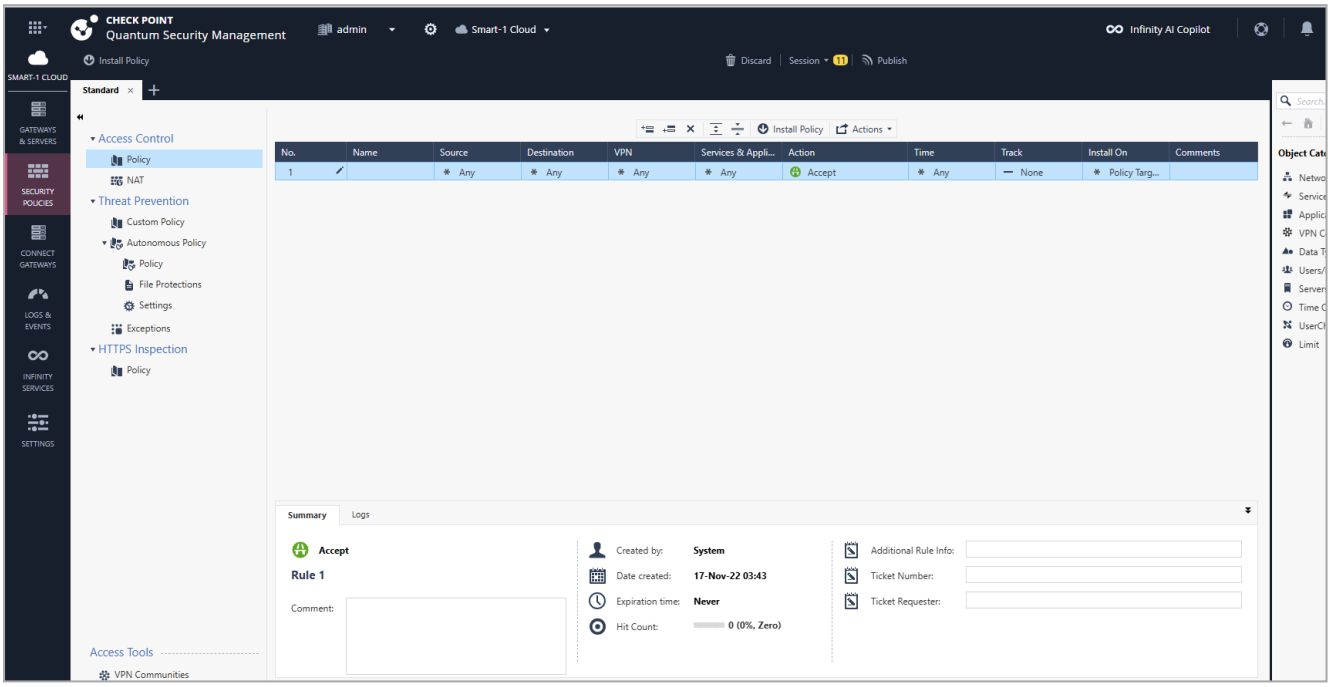
- **Production**
  The production environment includes a 30-day free trial. You can extend the trial period with an EVAL license. Contact your Check Point representative for this license.
- **Demo**
  The demo environment is for demonstration purposes only and cannot be used in production. This environment terminates after 24 hours with no option to extend it.

The **Preparing Account** window opens. It takes 1-2 minutes to create a new service.

After the process completes, a confirmation email is sent to your account.

A Smart-1 Cloud Home Page Overview

After service creation, the Smart-1 Cloud home page opens:

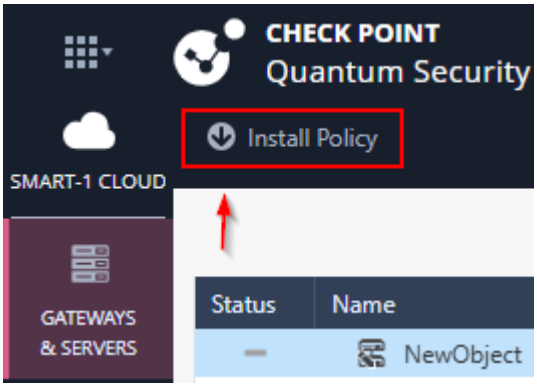


On the Smart-1 Cloud home page, you can:

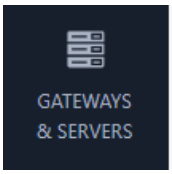
- Manage Access Control policies and layers.
- Manage Threat Prevention and HTTPS Inspection policies.
- Publish sessions.
- Install policy on managed Security Gateways.
- Discard changes made during the session.
- View session details to see the number of changes made.

Publish the session to make your changes visible to other administrators and ready to install on Security Gateways.

You can install policy with the **Install Policy** button in the top left of the home page.



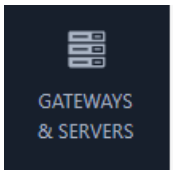
Connecting Gateways and Clusters in Smart-1 Cloud



Connecting on-premises Security Gateway or CloudGuard Network Security Gateway

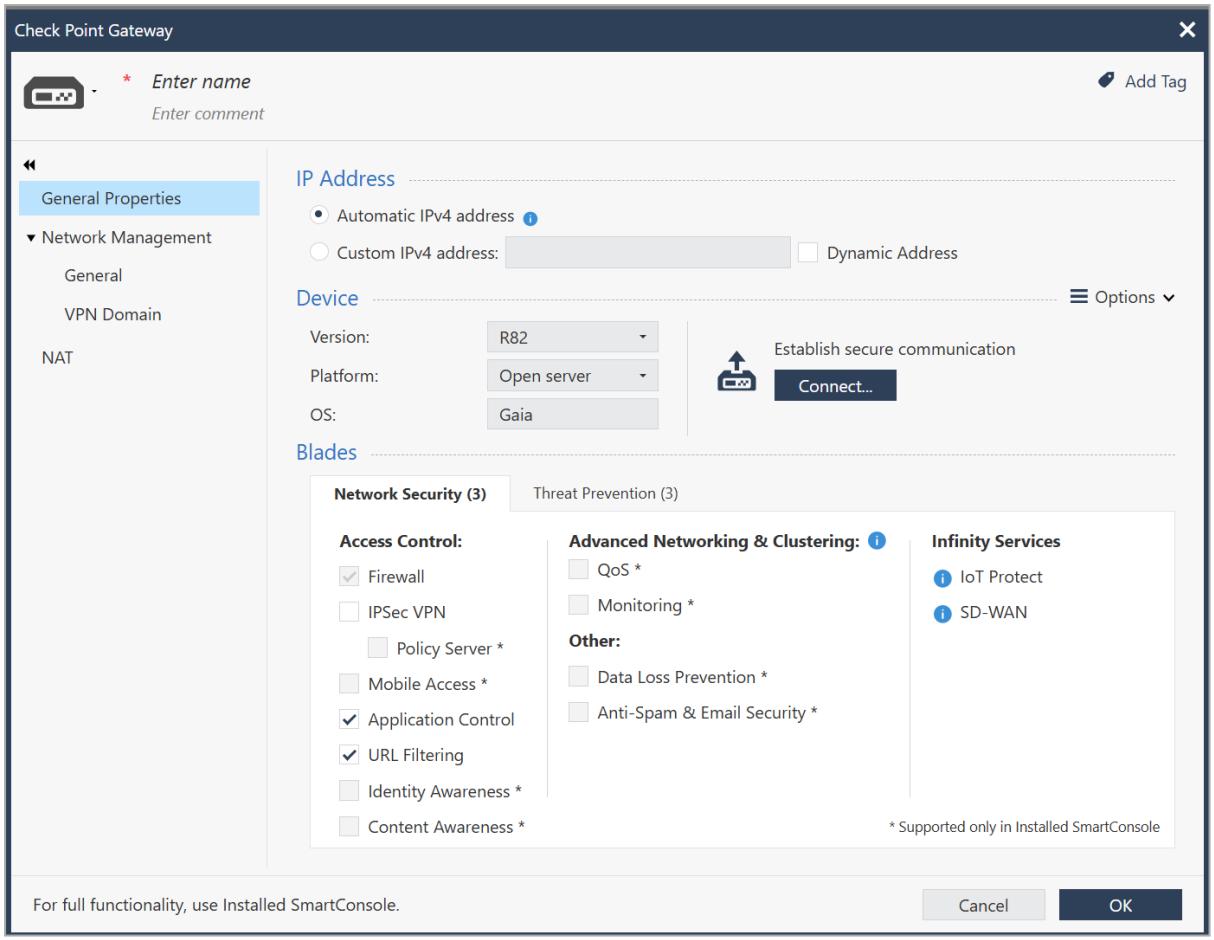
Procedure

1. From the left navigation panel, click **Gateways & Servers**.



2. Click the **New** icon or a New Gateway button and select **Gateway...**.

   The **Check Point Gateway** properties window opens.



3. Fill in the required fields for the Check Point Security Gateway:
   a. **Enter name** - The name for the Security Gateway.
   b. **IP Address**
      - **Automatic IPv4 address**: The Security Gateway's IP address is set to an internal IP address used for cloud communication over an outbound tunnel.
      - **Custom IPv4 address**: Configure a static IP address if it is not an SD-WAN Gateway.

      You can configure the Security Gateway object in Smart-1 Cloud with a static IP address as the primary IP address (in the same way you configure a Security Gateway from an on-premises Security Management Server).

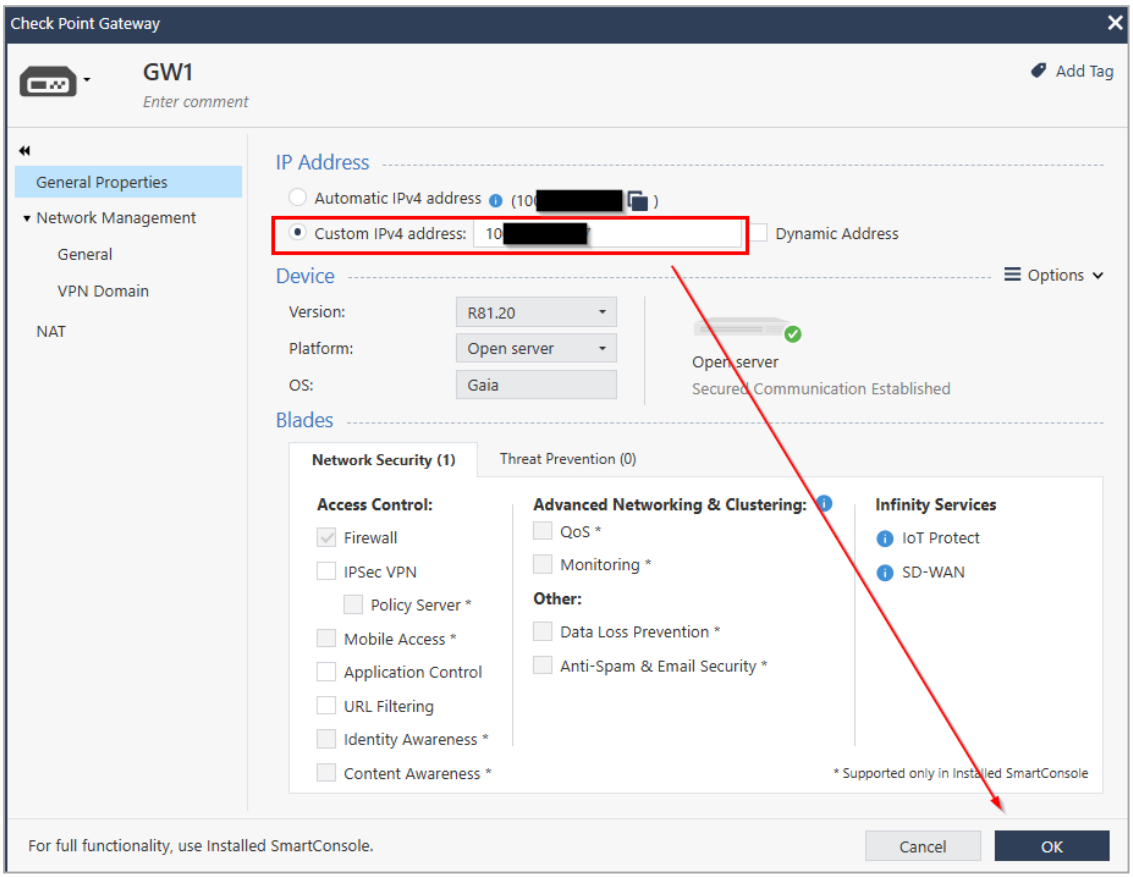
      When you configure the Security Gateway object with a Tunnel IP address, management traffic, control connections, and Smart-1 Cloud tenant communications use this main static IP address through the maas_tunnel interface.

      Note - We recommend using a static IP address when available, unless configuring an SD-WAN Gateway.
      This simplifies configuration for features such as UserCheck, NAT rules, and VPN configuration.
4. In the **Device** section, click **Connect**.

   The **Connect Device** window opens.
5. In the Security Gateway section, select **Appliance/Open Server**.
6. Connect to the CLI on the Security Gateway. In Clish, run the provided command to set the authentication token. The initial connection status is **Pending connection**. After the Security Gateway connects to Smart-1 Cloud, the status changes to **Connected**.
7. To establish Secure Internal Communication (SIC) between the Security Gateway and Smart-1 Cloud, enter the one-time password you set on the Security Gateway.
8. Click **Next** and wait until the Security Gateway connection process finishes. Then close the **Connect Device** window.
9. Click **OK**.

If you have an existing Security Gateway object configured with a Tunnel IP address, follow these steps to change it to a static IP address:

1. Edit the Security Gateway object in SmartConsole:
   a. Open Web SmartConsole or Streamed SmartConsole.
   b. Change the IP address in the Security Gateway object properties to a static IP address.
   c. Click OK.



   d. To test SIC communication, open the Security Gateway object again and click **Test Communication** in the Options drop-down menu.

2. Click **Register**.

   This creates a new Security Gateway object in Smart-1 Cloud with the name you entered.

3. Click **Connect Gateway**.

- For an **on-premises Security Gateway**, follow the on-screen instructions to complete the connection.

  Note - Connecting a new Security Gateway involves two steps:
  a. Connect the Security Gateway to the service by performing the required steps on the Security Gateway as instructed. When completed, the status in the portal shows **Pending SIC**.
  b. Connect the Security Management Server to the Security Gateway by logging into SmartConsole and establishing SIC between the Security Management Server and Security Gateway. When complete, the portal shows **Registration complete**.

- For a **CloudGuard Network Security Gateway**:

  i. Copy the **Token** from the **Connect Gateway** screen.

  ii. In the **Security Gateway deployment template**:

    a. Paste the **Token** into the appropriate field.

    b. Complete all other required fields and start the deployment.

    c. When Security Gateway deployment completes:

      i. A tunnel is established between the Security Gateway and Smart-1 Cloud.

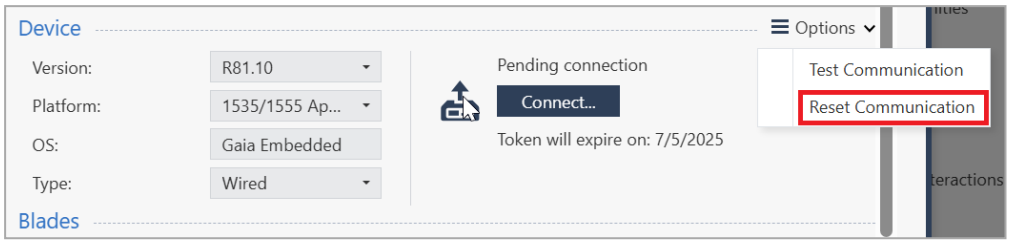
      ii. The Security Gateway status changes to **Pending trust (SIC) establishment**.

  iii. Connect to SmartConsole, open the new Security Gateway object, initialize SIC, and publish the session.

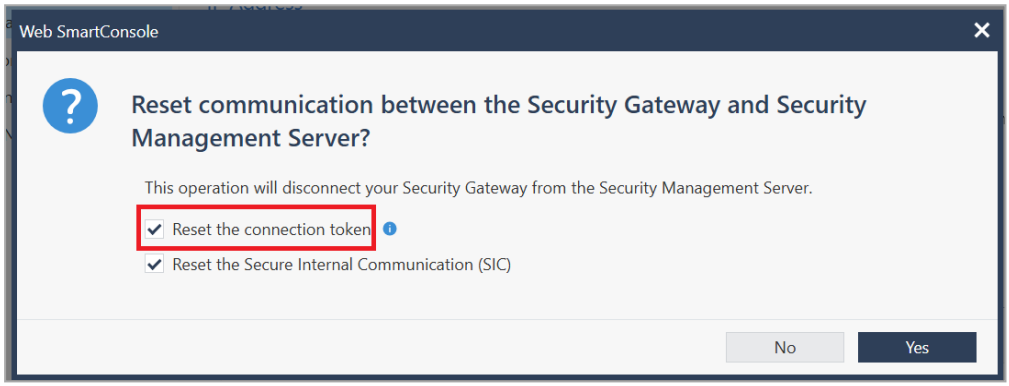
    Note - Connecting CloudGuard Security Gateway is supported across all major public cloud providers (AWS, Azure, GCP).

Important - To regenerate the token, follow these steps:

1. Double-click the Security Gateway which connection token you need to reset.
2. Click **Options** > **Reset communication**.



3. Select **Reset the connection token**.

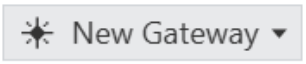


4. Click **Yes**.

Connecting a Cluster

Procedure

For on-premises Security Cluster:

1. From the left navigation panel, click **Gateways & Servers**.
2. Click the **New** icon or a 

button and select **Cluster...**.

   The **Check Point Cluster** window opens.

   Note - Web SmartConsole supports configuration of a Security Gateway/Cluster object for Gaia OS versions R80.10 and higher.
3. Fill in the required fields:
   - **Enter Name**: The Cluster name.
   - **IP address**: The Cluster VIP IP address.

4. Click **Add...** next to **Member ID 1**.

   The **Check Point Cluster Member** window opens.

   a. Enter the name and IP address of **Member ID 1**.

   Notes:
   - **Automatic IPv4 address**: The Security Gateway's IP address is set to an internal IP address used for cloud communication over an outbound tunnel.
   - **Custom IPv4 address**: Configure a static IP address if it is not an SD-WAN Gateway.

   b. Click **Connect**in the **Secure Internal Communication** section.

   The **Connect Device** window opens.

   c. In the Security Gateway section, select the Cluster Gateway type.

   d. Follow the on-screen instructions to connect the Cluster member to the Smart-1 Cloud management.

   e. When the **Connection Status** changes to **Connected**, click **Next**.

   f. To establish Secure Internal Communication (SIC) between the Cluster member and Smart-1 Cloud, enter the one-time password you set on the Cluster member.

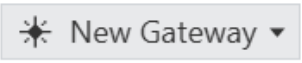
   g. Click **Next** and wait until the Cluster member connection process finishes. Then close the **Connect Device** window.

5. Click **Add...** next to **Member ID 2**.

   Follow steps 4.a-4.g again for this member.

6. Navigate to the **Network Management** tab.
7. Click **Get Interfaces** > **Get Interfaces With Topology**.
8. Click the **MaaS Tunnel interface**, and in **General** > **Network Type** section, select **Private**.
9. On the same MaaS Tunnel settings page, in **Advanced** > **Monitoring** section, make sure the **Monitored Interface** checkbox is cleared.
10. Finalize the topology definitions for the cluster.
11. Install the policy.

For CloudGuard Network Security Cluster:

1. From the left navigation panel, click **Gateways & Servers**.
2. Click the **New** icon or a 

button and select **Cluster...**.

   The **Check Point Cluster** window opens.

   Note - Web SmartConsole supports configuration of a Security Gateway/Cluster object for Gaia OS versions R80.10 and higher.
3. Fill in the required fields:
   - **Enter Name**: The Cluster name.
   - **IP address**: The Cluster VIP IP address.
4. Click **Add...** next to **Member ID 1**.

   The **Check Point Cluster Member** window opens.
   a. Enter the name and IP address of Member ID 1.

      Note:
      - **Automatic IPv4 address**: The Security Gateway's IP address is set to an internal IP address used for cloud communication over an outbound tunnel.
      - **Custom IPv4 address**: Configure a static IP address if it is not an SD-WAN Gateway.

   b. Click **Connect** below the Secure Internal Communication.

      The **Connect Device** window opens.

   c. Select **Appliance/Open Server** in the **Cluster Gateway type**.

   d. Copy the **Token** from the Connect Device screen.
5. Click **Add...** next to **Member ID 2**.

   Follow steps 4.a-4.d again for this member.
6. In the Security Cluster deployment template:
   a. Paste the Tokens you copied from the Smart-1 Cloud portal for each member into the appropriate fields.

   b. Fill in all remaining fields in the template and start the deployment.

c. When the CloudGuard Network Security Gateway deployment completes:

i. A tunnel is established between the Security Gateway and the Smart-1 Cloud.

ii. The status of the Security Gateway changes to Pending trust (SIC) establishment.

7. In SmartConsole or Streamed SmartConsole:

Follow the administration guide specific to your deployed solution to configure the Cluster object and Cluster members in SmartConsole.

Notes:

- When you enter the Cluster Virtual IP address, do not use IP addresses from these subnets:
  - 100.64.x.x
  - 100.70.x.x
  - 100.71.x.x
  - 100.100.x.x
  - 100.101.x.x
- When you add cluster members to the cluster object, use the existing members created in step 1.

Onboarding a new Quantum appliance using Zero Touch deployment

Procedure

Follow these steps to deploy a new appliance in Zero Touch mode and configure it as a Security Gateway or Cluster Member.

1. Remove your new appliance from the shipping carton, connect the power cable, and turn on the appliance.
2. Wait for the light on one of the network interface ports to start blinking, then:

- **If you have a DHCP server:**

  Connect the network cable to the blinking interface port.

  Make sure this connection leads to the environment with a working DHCP server.

- **If you do not have a DHCP server:**

Configure an interface with the appropriate networking settings:

a. Connect to the command line on the appliance.

b. In Expert mode, disable Zero Touch DHCP:

```
/opt/CPzetc/bin/zetc_setlaunch 0
```

c. In Gaia Clish, configure the IP address:

```
set interface <Name of Interface> on
```

```
set interface <Name of Interface> ipv4-address <IPv4 Address> mask-length <Subnet Mask Length>
```

d. In Gaia Clish, configure the default route:

```
set static-route default nexthop gateway address 192.168.1.254 off
```

```
set static-route default nexthop gateway address <IPv4 Address> on
```

e. In Gaia Clish, configure DNS servers:

```
set dns primary <IPv4 Address>
```

```
set dns secondary <IPv4 Address>
```

```
set dns tertiary <IPv4 Address>
```

f. In Gaia Clish, save the configuration:

```
save config
```

g. Plug the network cable into the configured interface port.

3. Go to the **Connect Gateways** page in the Smart-1 Cloud portal.
4. Wait for your appliance to appear (this typically takes 2-3 minutes).

   Note - If your appliance does not appear, check the Service and Contract page.

5. Click on your appliance's card, enter the required information, and click **OK**.

   To replace an existing Security Gateway, click the arrow next to the **Configure Device** button.

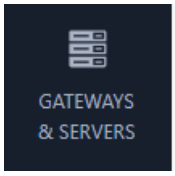
6. Follow the on-screen instructions in the portal.
7. After the card status changes to **Registration completed**, you can configure your new Security Gateway in SmartConsole.

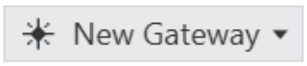
Connecting a Quantum Spark Appliance

Procedure

To connect Quantum Spark appliance to Smart-1 Cloud, follow these steps:

1. From the left navigation panel, click **Gateways & Servers**.

2. Click the **New** icon or a 

   button and select **Gateway...** or **Cluster...**.

   The **Check Point Gateway** properties window opens.

3. Fill in the required fields for the Check Point Security Gateway:

   a. **Enter name** - The name for the Security Gateway.

   b. **IP Address**

      - **Automatic IPv4 address**: The Security Gateway's IP address is set to an internal IP address used for cloud communication over an outbound tunnel.
      - **Custom IPv4 address**: Configure a static IP address if it is not an SD-WAN Gateway.

   You can configure the Security Gateway object in Smart-1 Cloud with a static IP address as the primary IP address (in the same way you configure a Security Gateway from an on-premises Security Management Server).

   When you configure the Security Gateway object with a Tunnel IP address, management traffic, control connections, and Smart-1 Cloud tenant communications use this main static IP address through the maas_tunnel interface.

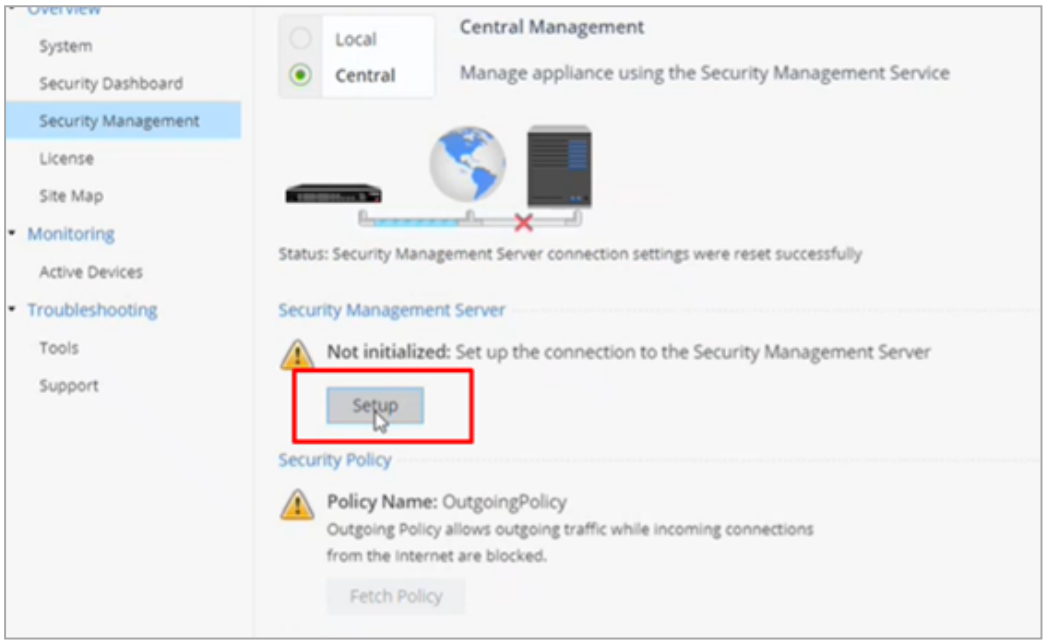
   Note - We recommend using a static IP address when available, unless configuring an SD-WAN Gateway.
   This simplifies configuration for features such as UserCheck, NAT rules, and VPN configuration.

4. Click **Connect** in the Device field.

   The **Connect Device** window opens.

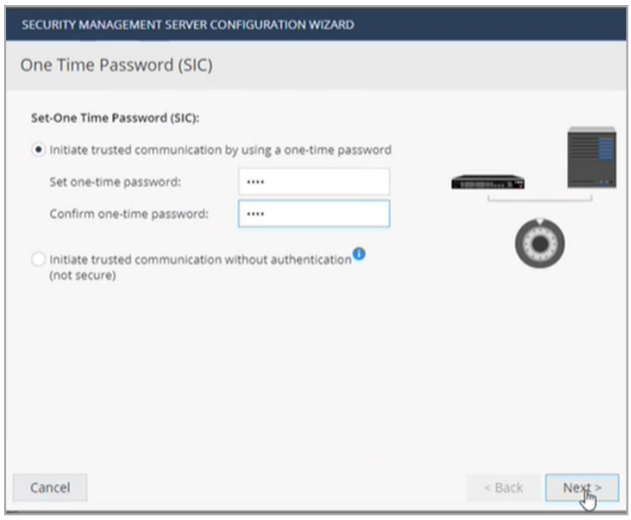
5. In the Security Gateway section, select **Quantum Spark**.

6. In the Connection preference section, select "Prepare the object now, connect the Security Gateway later". Click **Next**.
7. To establish trust between the Security Gateway and Smart-1 Cloud, configure the one-time password and enter it later on the Security Gateway. Click **Next**
8. Copy the authentication token to paste it later in the Security Management Server setup. Then close the **Connect Device** window.
9. Click **OK**.
10. Connect to the Quantum Spark WebUI, navigate to the Security Management tab, and click **Setup**.



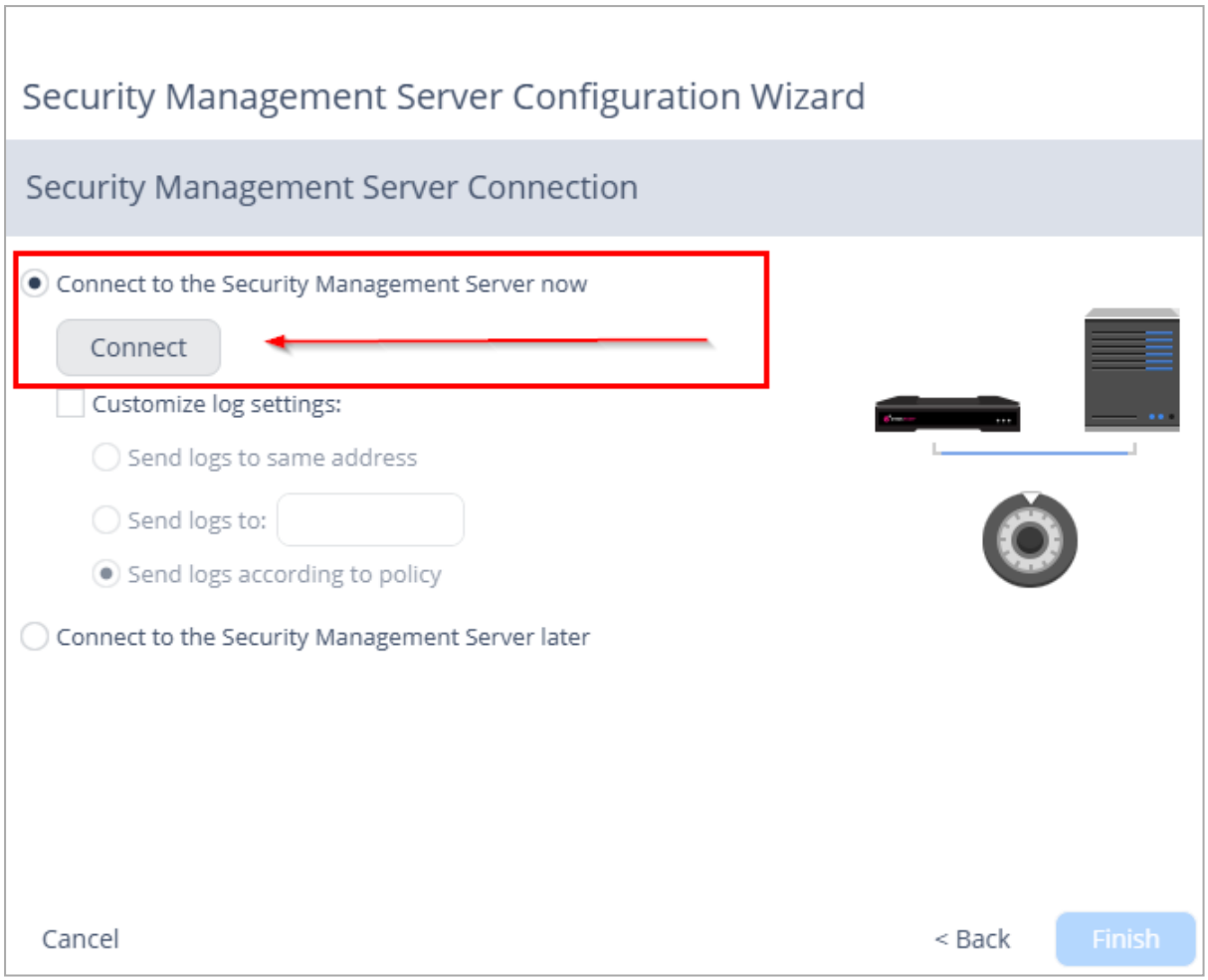
11. Select the **Use Security Management service** checkbox and click **Next**.
12. Click **Use the Infinity Portal to generate a new authentication token** and paste the token. Click Connect
13. Wait for the status to change to **Connected successfully to the Security Management Server**, then click **Next**.

14. Set the one-time password and click **Next**:



Important - Do not select the "Initiate trusted communication without authentication" option. Connecting an SMB device to Smart-1 Cloud without using the SIC password is not supported.

15. Check **Connect to the Security Management Server now** and click **Connect**.



Note - The following message will appear:
"Security Policy Installation: Trust is established with the Security Management Server. However, unable to fetch the Security Policy from the Management Server"
After the trust is established, you can continue with the process.

16. Click **Finish**.
17. Connect to the Smart-1 Cloud WebUI.
18. In **Gateways & Servers**, double-click the Quantum Spark device that was configured earlier. The device properties window opens.
19. Under **Network Management**, select **General**.
20. In the **Interfaces** menu, select **Get Interfaces with Topology**.
21. Once it is done, publish the changes and install the policy.

Connecting a Maestro Security Group

Important - This procedure supports only Maestro Security Groups that run R81.10 and higher versions.

Limitations

- Smart-1 Cloud does not support Maestro Security Groups in the VSX mode.
- The SMO Image Cloning is not supported if the Security Group R81.10 and higher contains different appliance models.
- DAIP is not supported.
- Automatic IP not supported with Maestro Security Group.

Procedure

1. On the Maestro Orchestrator, configure the required Security Group - in Gaia Portal or Gaia Clish.

   See the *Quantum Maestro Getting Started Guide* and the *Maestro Administration Guide* for your version.

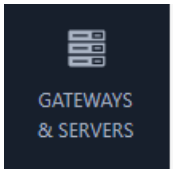
   Important - Write down the IP address of the Security Group. You must configure it later in Smart-1 Cloud.

2. Install the required Hotfixes on the Security Group: For details, refer to sk181495.
3. Connect to the Smart-1 Cloud Portal.

   See *"Getting Started with Smart-1 Cloud" on page 11*.

4. Add the Security Group as a new Security Gateway object:

   From the left navigation panel, click **Gateways & Servers**.

5. Click the **New** icon and select Gateway.

   The **Check Point Gateway** properties window opens.

6. Fill in the required fields for the Check Point Security Gateway:
    a. **Enter name** - The name for the Security Gateway.
    b. **IP Address** - In the IP address field, enter the IP address of the Security Group as you configured it on the Maestro Orchestrator (this is the IP address assigned to the **Mgmt** interface of the Security Group).
7. Click **Connect** in the Device field.

    The **Connect Device** window opens.
8. In the Security Gateway type drop-down, select **Appliance/Open Server**.
    a. Follow the on-screen instructions to connect your Security Group. The connection status is **Pending connection**, and when the Security Group connects to Smart-1 Cloud, the status change to **Connected**.
9. Click **Next** to close the Connect Device window.
10. Click **OK**.

Important Notes

- Before you add a **new**Security Group Member to the Security Group that is connected to Smart-1 Cloud (while the "`maas_tunnel`" is active and working), you must install the required Hotfixes on that Security Group Member.
- To examine the status of the Smart-1 Cloud connection on all Security Group Members:
  - In Gaia gClish:
    1. Connect to the command line on the Security Group.
    2. If your default shell is the Expert mode, go to Gaia gClish:

       ```
       gclish
       ```

    3. Run:

       ```
       show security-gateway cloud-mgmt-service
       ```

  - In the Expert mode:
    1. Connect to the command line on the Security Group.
    2. If your default shell is Gaia gClish, go to the Expert mode:

       ```
       expert
       ```

    3. Run:

       ```
       maas status
       ```

- To disable the Smart-1 Cloud connection on the Security Group:
  - In Gaia gClish:
    1. Connect to the command line on the Security Group.
    2. If your default shell is the Expert mode, go to Gaia gClish:

       ```
       gclish
       ```

    3. Run:

       ```
       set security-gateway cloud-mgmt-service off
       ```

  - In the Expert mode:
    1. Connect to the command line on the Security Group.
    2. If your default shell is Gaia gClish, go to the Expert mode:

       ```
       expert
       ```

    3. Run:

       ```
       maas off
       ```

- To enable the Smart-1 Cloud connection on the Security Group again:
  - In Gaia gClish:
    1. Connect to the command line on the Security Group.
    2. If your default shell is the Expert mode, go to Gaia gClish:

       ```
       gclish
       ```

    3. Run:

       ```
       set security-gateway cloud-mgmt-service on
       ```

  - In the Expert mode:
    1. Connect to the command line on the Security Group.
    2. If your default shell is Gaia gClish, go to the Expert mode:

       ```
       expert
       ```

    3. Run:

       ```
       maas on
       ```

Log in to SmartConsole from Smart-1 Cloud

Administrators can manage Smart-1 Cloud with one of these options:

- Web SmartConsole (browser-based)
- Streamed SmartConsole
- Desktop SmartConsole (Windows installation)
- Portable SmartConsole (no administrator rights required for Windows installation)

Note - Because of port tunneling limitations, you can only establish one connection to a Smart-1 Cloud tenant from a desktop SmartConsole on the same computer.
As an alternative, consider using Web SmartConsole or Streamed SmartConsole.

To access SmartConsole from a web browser

On the Smart-1 Cloud page, select **Settings** > **API & SmartConsole** > **Open Web SmartConsole**.

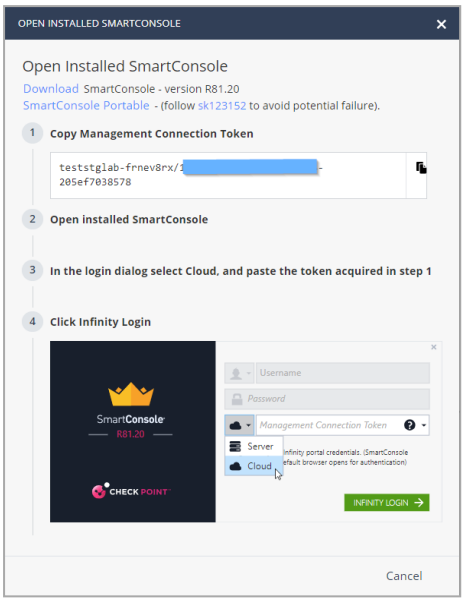
To access Streamed SmartConsole

On the Smart-1 Cloud page, select **Settings** > **API & SmartConsole** > **Open Streamed SmartConsole**.

The Streamed SmartConsole automatically opens.

To set up the desktop SmartConsole application

Go to **Settings** > **API & SmartConsole** > **Instructions for using Installed SmartConsole**.



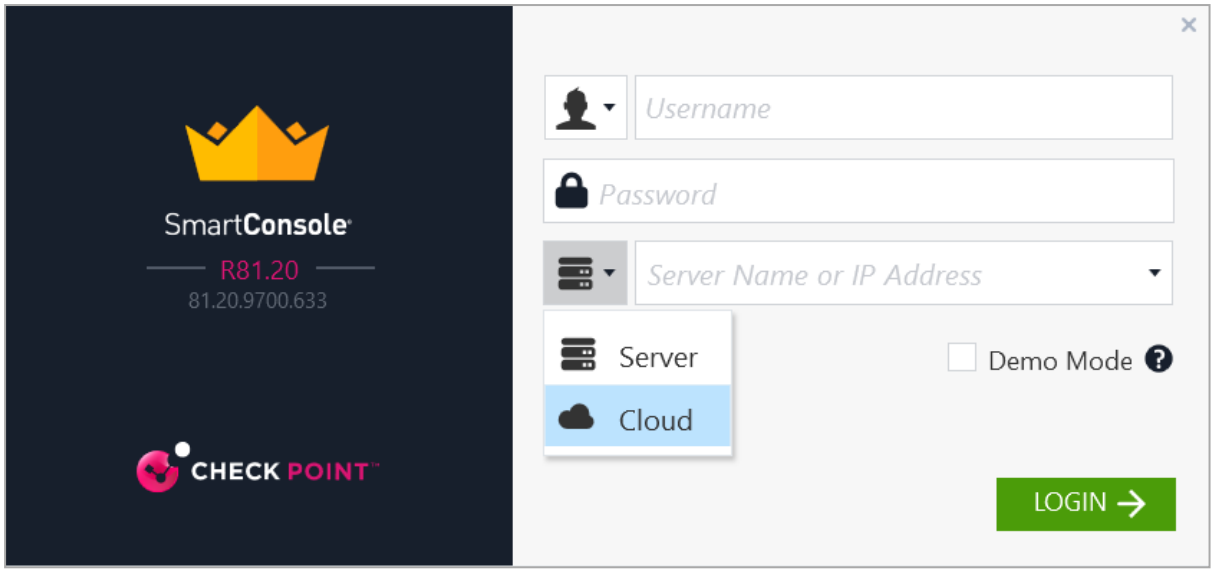
Note - SmartConsole is available as a Windows installer or as a Portable (ZIP) version.

1. Download SmartConsole from the **Open Installed SmartConsole** window.
2. Choose your preferred package:
   - **SmartConsole installation**.
   - **SmartConsole Portable** (for more information, refer to sk116158).
3. Install SmartConsole.

   If you downloaded the EXE file, double-click it and follow the on-screen instructions.

   If you downloaded the ZIP file, extract it. Refer to sk116158 for details.
4. Open SmartConsole.

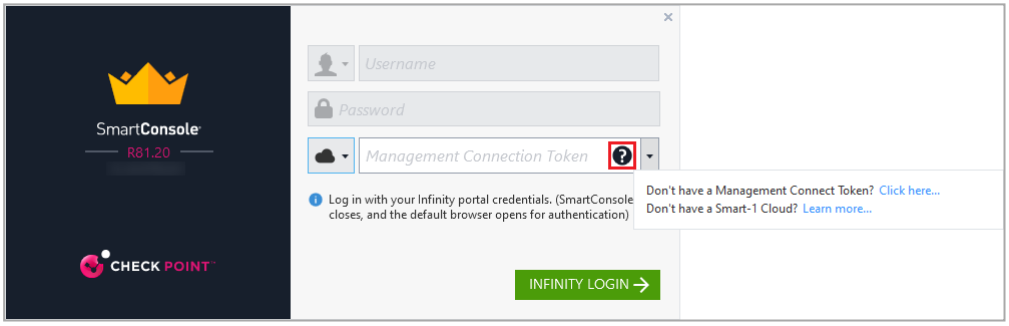
   See the R81.20 SmartConsole Online Help Guide for more information about how to use SmartConsole.
5. From the **server** drop-down menu, select **Cloud**.



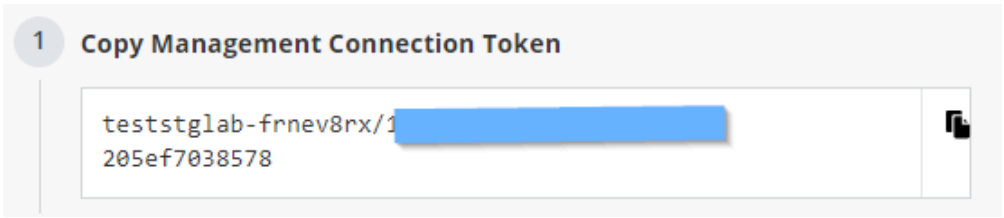
6. Enter the Management Connection Token.

Notes

- Hover over the help icon to view the relevant links:



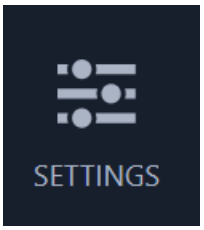
- Get the Management Connection Token from **Settings** view > **API & SmartConsole** > **Instructions for using Installed SmartConsole**.



7. Click **Infinity Login**.
8. SmartConsole closes and the default browser opens for authentication.
9. Enter your Infinity Portal administrator credentials (the login credentials for `portal.checkpoint.com`).
10. Click **Sign in** to authorize SmartConsole.

    SmartConsole opens for you to start working.

Using the Settings in Smart-1 Cloud



Use the Settings tab to learn how to use Management APIs, set the administrator's password, or migrate an on-premises Security Management Server to Smart-1 Cloud.

General

Note - You can interact with the Security Management Server through APIs to perform the same tasks available in SmartConsole, such as creating objects, defining Security Policies, and deploying configurations.

Service Information:

- **Status**: The current service status.
- **Service Identifier**: The unique service identifier based on the prefix provided during the service creation. When you contact Check Point, you must use this service identifier.
- **Version**: The current Security Management Server version.
- **License**: Shows "active" for the purchased Smart-1 Cloud license or "trial" for the evaluation license.
- **Expires**: Shows the number of days before license expiration.

API & SmartConsole

SmartConsole:

- Web SmartConsole
- Instructions for using Installed SmartConsole
- Streamed SmartConsole

To use the Management API settings

From the Smart-1 Cloud home page, select **Settings** > **API & SmartConsole**.

The Management API page shows the current web request structure.

To copy these details, click the clipboard button.

For additional information, see *Check Point Management API Reference*.

To restart your service

1. On the Smart-1 Cloud home page, go to **Settings** > **Advanced** > **Restart Service**.
2. Click **Restart Environment**.

   The **Restart Environment Confirmation** window opens.
3. Follow the instruction on the screen.
4. Click **Restart**.

Note - The **Restart Environment** function is equivalent to executing `cpstop` and `cpstart` commands in the on-premises management environment.

Migrate

You can migrate your self-hosted Security Management Server to the Smart-1 Cloud environment.

Note - The migration operation overwrites tenant information and does not merge existing tenant data.

Recommended option - Migrating a Self-Hosted (on-premises) Security Management environment already connected to Infinity Portal

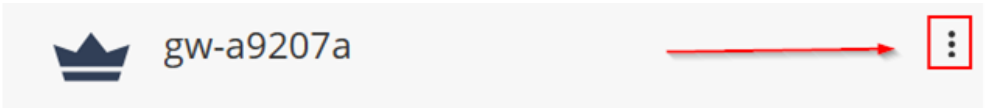
Note - To connect your Self-Hosted (on-premises) Security Management Server to Infinity Services:

1. In SmartConsole, click **Infinity Services**.
2. In the **Connect to Infinity Portal to use Infinity Services** section, click **Get Started** and follow the instructions.

For detailed instructions, see sk177205.

Important - You can migrate a Self-Hosted Security Management environment to Smart-1 Cloud only if Smart-1 Cloud has not been previously created in this Infinity Portal tenant.

1. Open the Infinity Portal tenant connected to the Self-Hosted Security Management environment.
2. Select the self-hosted Security Management Server you want to migrate.
3. Click the three-dot menu:



4. To make sure you can migrate this Security Management Server to Smart-1 Cloud, select **Run Pre-migrate verifier**.
5. Click **Migrate to Smart-1 Cloud**.

   Important - The migration process may take considerable time. The Smart-1 Cloud application will be unavailable during import. You will receive an email notification when the process completes and the service becomes available.

Notes:

- After migrating a Standalone environment, it is divided into separate Security Management Server and Security Gateway components. Post-migration, you must follow the procedure described in sk179444 - Migration from a Standalone environment to a Distributed environment. This change is permanent. Security Management Server and Security Gateway replace the Standalone.
- When migrating a Management High Availability environment to Smart-1 Cloud, you must remove the Secondary Management after migration (Management High Availability is not supported with Smart-1 Cloud).
- Multi-Domain Security Management and Log Server are not supported.

6. After successful migration, in Smart-1 Cloud, navigate to **Connect Gateway**.
7. Click the plus (**+**) icon below the existing Security Gateway. Then select the Security Gateway you want to connect and follow the on-screen instructions.
8. For a Security Gateway running a version lower than R80.40 with Jumbo Hotfix Accumulator Take 89, reset the Secure Internal Communication (SIC) before initializing communication from SmartConsole to the Security Gateway. For more information, see sk65764.

   Note - For Security Gateway/Security Management version R80.40 with Jumbo Hotfix Accumulator Take 89 and higher or Quantum Spark/Quantum Edge with version R80.20.40 and higher, SIC reset is not required on the Security Gateway.

Migrating a Self-Hosted (on-premises) Security Management environment that is not connected to Infinity Portal

You can import configurations from an on-premises Management Server to Smart-1 Cloud.

Migration to Smart-1 Cloud is supported starting from Security Management Server version R81.10.

To migrate an on-premises Security Management Server to Smart-1 Cloud:

1. On the Smart-1 Cloud home page in Infinity Portal, go to **Settings** > **Migrate**.
2. Below **Export Data**, click **Download** to download the migration tools.
3. On the on-premises Security Management, run the export tool.
4. Below **Import and Start**, click **Choose file** to upload the export file.
5. Click **Upload & Start** to start the migration process.

   Important - The migration process may take considerable time. During import, the Smart-1 Cloud application will be unavailable. You will receive an email notification when the process completes and the service becomes available.
6. After successful migration, in Smart-1 Cloud, navigate to **Connect Gateway**.

7. Click the plus (+) icon below the existing Security Gateway. Then select the Security Gateway you want to connect and follow the on-screen instructions.
8. For a Security Gateway running a version lower than R80.40 with Jumbo Hotfix Accumulator Take 89, reset the Secure Internal Communication (SIC) before initializing communication from SmartConsole to the Security Gateway. For more information, see sk65764.

   Note - For Security Gateway/Security Management version R80.40 with Jumbo Hotfix Accumulator Take 89 and higher or Quantum Spark/Quantum Edge with version R80.20.40 and higher, SIC reset is not required on the Security Gateway.

CloudGuard Network Configuration

Smart-1 Cloud lets administrators configure CloudGuard Network in the GUI.

Limitations:

- The GUI does not support the Oracle Cloud Infrastructure (OCI).

How to enable CloudGuard Network in Smart-1 Cloud

In the Quantum Smart-1 Cloud view in the Infinity portal, go to **Settings** > **Advanced** > **CloudGuard Network**.

Add an account

1. To add an account, on the corresponding cloud provider tile, click **Add account**.

   The **CME Account** window opens.
2. Give the account a name.
3. In the **Platform** drop-down list, select AWS, GCP, or Azure.
4. Enter the parameters.
5. Click **OK** to save the changes.

Parameters for AWS

Parameter	Description
Access Key ID	AWS Access Key ID. This parameter is mandatory.
Secret Access Key	AWS Secret Key. This parameter is mandatory.
Role Authentication (IAM)	This option is available only in on-premises Security Management Serverdeployments. It is not available in Smart-1 Cloud.

Parameter	Description
Regions	The AWS regions in which the Security Gateways are being deployed.
STS Role	The Amazon Resource Name (ARN) of an IAM role to assume.
STS External ID	An optional STS External ID to use when assuming an IAM role in the account.
Scan Gateway Load Balancer subnets	Enable to scan Gateway Load Balancer subnets.
Synchronize VPN	Enable to synchronize VPN.
Sub Accounts	Add new sub accounts or configure properties of existing sub accounts. The sub-account name must be unique. Enter STS Role or STS External ID.

Parameters for Azure

Parameter	Description
Application ID	The service principal's application ID in UUID format.
Client Secret	The service principal's client secret value.
Directory ID	The service principal's Directory ID in UUID format.
Subscription ID	The subscription ID where the VMSS resides in UUID format.
Azure Environment	Select the environment in the drop-down list. The default value is "Azure Cloud".

Parameters for GCP

Parameter	Description
Service Account Key Authentication	Download a public service account key file in JSON format.

Edit an account

1. To edit an account, click the **Edit** button at the right, above the cloud provider tiles.

   The **CME Overview** window opens.

2. In the **Accounts** table, select the account you want to edit and click the "pencil" icon in the toolbar above the table.

   The **CME Account** window opens.

3. Edit the parameters.

4. Click **OK** to save the changes.

Add a Security Gateway configuration template

1. To add a Security Gateway configuration template to the account, on the corresponding cloud provider tile, click **Add template**.

   The **CME Template** window opens.

2. Give the Security Gateway configuration template a **name**.

3. In the **Gateway Settings** section, in the **Account** drop-down list, select the applicable **Account**.

4. Select the Security Gateway version.

5. Enter a one-time password.

6. Confirm the one-time password.

7. On the **Network Security** and **Threat Prevention** tabs, select the checkboxes for the blades you want to enable on the Security Gateway.

8. In the **CME Attributes** section, select the policy to install on the Security Gateway.

Note - To add support for AWS Transit Gateways to the AWS account, configure the below parameters in the **CME Attributes** section.

Parameters for AWS Transit Gateway

Parameter	Description
VPN Domain	A VPN Domain.
VPN Community	A VPN Star community where the VPN Gateway is the center.
TGW Static Routes	Enter network addresses (CIDR) to create a static route on each Gateway of the Transit Gateway auto-scaling group.
TGW Static Spokes	Spoke CIDR is learned from the TGW over BGP and is re-advertised by the Gateways of the TGW auto-scaling group to the AWS TGW.

For more information on AWS Transit Gateway, refer to CloudGuard Network for AWS Transit Gateway Deployment Guide.

Note - To add IPv6 support to the Azure account, select the **IPv6** checkbox in the **CME Attributes** section.

9. Provide the repository script name and parameters if necessary.
10. In the **Logs** section, add log servers.
11. In the **NAT** section, select which settings to use for communication with the Security Management Server or log servers when they are behind NAT or in the public cloud.

    Note - This section is enabled only for the R82 version of Security Gateway.

12. Click **OK** to save the changes.

Edit a Security Gateway configuration template

1. To edit a Security Gateway configuration template, click the **Edit** button at the right, above the cloud provider tiles.

   The **CME Overview** window opens.

2. In the **Accounts** table, select the account which templates you want to edit.
3. In the **Gateway Templates** table, select the template you want to edit and click the "pencil" icon in the toolbar above the table.

The **CME Template** window opens.

4. Edit the parameters.
5. Click **OK** to save the changes.

Advanced settings

To open the Advanced Settings window, click the **Advanced** link at the right, above the cloud provider tiles. In this section, you can:

- Change the Security Management Server name.
- Change the Delay Cycle value (the waiting time after each poll cycle).
- Download logs with information about CME operations and API calls.

Forwarding Events to SIEM

Event forwarding is an easy and secure procedure to export logs. You can forward logs, events, and saved applications data from the Check Point environment to a Syslog server or a SIEM (Security Information and Event Management) provider such as Splunk, QRadar, or ArcSight. These SIEM providers process large amounts of data and then display it on dashboards for analysis or send notifications.

Forward to SIEM configuration

To access the **Forward to SIEM Configuration**, from the Smart-1 Cloud home page, select **Settings** > **Advanced** > **Forward to SIEM**.

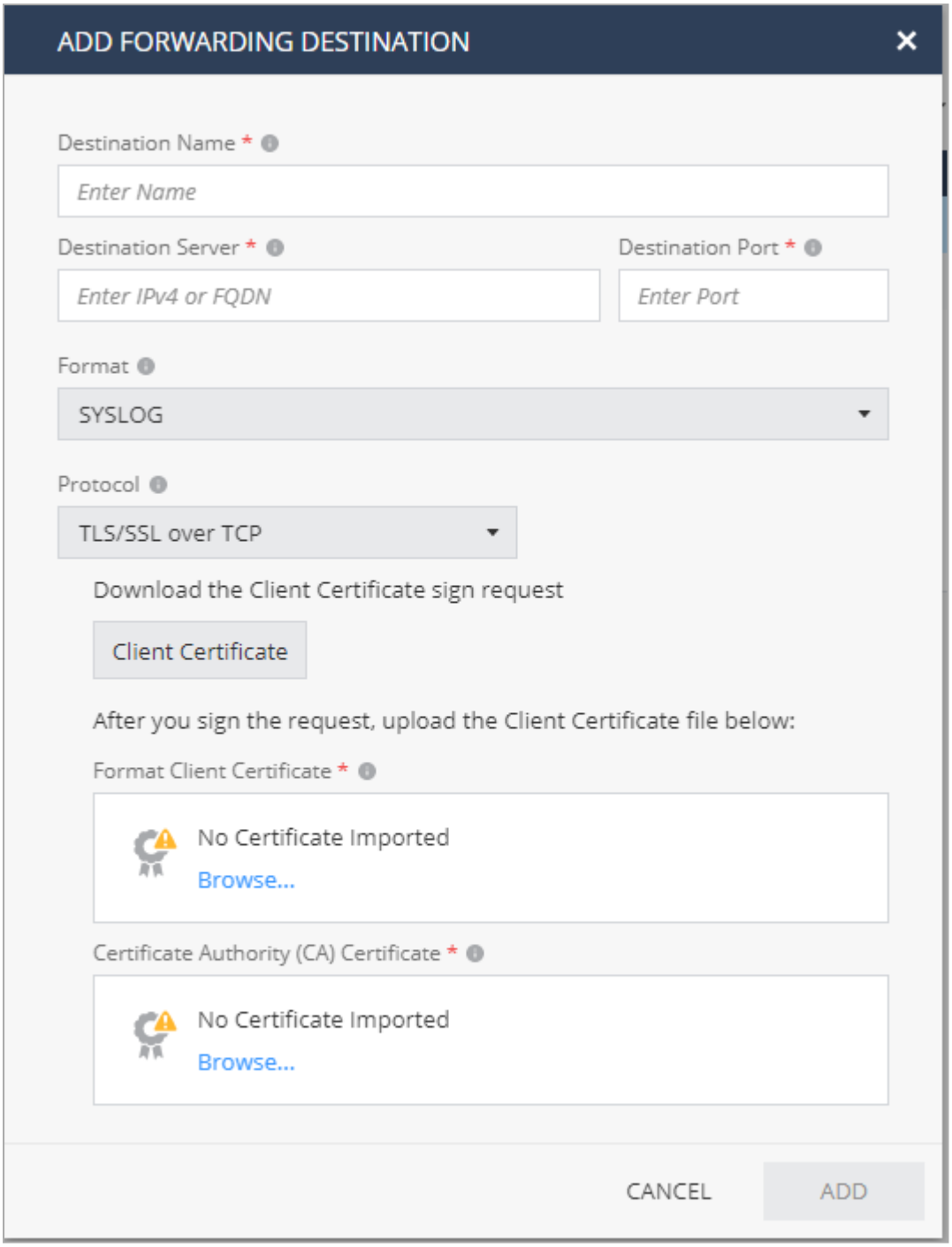
In the configuration page you see a table with forward to SIEM destinations, and information for the destination, such as status, encryption, name, target port, protocol and format.

Adding a new destination

To add a new destination, on the Forward to SIEM Configuration screen, click **New**.

Note - It is currently supported to add up to 3 destinations.

The **Add Forwarding Destination** window opens.



- **Destination name**: Enter a unique name for the destination.
- **Destination Server**: Enter IP address or FQDN.

  Note - The IP address must be public.

- **Destination Port**: The destination port number.
- **Format**: The destination log format. Can be Syslog, CEF, JSON, Splunk, LEEF, Generic,

LogRhythm, or RSA.

- **Protocol**: The destination protocol, can be either TLS over TCP, TCP, or UDP

TLS/SSL over TCP Configuration

It is recommended to export logs over an encrypted connection using the TLS protocol. When using TLS, it is important to know that only mutual authentication is allowed. For mutual authentication, you need these two certificates:

- The Certificate Authority (CA) certificate (in PEM format) that signs both the client (Smart-1 Cloud side) and the server (SIEM side) certificates. The CA certificate can be a self-signed certificate.
- Client certificate.

Procedure:

- Click the **Client Certificate** box to download the Client certificate sign request (cp_client.csr).

  Note - Signing the request is done in your organization and is not part of Smart-1 Cloud services.

- After you sign the request, click **Browse** below the Client Certificate box to upload the signed certificate.

  Important - If it takes time to obtain the signed certificate for upload, you can close the Add Forwarding Destination window. Open it again later when you have the signed certificate, fill in all the details, and just click **Browse** to upload the certificate.
  You do not need to click the Client Certificate box again, because this will create a new sign request.

- Upload the CA certificate.

Edit the destination

To edit the destination, on the Forward to SIEM page, select a destination and click **Edit**.

You can change all destination properties except for the destination name.

Delete the destination

To delete a destination, on the Forward to SIEM page, select a destination and click: **Delete**.

Write **confirm** in the deletion dialog box.

Start, stop, or restart the destination

To start, stop, or restart sending logs to the destination, on the Forward to SIEM page, select a destination, click **More Actions**, and select the action you want to perform:

- Stop Forwarding - Stop sending logs to the destination
- Start Forwarding - Start sending logs to the destination
- Restart Forwarding - Restart sending logs to the destination

Troubleshooting

If no logs arrive to your SIEM, follow these steps:

Important - For information and updates on Smart-1 Cloud external FQDNs and their associated IP addresses, see sk182699.

- Make sure that your Security Gateway does not block traffic from the Smart-1 Cloud public FQDN:
  - **Ireland**: `eu-west-1.allowed-ips.checkpoint.com`
  - **London**: `eu-west-2.allowed-ips.checkpoint.com`
  - **N. Virginia**: `us-east-1.allowed-ips.checkpoint.com`
  - **Sydney**: `ap-southeast-2.allowed-ips.checkpoint.com`
  - **Mumbai**: `ap-south-1.allowed-ips.checkpoint.com`
- Check if all the details in the configuration are correct.
- If you use TLS, make sure you are using the correct certificates.
- Restart the destination.

If the issue persist, contact Check Point support and open a Service Request.

Smart-1 Cloud Advanced Configuration

Use these commands on the Security Gateway to see the communication status and clear the communication between the Security Gateway and the Smart-1 Cloud service.

Smart-1 Cloud Gateway Commands

Description	Gaia R81 and higher	Gaia R80.40	Gaia R80.30 and lower	Gaia Embedded
Opens the communication between the Security Gateway and the service. This command creates a HTTPS tunnel between the Security Gateway and the Smart-1 Cloud service. All communication between the Security Gateway and the Cloud management runs on top of this tunnel.	`set security-gateway cloud-mgmt-service on auth-token <Auth-Token>`	`set security-gateway maas on auth-token <Auth-Token>`	`maas on --auth-token <Auth-Token>`	▪ `connect maas auth-token <Auth-Token>` ▪ `set maas mode enable`
Shows the communication status with the service. Show the status of the HTTPS tunnel between the Security Gateway and the service.	`show security-gateway cloud-mgmt-service`	`show security-gateway maas`	`maas status`	`show maas`
Run this command to disconnect the Security Gateway and stop the Smart-1 Cloud management.	`set security-gateway cloud-mgmt-service off`	`set security-gateway maas off`	`maas off`	`set maas mode disable`

How to Connect a Security Gateway Behind a NAT/Proxy or Third-Party Security Gateway

In Smart-1 Cloud, the Security Gateway opens a HTTPS tunnel to the service. Smart-1 Cloud can open A Secure Internal Communication (SIC) to the Security Gateway when the tunnel is finished and operational.

You must allow outbound HTTPS traffic to FQDN listed below to allow the communication between the Security Gateway and the service:

- To your domain at Smart-1 Cloud:

  `<Service-Identifier>.maas.checkpoint.com`

- For Smart-1 Cloud deployments in Europe:

  `cloudinfra-gw.portal.checkpoint.com`

- For Smart-1 Cloud deployments in the United States:

  `cloudinfra-gw-us.portal.checkpoint.com`

- For Smart-1 Cloud deployments in the APAC:

  `https://cloudinfra-gw.ap.portal.checkpoint.com`

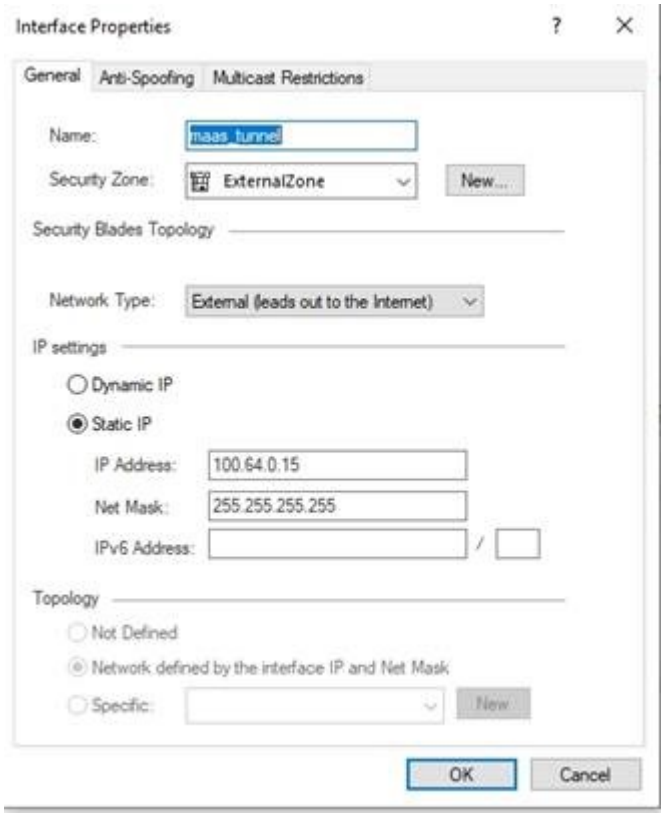
How to Connect a Quantum Spark Appliance with a Dynamic IP

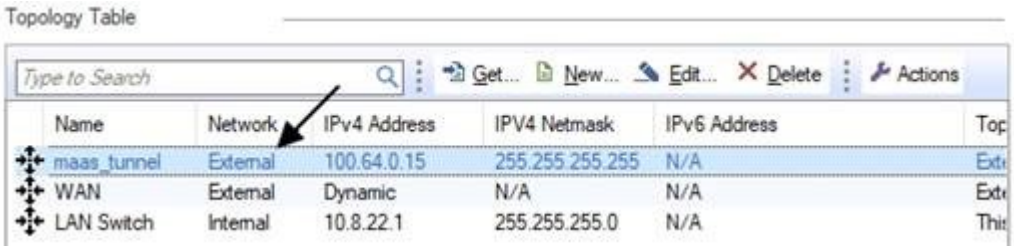
To connect a Quantum Spark Appliance with a Dynamic IP:

1. In the Infinity Portal, connect the Security Gateways to the service.
2. In SmartConsole, navigate to **Gateways & Servers**.
3. Open the Security Gateway object > change the **Hardware** (below **Platform**) to the applicable model (for example, **1590 Appliances**).
4. Below **General Properties** > select the check box **Dynamic Address**.
5. When the SmartConsole notification says "Changing the gateway to Dynamic Address will reset the portals on the gateway", click **Yes**.
6. Click **Yes** when the SmartConsole notification says:

   "`Selecting Dynamic Address option will remove your selection in the Check Point Software Blades list. Change Version to the latest, reset traditional mod IKE properties, reset VPN link selection properties and will remove NAT Definition.`"
7. Start SIC > based on "First to connect."
8. Publish the SmartConsole session.
9. Open the Security Gateway object.
10. Navigate to **Topology**.

11. Manually add the "`maas_tunnel`" interface with the automatic generated Security Gateway IP address (100.64.0.X) and Net Mask (255.255.255.255):





12. In the Quantum Spark Appliance's WebUI, click **Security Management Server** > **Connect SIC Menu** > **Re-Enter SIC password** (if it does not exist already) > **Connect to Management Server**.
13. In the Quantum Spark Appliance's WebUI, click **Fetch policy**.

How to Configure the Query Settings in SmartConsole

1. From the left navigation panel, click **Logs & Monitor** > **Logs**.
2. To the right of the query field, click **Options** > **Tools** > **Query Settings**.
3. In the **Query Settings** window, configure the applicable settings.
4. Click **OK**.

For more information, see the *Logging and Monitoring Administration Guide* for your version.

How to Connect a Local Active Directory to Smart-1 Cloud

Smart-1 Cloud customers that want to use their local AD server in their Identity Awareness configuration must configure the gateway as proxy for the cloud management.

To connect your local AD server to Smart-1 Cloud:

1. In the Streamed SmartConsole > **Objects** window on the right click **New** > **Host**, and create a host for your Domain Controller.
2. Create LDAP Account Unit: Click **New** > **More** > **User/Identity** > **LDAP Account Unit**.
3. On the LDAP Account Unit **Servers** tab, add a LDAP server.
4. On the **Object Management** tab > **Server to connect** field > Select the host object you created for the Domain Controller.
5. Manually add the branch(es).

   Fetching branches is not supported, it is necessary to add them manually.

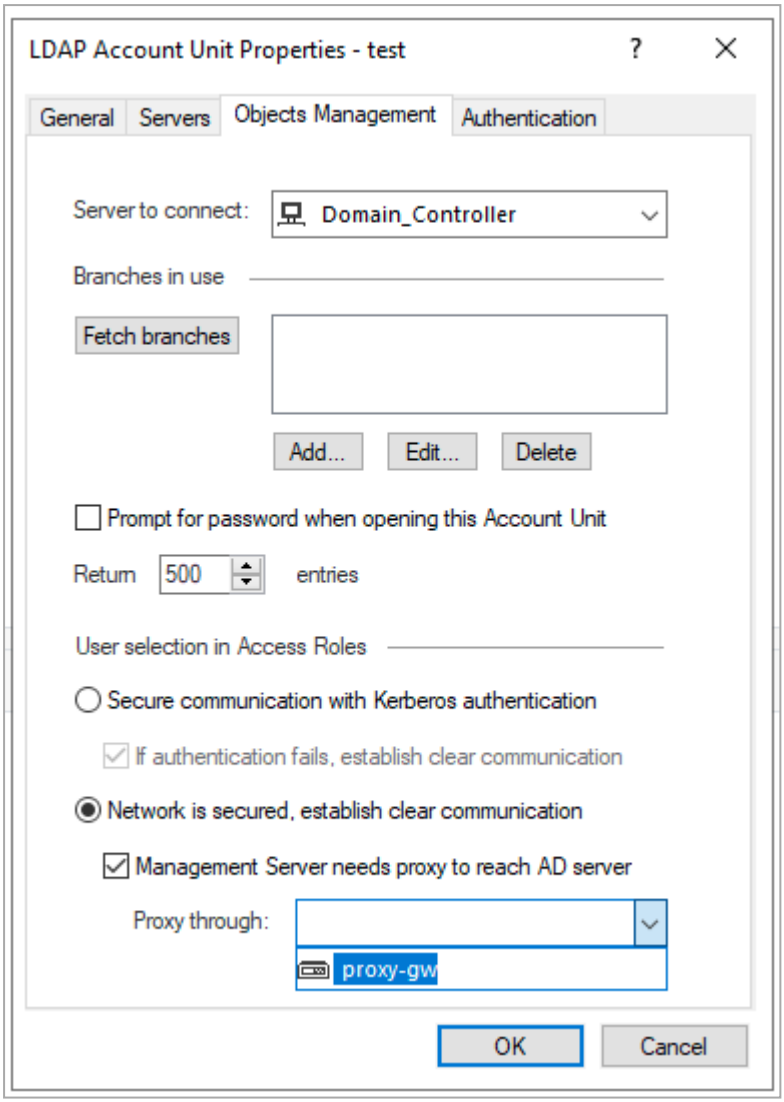
   The branch name is the suffix of the Login DN that begins with `DC=`.

   Example:

   If the Login DN is: `CN=John.Smith,CN=Users,DC=mycompany,DC=com`

   then the branch name is: `DC=mycompany,DC=com`
6. Select **Management Server needs proxy to reach AD server**.

7. In the **Proxy through** field, select the Security Gateway / Security Cluster that has a route to your AD server.



Important - Notes about the Identity Awareness Gateway as Active Directory Proxy feature:

- This feature operates only with Microsoft Active Directory.
- This feature supports only the user picker in the Access Role object. Other settings, such as Identity Awareness Configuration wizard, Client certificate, Legacy user picker, Fetch branches, Fetch fingerprint, and LDAP tree are not supported.
- This feature operates only with Security Gateway R80.20 and higher running Gaia OS.
- This feature operates only with Quantum Spark appliances R80.20.00 and higher running Gaia Embedded OS (see the *Quantum Spark Appliances Centrally Managed Administration Guide* for your version (*2000 models*, *19000 models*, *1800 models*, *1600 models*, *1500 models*)).
- This feature does **not** support DAIP gateways or Externally managed gateways.
- Available communication types:
  - **Clear** - Communication between the Security Management Server and the Security Gateway is encrypted by SIC. But the communication from the Security Gateway to the Active Directory server is not encrypted.
  - **SSL** - Active Directory domain controller needs to allow SSL.
- Required Active Directory permissions for the account used to configure the Account Unit:
- For user picker functionality, the account must have permission to do LDAP queries.
  - For Security Gateway functionality - depends on the identity sources that are used on the Security Gateway.
  - To get identities with the Active Directory Query, without use of domain admin credentials, refer to sk93938.

Important -Identity Logging is not supported in Smart-1 Cloud.

How to Configure Access to Security Gateway Gaia Portal

The IP address in the Security Gateway object represents the interface between the Security Gateway and the service.

This IP address is internal (private) and you cannot use it on the Internet.

Note - If a Security Gateway object is created with a static IP address, access to the Security Gateway Gaia Portal is allowed without any change.

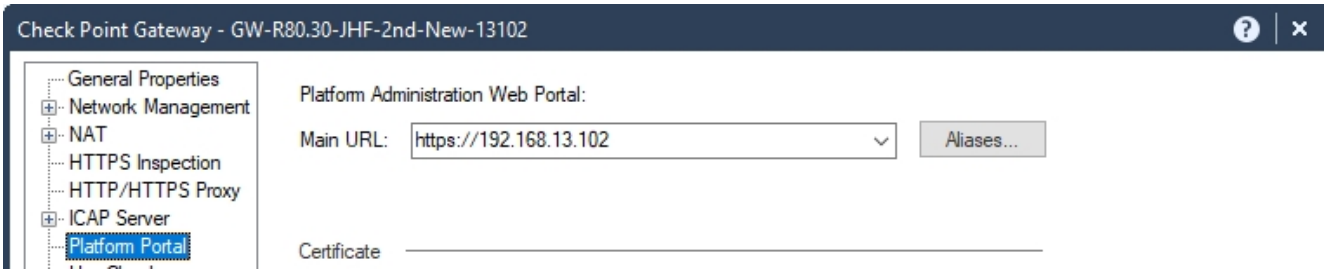
To allow access to the Security Gateway Gaia Portal:

1. In SmartConsole, navigate to **Gateways & Servers**.
2. Open the Security Gateway object.
3. From the left tree, click **Platform Portal**.
4. Change the primary URL to the Security Gateway IP address used for Gaia login.
5. Publish the SmartConsole session.
6. Install the Access Control policy.

Example:

The displayed Gateway IP address is the MaaS tunnel IP address.

Change the **Platform Portal** IP address to the Security Gateway IP address used for the Gaia login.



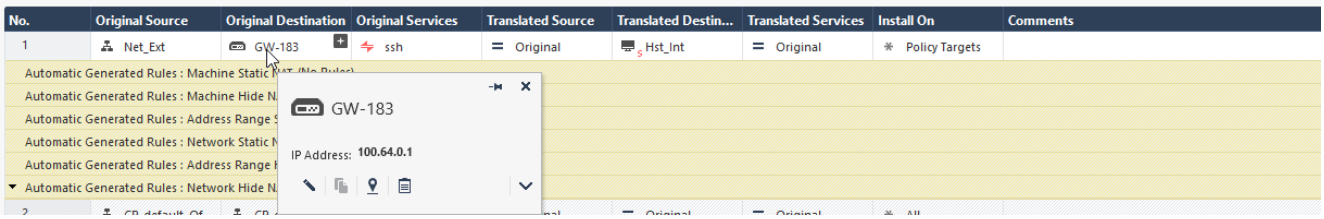
How to Configure Access from the Security Gateway External IP Address to the Internal Asset with Static NAT

Smart-1 Cloud uses the Security Gateway object's primary IP address for the tunnel communication between the Security Gateway and the service in cloud. It is a virtual interface.

Note - When configuring NAT rules, standard settings are available if the Security Gateway object is created with a static IP address.

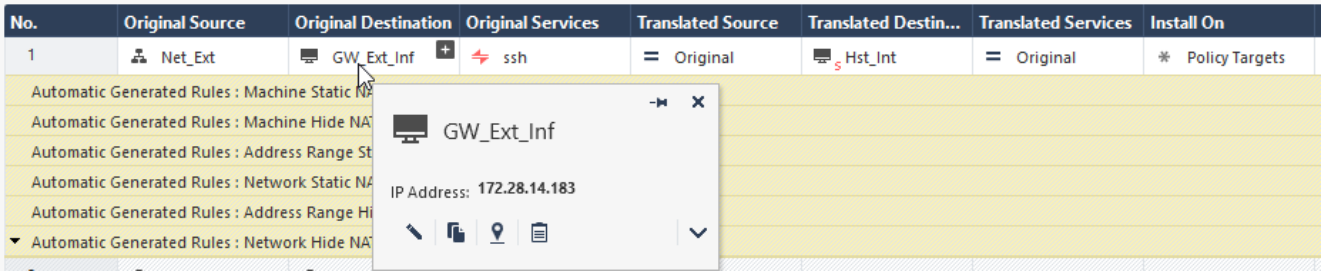
Consequently, the destination IP address of this rule is actually a virtual tunnel IP address, and not the Security Gateway's physical external interface.

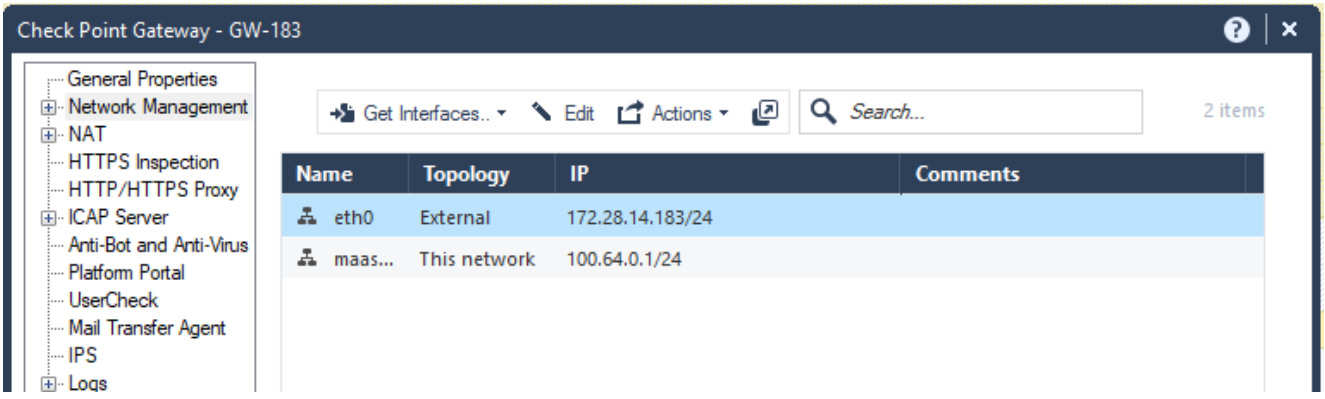
This screenshot shows the IP address in the tooltip:



To configure access **from** the Security Gateway's External IP address **to** the Internal Asset with NAT Policy, a static rule in Smart-1 Cloud, you must create a dummy object with the physical IP address of the Security Gateway. You then use it in the NAT rule.

In this screenshot, the dummy Host object ("GW_Ext_int") that contains the Security Gateway's physical IP address, replaces the Security Gateway object ("GW-183").





How to Configure IP Address Selection by Remote VPN Peer

There are some methods that can determine how remote peers resolve the IP address of the local Security Gateway.

Configure these settings in **Security Gateway Properties** > **IPsec VPN** > **Link Selection**.

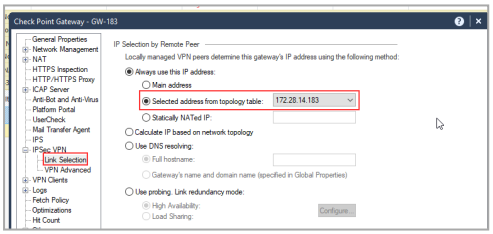
Note - If you create the Security Gateway object with a static IP address and not with the tunnel IP, link selection is not required. You can use the standard settings for VPN configuration on the Security Gateway.
We recommend configuring in Smart-1 Cloud a static IP address in the Security Gateway object for VPN configuration.

Smart-1 Cloud uses the Security Gateway object's primary IP address for the tunnel communication between the Security Gateway and our service in cloud. It is a virtual interface.

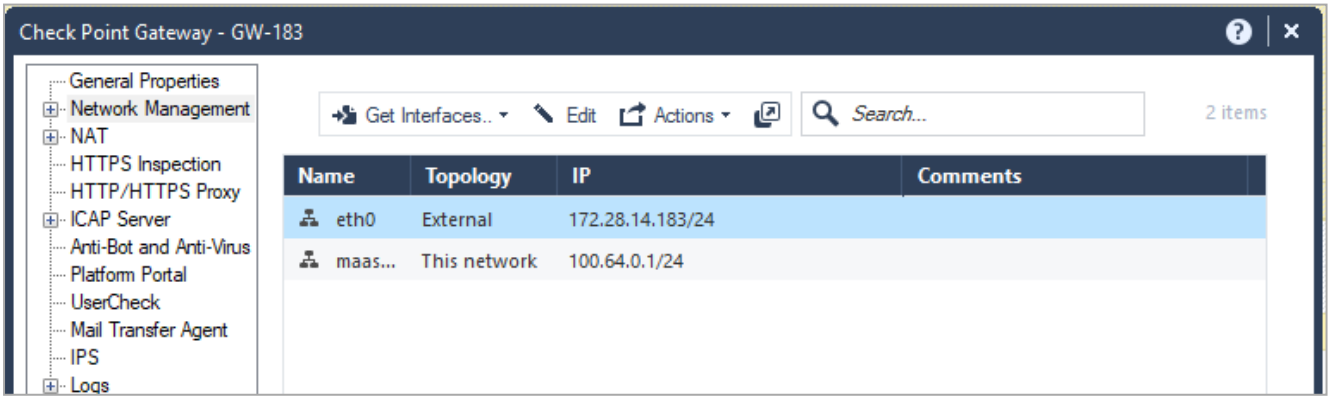
Consequently, you cannot use the **Main address** option.

As an alternative, use one of these options to select an address from topology table:

Option 1:



Option: 2



Smart-1 Cloud Configuration for Site-to-Site VPN

When you configure a Site-to-Site VPN between two gateways, the VPN status can show as "down".

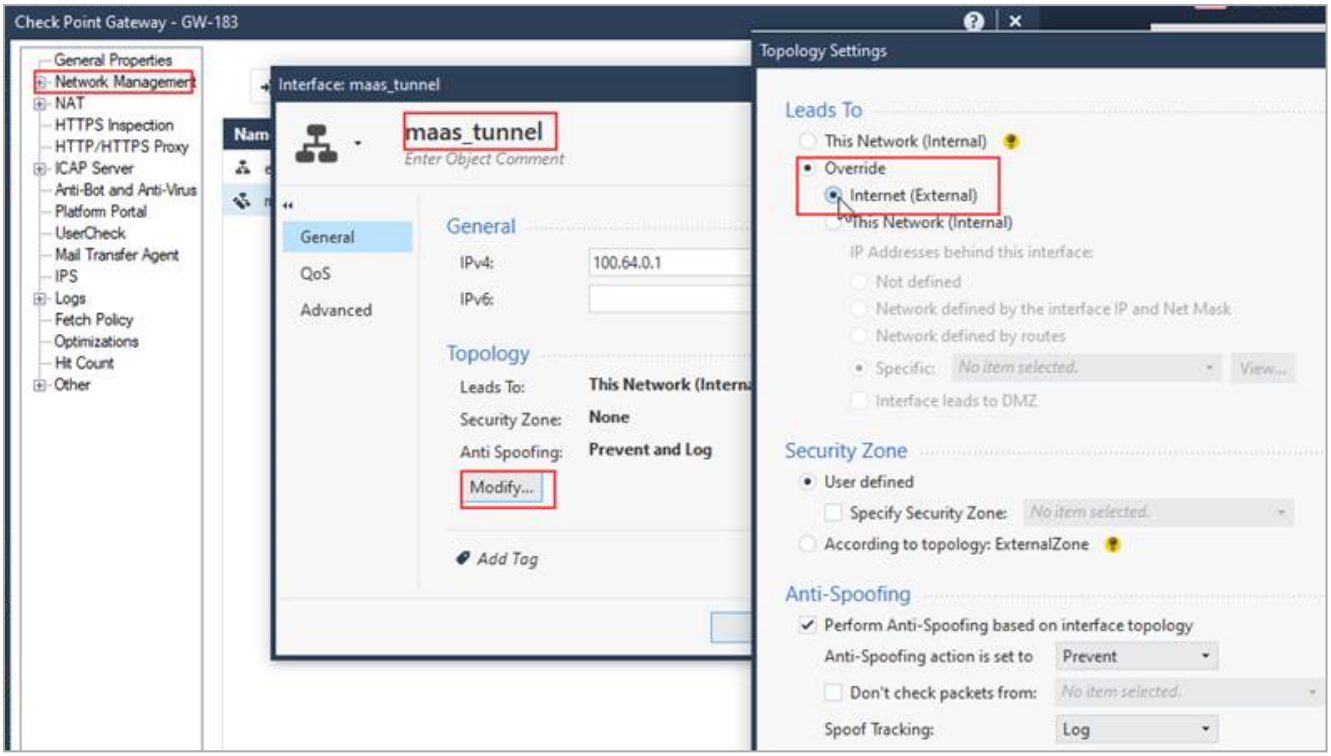
To resolve this issue, it is necessary to configure the topology of the `maas_tunnel` interface as" **Internet (External)**."

Note - You require this configuration only when you have Site-to-Site VPN between two Security Gateways (not clusters).

To configure a Site-to-Site VPN in SmartConsole:

1. From the left navigation panel, click **Gateways & Servers**.
2. Open the Security Gateway object.
3. Navigate to **Network Management**.
4. Select the **maas_tunnel** interface > click **Edit**.
5. On the general page, click **Modify**.
6. Select **Override** > **Internet (External)**.
7. Click **OK**.
8. Run steps 2-7 again for all Security Gateways in the Site-to-Site VPN.
9. Install the Access Control policy on all applicable Security Gateways.

Example:


Check Point Gateway - GW-183
General Properties
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
ICAP Server
Anti-Bot and Anti-Virus
Platform Portal
UserCheck
Mail Transfer Agent
IPS
Logs
Fetch Policy
Optimizations
Hit Count
Other
Interface: maas_tunnel
maas_tunnel
Enter Object Comment
General
QoS
Advanced
General
IPv4:
100.64.0.1
IPv6:
Topology
Leads To:
This Network (Interna
Security Zone:
None
Anti Spoofing:
Prevent and Log
Modify...
Add Tag
Topology Settings
Leads To
This Network (Internal)
Override
Internet (External)
This Network (Internal)
IP Addresses behind this interface:
Not defined
Network defined by the interface IP and Net Mask
Network defined by routes
Specific:
No item selected.
View...
Interface leads to DMZ
Security Zone
User defined
Specify Security Zone:
No item selected.
According to topology: ExternalZone
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
Anti-Spoofing action is set to
Prevent
Don't check packets from:
No item selected.
Spoof Tracking:
Log

General Capabilities of Smart-1 Cloud

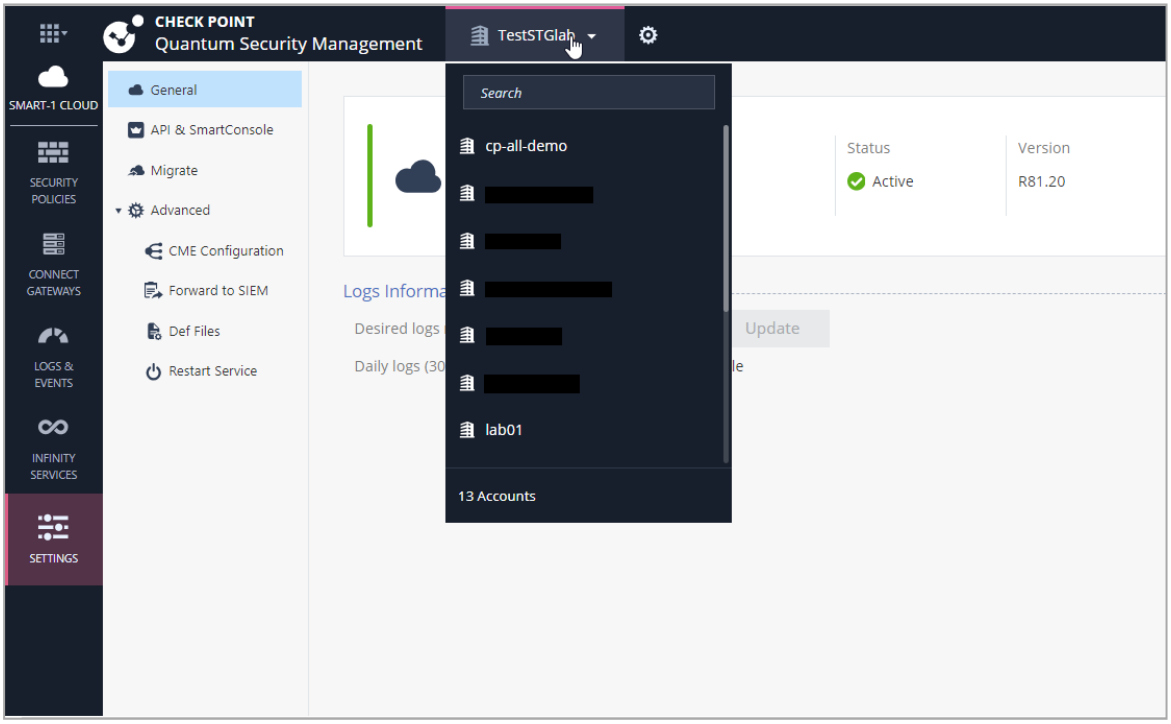
Smart-1 Cloud is a Check Point service that delivers Check Point Security Management as part of Check Point's SaaS solution.

Smart-1 Cloud enables administrators to manage their security policies, network objects, and logs analysis from a web browser, similar to on-premises deployments.

There may be behavioral differences between the cloud environment and the on-premises environment, which are listed below.

Management Capabilities

- **Multi-Domain Security Management**
  - With Smart-1 Cloud, a customer can have multiple environments on the same Infinity Portal account registered with the same email address. This is the equivalent of managing multiple domains.
  - You can easily switch between different environments in the portal by selecting the environment name from the drop-down list at the top of the window.



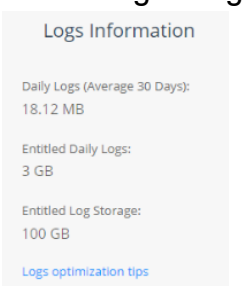
  - Single Sign-On (SSO) to the environments - The login from the portal to the Streamed SmartConsole uses the portal's credentials and enables SSO.

- **Management Objects**
  - The management object in Smart-1 Cloud is read-only and is not visible in the gateways and servers view. It can be seen in the object explorer in read-only mode.
  - Running actions on the management object is not required. As part of the service, environment backups run automatically every 12 hours.
- **Management Login - Supported Methods**
  - Log into SmartConsole using your Infinity Portal credentials. For available Infinity Portal login methods, see the *Infinity Portal Administration Guide*.
- **Two-Factor Authentication**
  - For Infinity Portal login, enable this option in **Global Settings**.
- **Managing Endpoint**
  - Use the new Harmony Endpoint (also available in the Infinity Portal) to manage Endpoint clients.
- **Managing HA**
  - In Smart-1 Cloud, the target is availability is 99.9% uptime; no additional HA solution is required.
- **CloudGuard Network Auto Scaling Solutions**
  - If you use Smart-1 Cloud to manage Auto Scaling groups, you must manage the Security Gateways with their public IPs.
  - To configure Smart-1 Cloud to automatically provision CloudGuard Network Security Gateways, contact *Check Point Support* for the required `autoprov` commands to run on the Management Server.
  - To use the "`vsec_lic_cli`" tool to apply CloudGuard Network licenses, contact *Check Point Support*.
  - Connection of a CloudGuard Network Auto Scaling Security Gateway as a new gateway is supported.

Logs & Events

- Logs Information.
  - Logs Information shows your tenant logs usage and entitled storage.
  - For how to optimize Smart-1 Cloud Logs, refer to sk181096.

  Note - Logs usage does not count the external exporters, for example:

- Logs & Events SmartView.
  - Use the Logs & Monitor view in SmartConsole.
  - Use the Logs & Events view in the Infinity Portal.
- Support for SmartEvent Views and Reports is automatically activated based on the purchased license.
- There may be a maximum latency of two minutes from the time the gateway creates a log until it is visible in **Logs & Events**.
- Free text search works only on a small list of fields. When you search, use a specific column's name.

  For example:
  - `action: "Drop"`
  - `severity: "Critical"`
- Paging/Scrolling is limited to 20 pages.
- Export logs to Excel CSV is limited to 10K records.
- All filters are case sensitive in value, including *action*, *type*, and *product*.
- To filter logs for only one value when `Blade/Product` has multiple values, add wildcards before and after the Blade's name, such as "`blade:*Firewall*`."
- Threat Prevention Rule Base - Lower logs pane does not return results for Threat Prevention rule base. Instead, it returns "`No matches found`." To filter Threat Prevention logs, use the **Logs** view in **Logs & Events**.

- Tufin: Hostname or LogID = Service Identifier (for logs from forward to SIEM configuration (Syslog)).

  You can find the Service Identifier in **Settings** > **General**.

- Tufin's SecureTrack is supported to manage policies on Smart-1 Cloud.

Migration

When migrating a Security Management Server to Smart-1 Cloud from on-premises, review these requirements before starting.

In some cases, configuration changes are required before or after the migration.

Important to know before you start:

1. Migration is supported from version R81.10 and higher.
2. Reset SIC after migration:
   a. Gateways running R80.40 Jumbo Hotfix Accumulator Take 89 or higher do not require SIC reset after migration.
   b. All others Gateways must reset SIC on the gateway before initializing communication from SmartConsole to the gateway.
3. Run the export command from inside the `/var/log` directory.
4. Make sure you have sufficient disk space in the partition before you start.

Configuration	Required Step
Gateway object with an unsupported appliance or version	See the list of *"Supported Gateways and Versions" on page 9*. A Gateway that belongs to an unsupported appliance or has an unsupported version is migrated but cannot be connected to the Service.
Management High Availability	Disable.
Management Object Configuration	You cannot edit the Management object in Smart-1 Cloud. During the import process: ■ NAT configuration is removed. ■ Proxy configuration is removed. ■ Old network configuration is ignored.
Endpoint Manager	Before you run export on the on-premises Security Management Server, disable the Endpoint Policy Management Software Blade and install the database.

Configuration	Required Step
Consent flag - Automatically download Blade contracts and other important data	This flag is enabled by default during import.
Central License	Regenerate a new license with this Management IP address: `100.64.0.52`.
Running scripts on the management objects	Disable.
Multi-Domain Server	Migration is supported only from a Security Management Server. To migrate a Domain to a Security Management Server, follow the instruction in sk156072 - Domain Migration in R80.x > section "Migrating from Domain Management Server to Security Management Server."
Standalone	Migrations is supported only from a Security Management Server. To migrate from Standalone to Distributed configuration before migrating to Smart-1 Cloud, follow the instruction in sk179444 - Migration from a Standalone environment to a Distributed environment.
Authentication methods: OS Password, SecurID, RADIUS, TACACS, API Key	Change the authentication method to a Check Point password. If the authentication method was not changed before the import, log in with Streamed SmartConsole and change it.
Network objects with IP addresses from the subnet `100.64.0.0/24`. See details here.	Smart-1 Cloud uses this subnet. Change IP addresses to a different subnet.

Integrations with Other Services and Third-Party Tools

- Integrations between third-party tools and Smart-1 Cloud are supported with the Management APIs.

Smart-1 Cloud Limitations

Management Limitations

- **Multi-Domain Security Management**

  Sharing global objects, global policies, and global rules between environments is not supported.

- **Management objects**

  SSH access to the Security Management Server is not available. Contact support for actions that require SSH access.

- **Unsupported management features**

  - VSX Gateways and VSX Clusters management is not supported.
  - SmartProvisioning is not supported.
  - In SmartTasks, the **Run Script** feature is not supported. (Smart-1 Cloud supports **Send Web Request** and **Send Mail** only).

    Important - For information and updates on Smart-1 Cloud external FQDNs and their associated IP addresses, see sk182699.

    Note - To access on-premises/cloud SMTP server, you must allow inbound traffic from Smart-1 Cloud FQDNs based on your region:
    - **Ireland**: eu-west-1.allowed-ips.checkpoint.com
    - **London** eu-west-2.allowed-ips.checkpoint.com
    - **N. Virginia**: us-east-1.allowed-ips.checkpoint.com
    - **Sydney**: ap-southeast-2.allowed-ips.checkpoint.com
    - **Mumbai**: ap-south-1.allowed-ips.checkpoint.com
  - Auto-complete of dynamic entities is not supported (for example, if you enter a source, destination, or service in the query bar, the pop-up suggestion bar remains empty).
  - Upgrading Quantum Spark Gateways from the CDT (Central Deployment Tool) is not supported.
  - SmartUpdate is not supported.
  - Uploading files to the Package Repository is not supported in Smart-1 Cloud.

- **Unsupported Management APIs**

  Note - Running these APIs may cause unwanted behavior.

  - `run_script` on the Management Server object
  - `migrate-export-domain`
  - `put-file`
  - SmartTasks

- **CloudGuard Network Auto Scaling Solutions**

  - CME Automatic Hotfix Deployment is not supported.
  - Migration of an on-premises management database with CloudGuard Network Auto Scaling gateway is not supported. Communication issues may occur between Smart-1 Cloud and the existing CloudGuard Network Auto Scaling gateways.

- **VPN**

  - Automatic MEP Topology is not supported.

Logs & Events

- SmartEvent Policies are not supported. It is not possible to configure custom events or automatic reactions.

  Important - The checkboxes for SmartEvent Software Blades are automatically selected if the user has a corresponding license which is functioning as intended.

- OPSEC and LEA are not supported.
- Some widgets in these Views and Reports may not work and return a "`Failed to query`" error:
  - **Views** - MTA Live Monitoring
  - **Reports** - GDPR Security Report, Security Checkup - Advanced
- Auto-refresh does not refresh the information.
- Suggestions in Log view is not supported for some values.
- Cannot search for a specific updatable object in logs.
- **Logs** view > **Edit profile** - Some fields may cause "`query failed`" error - in this case, open a support ticket.
- Opening log file from **Logs & Events** is not supported.
- Blobs and packet captures are not supported.
- SmartView web access through the SmartConsole link is not supported.

  To view logs, use the embedded SmartView functionality in SmartConsole.

Migration

- Migrating on-premises Security Management Server in the Full High Availability Cluster mode to Smart-1 Cloud is not supported.
- Migration from pre-R81 Multi-Domain Security Management Server to a Smart-1 Cloud server fails (see sk180650 for details).

Integrations with Other Services and Third-party Tools

- Integration with third-party tools that use SSH access or OPSEC/LEA to the Management Server are not supported.
- Known unsupported integrations:
  - ThreatCloud Managed Security Service

Best Practices for Smart-1 Cloud

Management APIs

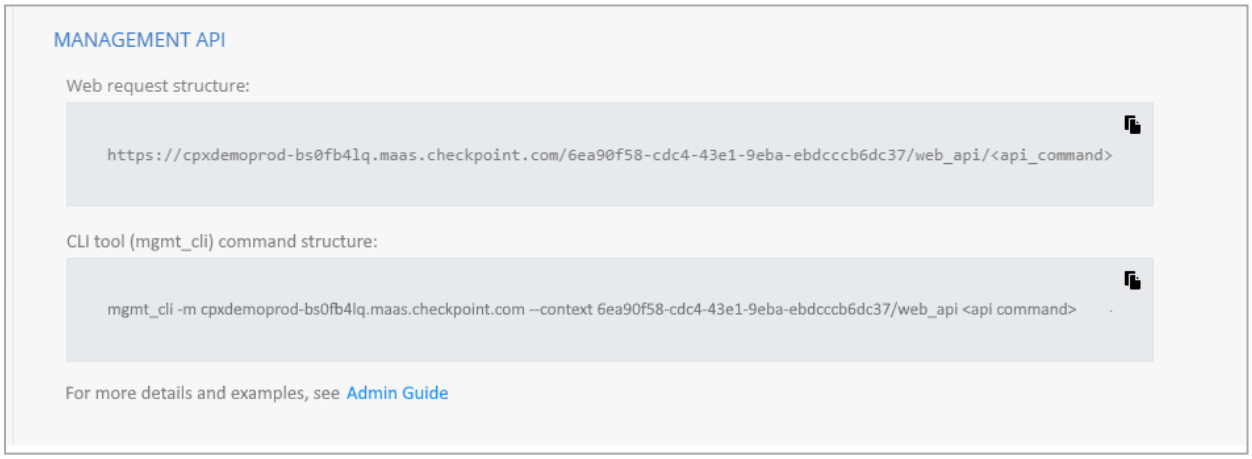
It is possible to read information and to send commands to the Check Point Management Server. In an equivalent procedure to creation of objects, Security Policy configuration, and use of the SmartConsole GUI, it is possible to do the same tasks with command line tools and web services.

Before you start, create an administrator in SmartConsole, give it the required permission profile, and make sure the permission profile has API permissions enabled:

Open the **Permission Profile**, navigate to **Management**, make sure **Management API Login** is enabled.

Two ways to connect with the management APIs in Smart-1 Cloud:

1. Enter API commands with the "`mgmt_cli`" executable (available in Windows, Linux/Gaia).
2. Send API commands on a HTTPS connection with web services.



Use the "mgmt_cli" tool with:

The `mgmt_cli` tool is installed as part of Gaia on all Security Gateways R80.10 and higher and you can use it in scripts running in the Expert mode.

The `mgmt_cli.exe` tool is installed as part of the SmartConsole installation, usually in: `C:\Program Files (x86)\CheckPoint\SmartConsole\R8x.x\PROGRAM\)`

You can copy and run it on a Windows computer.

For a full list of the `mgmt_cli` options, run "`mgmt_cli`". For more information about the `mgmt_cli` tool, see the *Check Point Management API Reference*.

Example:

The CLI requests username and password.

```
mgmt_cli -m <Service_identifier>.maas.checkpoint.com --context
<Connection Token>/web_api add host name host1 ip-address
192.0.2.101
```

Smart-1 Cloud APIs

Automate your Smart-1 Cloud operations with the use of REST APIs to run operations such as create new Smart-1 Cloud environment, register a gateway, and get the service information.

To configure and show the Security Policy and objects in the Security Management use the Management APIs.

For more information, see *Check Point Management API Reference*.

The Streamed SmartConsole

Smart-1 Cloud supplies SmartConsole that runs on a web Browser. The Streamed SmartConsole has the full functionality as the Windows SmartConsole. But it runs in a different I/S.

Note - The Streamed SmartConsole has a built-in timeout mechanism which expires after 15 minutes of idle operation and, or after two hours. After the session expires, you need to log in again.

How to upload or download files from SmartConsole:

- Use this top toolbar:

- You can save the files locally in **My files**. When it is necessary to upload files, use this toolbar:

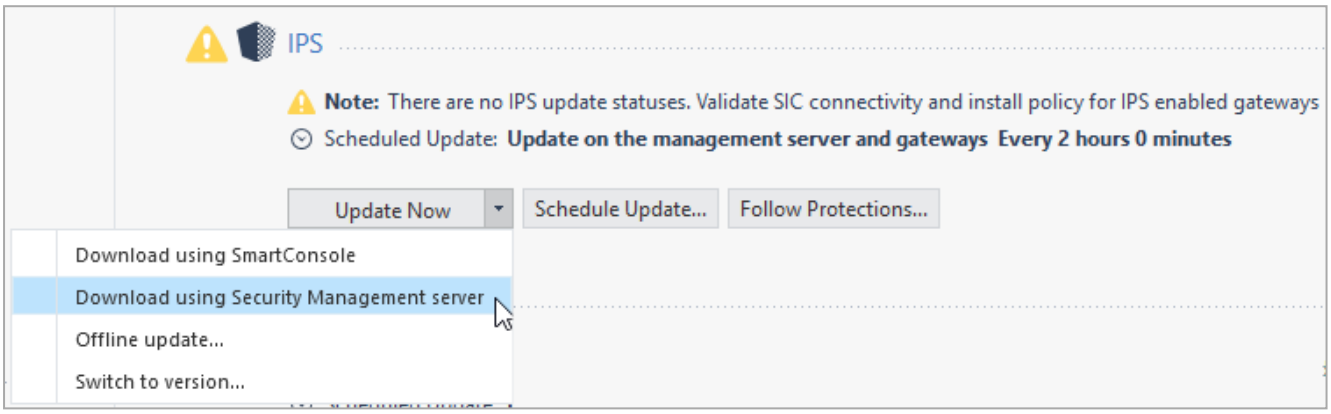
- Upload the files to a temporary folder in **my files**. Downloaded files are saved here. Use the folder icon, on the top toolbar, to download files to the local computer.

IPS Updates

To fetch IPS Updates in Smart-1 Cloud, it is recommended to configure Smart-1 Cloud to download with Security Management Server and not with SmartConsole.

In Smart-1 Cloud, by default, your Management Environment has Internet connectivity.

This is the recommended configuration that results in better performance.



Automatic Updates

Refer to sk166056 to see the up-to-date list of Smart-1 Cloud Automatic Updates.

Smart-1 Cloud Licensing

The Management License

In Smart-1 Cloud, the service does the management licenses and enforcement.

Therefore, unlike the licenses for the on-premises Management Server, there is no need to apply or monitor the management licenses.

The service applies default licenses on the Management Server with the maximum capabilities.

But services and capabilities entitlements are a direct reflection of your Smart-1 Cloud licenses.

Smart-1 Cloud License

A new Smart-1 Cloud account has a 30-day trial period by default in which you can connect Security Gateways and examine the service.

If you want to continue to use the service after the trial period ends, contact Check Point Sales to purchase a license.

All Smart-1 Cloud functionality is available by default for trial accounts, but it does not include:

- Compliance
- Updates and upgrades to the latest version
- Export of logs to a SIEM vendor

Note - Licenses in Smart-1 Cloud are additive. Make sure to allocate all licenses to the Check Point User Center account linked with the Infinity Portal account.

Activating a license

1. In Smart-1 Cloud, go to **Global Settings** > **Contracts**.
2. From the top-right, click **Associated Accounts**.

   The Managed Accounts window opens.
3. Click **Attach Account**.

   The Attach Account window opens.
4. Enter the User Center credentials > click **Next**.
5. Select the license to apply > click **Finish**.

   Your license is shown in the **Contracts** page.

Notes:

- If you already have a related account and want to add one more license, go to **Global Settings** > **Contracts** > **Associated Accounts** and use the sync option to update the license.
  In Smart-1 Cloud, the license status shows at this time: **Active**.
- It can take up to 24 hours for the license status to update to **Active** in Smart-1 Cloud.
  In the 'Trial' status there are no limitations to start and use the service.
  If the status continue to show **Trial**, contact maas@checkpoint.com.

Smart-1 Cloud Administrator Roles

To add a new user to Smart-1 Cloud, refer to the Users section in Infinity Portal Administration Guide.

Smart-1 Cloud Roles are equivalent to SmartConsole permission profiles:

Smart-1 Cloud Role	SmartConsole Permission Profile	Description
Admin	Super User	Full Read/Write Permissions including managing administrators and sessions.
Submitter Administrator	Smart-1 Cloud Submitter Administrator	SmartConsole Read/Write permissions - Publishing of sessions requires approval. Smart-1 Cloud Portal permission - Read Only permissions.
Read-Only	Read Only All	Full Read Permissions, no write.

Notes:

- Smart-1 Cloud specific service roles are in addition to the global roles and do not override them.
- Smart-1 Cloud Portal permission is relevant for **CONNECT GATEWAYS** and **SETTINGS** tabs.
- Custom permission profiles in SmartConsole are always overridden by system profiles pushed by the Infinity Portal.

For more information about user management, refer to the Infinity Portal Administration Guide.

Troubleshooting of Smart-1 Cloud

This section is for common issues and solutions. If you cannot resolve the issue with these troubleshooting solutions, contact *Check Point Support*. Make sure to open the ticket for Cloud Management / Smart-1 Cloud.

Include these items in your support request:

- The service identifier (from the overview page)
- Log files:
  - If the issue is in the connectivity between the Security Gateway and service, upload these log files from the Security Gateway:
    - `$FWDIR/log/vtunnel`
    - `$FWDIR/log/wstunnel`
  - If the issue is with SmartConsole upload these log files:
    - SmartConsole logs

Table: Troubleshooting

Symptom	Solution
Cannot open a tunnel from the Security Gateway to the service. `Error: maas: command not found.`	■ Make sure the Security Gateway can contact: `updates.checkpoint.com` ■ Make sure the gateway can contact: `https://<Service-Identifier>.maas.checkpoint.com`
Security Gateway is unable to connect to the service.	Enable the **Download** consent flag for this Security Gateway. For instructions: ■ For R81.20 and higher, refer to: sk175504. ■ For R81.10 and lower, refer to: sk111080.
Upgrade of the Security Gateway is stuck, or the Security Gateway is unable to connect to the service after an upgrade.	Follow sk166036.

Table: Troubleshooting (continued)

Symptom	Solution
No SIC with the Security Gateway.	■ Do these steps to connect the Security Gateway: Navigate to the *Check Point Infinity Portal* > Smart-1 Cloud > select **Connect Gateway**. ■ Make sure the MaaS tunnel is up and running: • Run one of these commands: ◦ `maas status` ◦ `show security-gateway cloud-mgmt-service` • Run the `ifconfig` command and make sure you have an interface "`maas_tunnel`" configured with the same IP address as the Security Gateway object. ■ Make sure the Security Gateway clock is correct and synced.
Tunnel works, but there is no communication between the Security Gateway and the service.	■ Make sure the MaaS tunnel is up and running: • Run one of these commands: ◦ `maas status` ◦ `show security-gateway cloud-mgmt-service` • Run the `ifconfig` command and make sure that you have an interface "`maas_tunnel`" configured with the same IP address as the Security Gateway object. ■ Make sure the Security Gateway can contact: `https://<Service-Identifer>.maas.checkpoint.com`

Table: Troubleshooting (continued)

Symptom	Solution
After I installed policy, I lost management communication with the Security Gateway.	■ You must allow outbound HTTPS traffic to FQDN listed below to allow the communication between the Security Gateway and the service: • To your domain at Smart-1 Cloud: `<Service-Identifier>.maas.checkpoint.com` • For Smart-1 Cloud deployments in Europe: `cloudinfra-gw.portal.checkpoint.com` • For Smart-1 Cloud deployments in the United States: `cloudinfra-gw-us.portal.checkpoint.com` • For Smart-1 Cloud deployments in the APAC: `https://cloudinfra-gw.ap.portal.checkpoint.com` ■ If this is not possible, then reset the SIC, or contact *Check Point Support*.
The "`maas on`" or "`set security-gateway cloud-mgmt-service on auth-token XXXX`" command shows this error message: `check for Internet connectivity.`	Examine connectivity to: `<Service-Identifier>.maas.checkpoint.com`
The "`maas on` or "`set security-gateway cloud-mgmt-service on auth-token XXXX`" command shows this error: `error 132`	Make sure that the Security Gateway time is correct and synced with NTP.

Table: Troubleshooting (continued)

Symptom	Solution
The "`maas status`" or "`show security-gateway cloud-mgmt-service`" command returned: `MaaS Status: Enabled` `MaaS Tunnel State: Down` `Unable to connect to MaaS at https://<Service-Identifier>.maas.checkpoint.com`	1. Make sure your policy enables outgoing HTTPS (TCP 443) to your domain at MaaS: `<Tenant-ID>.maas.checkpoint.com` If the Security Gateway connects to Smart-1 Cloud through a Proxy Server, make sure the Security Gateway can connect to this Proxy Server. 2. If the Security Gateway connects to Smart-1 Cloud through a Proxy Server, make sure your policy allows the HTTPS traffic to your Proxy Server. 3. Make sure the Security Gateway can connect to Smart-1 Cloud using FQDN, and there is no HTTPS inspection: a. Connect to the command line on the Security Gateway and log in to the Expert mode. b. Get the Smart-1 Cloud FQDN and CloudInfra URL: `CloudInfraURL=`jq -r ".data.cloudInfaUrl" $FWDIR/conf/cloudinfra.conf` `FQDNURL=`jq -r ".data.fqdn" $FWDIR/conf/cloudinfra.conf` c. Try to connect to Smart-1 Cloud using FQDN: `curl_cli $CloudInfraURL -k -vvv` `curl_cli https://$FQDNURL -k -vvv` 4. Compare the certificate the Security Gateway gets in the `curl_cli` command output to the certificate you see when you do not use the proxy.
Gateway Gaia Portal not accessible.	See *"How to Configure Access to Security Gateway Gaia Portal" on page 62*.
"Failure in deserializing object of type" error in SmartConsole when trying to connect to Security Management Server with Portable SmartConsole.	See sk123152.

Table: Troubleshooting (continued)

Symptom	Solution
Cannot change the SmartConsole admin password from the Infinity Portal.	Go to SmartConsole > **Manage & Settings** and make sure that the administrator password is not configured as an **OS** password. If it is, change it to **Check Point** password.
Error message in SmartConsole log in, "`Could not verify shared secret`".	Make sure that you have the latest SmartConsole version. Download the SmartConsole from the Smart-1 Cloud portal (topic SmartConsole)
When you add a Cluster Member, the "`failed to save object validation error on maas_tunnel network object`" messages appears.	Fetch cluster topology again, see sk171157.
Upgrade of Security Gateways with SmartConsole fails, times-out or appears stuck at approximately 62%.	See sk166036.
Cannot see Security Gateway logs in SmartConsole, or the Security Gateway does not send logs to Smart-1 Cloud.	▪ Make sure the consent flag to upload data to Check Point is enabled on the Security Gateway (see sk111080). ▪ Install Database: 1. Open SmartConsole. 2. Click the Menu > Install Database. 3. Select the Management Server object. 4. Click **Install**.
"`Loss connectivity to client`" error with the "`Try again`" option.	1. On the Security Gateway appliance, make sure the network settings are correct. 2. In the Smart-1 Cloud portal, click **Try again**.
"`Loss connectivity to client`" error without the "`Try again`" option.	1. On the Security Gateway appliance, run the "`fcd revert`" command and wait for the appliance to reboot. 2. Connect to the Gaia Portal of the Security Gateway appliance. 3. Follow through the Gaia First Time Configuration wizard. 4. In the Smart-1 Cloud portal, add the appliance manually.

Table: Troubleshooting (continued)

Symptom	Solution
"`Authentication failed`" error with the "`Try again`" option.	1. On the Security Gateway appliance, make sure the network settings are correct. 2. In the Smart-1 Cloud portal, click **Try again**.
"`Authentication failed`" error without the "`Try again`" option.	1. Connect to the Gaia Portal of the Security Gateway appliance. 2. Follow through the Gaia First Time Configuration wizard. 3. In the Smart-1 Cloud portal, add the appliance manually.
"`Tunnel Down`" error.	1. On the Security Gateway appliance, make sure you have connectivity to the Smart-1 Cloud service. 2. See sk83520 - How to verify that Security Gateway and/or Security Management Server can access Check Point servers. 3. In the Smart-1 Cloud portal, click the button with the three vertical dots to open the menu. 4. Click **Regenerate Token**. 5. Follow the instructions on the screen.

"`Trust (SIC) establishment failed`" error.	1. On the Security Gateway appliance, make sure it can connect to the Smart-1 Cloud service.
	See sk83520 - How to verify that Security Gateway and/or Security Management Server can access Check Point servers.
	2. On the Security Gateway appliance, run **one** of these commands to make sure the tunnel is up:
	▪ In the Expert mode:
	`maas status`
	▪ In Gaia Clish:
	`show security-gateway cloud-mgmt-service`
	3. Reset SIC on the Security Gateway appliance and the Security Management Server. Follow sk65764 - How to Reset SIC.

Table: Troubleshooting (continued)

Symptom	Solution
"`Fetch interfaces failed`" warning.	1. In SmartConsole, open the Security Gateway object. 2. From the left, click **Network Management**. 3. Click **Get Interfaces** > **Get Interfaces With Topology** > click **Accept**. 4. Click **OK**. 5. Publish the session.
"`Installation failed (install policy)`" error.	1. Open SmartConsole. 2. In the bottom left corner, click the details of the failed policy installation. 3. Read the details about the root cause, fix the issues, and try again. **Note** - The card you see on the screen shows the initial policy. During the next policy installation (successful or failed), the card is not updated with the real status.

1. New Quantum appliance is not discovered automatically on the **Connected Gateways** page.
2. Attempt to on board a new Quantum appliance encounters an issue with connectivity resulting in a "`No internet connection`" page.
	1. Make sure the Service and Contract page shows the correct contract.
	2. Make sure the appliance is powered on and connected to the Internet with the blinking interface (this interface is configured to get an IP address from a DHCP server).
	3. Make sure the appliance received the required IP address configuration from the DHCP server:
	a. Connect to the command line on the appliance.
	b. Log in.
	c. If you default shell is the Expert mode, then go to Gaia Clish:
	`clish`
	d. Make sure the appliance received the correct IP address:
	`show interface <Name of Blinking Interface> all`
	e. Make sure the appliance received the correct Default Gateway:
	`show route`
	4. Make sure your network allows the connection from this appliance to the *zerotouch.checkpoint.com* server.

Frequently Asked Questions about Smart-1 Cloud

What is my Smart-1 Cloud Management Server IP address?

In Smart-1 Cloud the Management Server holds an internal IP address, which is inaccessible from the outside.

Usually it is not necessary to know or use the Management IP address, but in some cases you are required to provide it.

Because the Management IP address is internal, it is the same for all deployments.

Therefore, when required to use the Management IP address, such as Central License, use this IP address: 100.64.0.52.

After Check Point releases a new software version, when is my Smart-1 Cloud environment upgraded?

Several weeks after the release of a new GA version, Smart-1 Cloud is upgraded and runs the new version for new environments.

Afterward, we gradually upgrade for existing customers.

Do I receive a notification before an upgrade runs on my Smart-1 Cloud environment?

- In Smart-1 Cloud, Check Point upgrades your Smart-1 Cloud environment.

  A customer receives a notification two weeks before the upgrade occur.

  Upgrades are done based on the region in which your Smart-1 Cloud environment is deployed (after local business hours).
- Smart-1 Cloud sends notifications to the primary administrator as defined in your Infinity Portal account settings.
- After a customer receives the notification for a planned upgrade, they can ask to reschedule.

  A new upgrade window is then allocated for the customer, and a new notification is sent before the next planned upgrade.

  A customer's upgrade does not effect other customers Smart-1 Cloud environment.

What are the Service Maintenance Windows?

The service runs pro-active monitoring on all production environments; in some cases, maintenance actions are required to provide stable operation.

All maintenance operations are done after usual work hours for each deployed region and in accordance with the regional maintenance windows.

For non-disrupted operations or operations with disruptions lasting up to 10 minutes, no notification is shared with the customer.

(This is done only during regular off-hours.)

There are rare cases, such as major version upgrades, in which the maintenance operation may take 1-2 hours. In such cases, an email notification is sent 10–14 days in advance, providing a range of 2–3 days in which the operation will take place (again, always within regional off-hours). The customer can reply to the email and request to reschedule to another range.

Regional maintenance windows:

- APAC, India, EU and US - Every Sunday
- EU/UK - weekdays - from 20:00 to 06:00 am CET
- US - weekdays - from 20:00 to 06:00 am CST
- IN - weekdays - from 20:00 to 06:00 am IST
- APC - weekdays - from 20:00 to 06:00 am ACT (Australian Central Time)

How can I revert my management database to an earlier version?

- Starting from R80.40, customers can use SmartConsole or an API to revert to an earlier revision.
- To revert all the management to an earlier version, it is necessary to open a Service Request with *Check Point Support*.

  Note - After this procedure is done, you cannot cancel it.

Which ports must be open on the Security Gateway?

You must allow outbound HTTPS traffic to FQDN listed below to allow the communication between the Security Gateway and the service:

- To your domain at Smart-1 Cloud:

  `<Service-Identifier>.maas.checkpoint.com`

- For Smart-1 Cloud deployments in Europe:

  `cloudinfra-gw.portal.checkpoint.com`

- For Smart-1 Cloud deployments in the United States:

  `cloudinfra-gw-us.portal.checkpoint.com`

- For Smart-1 Cloud deployments in the APAC:

  `https://cloudinfra-gw.ap.portal.checkpoint.com`

From version R80.40, there is an implied rule that always allows this traffic when working in the MaaS mode.

What if I already have SmartConsole for a different on-premises management?

You can use the same SmartConsole to connect to your Smart-1 Cloud environments and to your on-premises environments.

Does Smart-1 Cloud support APIs?

Yes, you can use the Management APIs with Smart-1 Cloud, go to **Settings** > **API & SmartConsole**.

For more information, see the *Check Point Management API Reference*.

How frequently do you run backups?

Backups of the environments are taken daily for the first ten days and, after that, less frequently..

How many gateways can you manage with Smart-1 Cloud?

Smart-1 Cloud can manage up to 400 Security Gateways.

How do I manage to do tasks that must have SSH on the machine?

All tasks related to the maintenance of the environment are part of the service.

You can open a ticket with *Check Point Support* for assistance with SSH.

If it is necessary to cancel the service, what must I do?

A customer that decides to cancel the service and needs the management DB (to move it to the on-premises management), must open a Service Request with *Check Point Support* and ask for the management database.

Note - It is not possible to download the logs.

Do these changes in configuration:

- Change the IP address in the management object (that primary IP address that holds the Smart-1 Cloud management IP address).
- If "`*.def`" files were changed, then it is necessary to apply the changes. As an alternative, request the files from *Check Point Support*.
- Other special configuration such as Security Gateway as a proxy to access the LDAP.
- On the Security Gateway, disconnect the Security Gateway from Smart-1 Cloud, run the "`maas off`" command on the Security Gateway.

  See *"Smart-1 Cloud Gateway Commands" on page 54*.

I purchased a Smart-1 Cloud license. How do I apply it, and what visibility do I have?

Congratulations, you have decided to join Smart-1 Cloud and purchased a license.

To help you ,our team will reach out to your sales representatives to get all the necessary information.

For more information, see *"Smart-1 Cloud License" on page 78*.

If the issues continue, contact Account Services and ask to configure your account as *production*.

Provide these details:

- Infinity Portal account name
- Smart-1 Cloud Service Identifier
- User Center Account

Which IP addresses the service uses to connect the Security Gateway to the Smart-1 Cloud?

When you register a new Gateway to the service, an IP address from one of these subnets is used for the creation of a secure tunnel between the Security Gateway and the Smart-1 Cloud:

- 100.64.0.0/16
- 100.70.0.0/16
- 100.71.0.0/16
- 100.100.0.0/16
- 100.101.0.0/16

Note - The virtual interface that is created on the Security Gateway uses this IP address as the primary IP address in the object that shows the Gateway in SmartConsole..

Log Ingestion and Retention

Your Smart-1 Cloud license determines two key parameters for log management:

- Maximum daily log ingestion rate
- Log retention period (the number of days logs are stored)

These parameters vary based on your specific license SKU.

Important - It is strongly recommended to purchase a license with a daily ingestion limit that exceeds your actual average log ingestion rate.

The standard offering includes **90 days** of data retention. Extended retention periods (6 months or 1 year) are available for specific license SKUs (for more information on license SKUs, see sk182394).

To monitor your log usage, check the **Average Monthly Ingestion** and **Daily Log Ingestion** graphs on the **Infinity Events > Log Ingestion** page.

Note - See sk181096 for information on logs optimization.

DAIP Gateway and Smart-1 Cloud

1. If you have a DAIP Security Gateway and you are concerned with the connectivity between the Security Management Server and the Security Gateway, you can configure the tunnel IP in the Security Gateway object.
2. When you configure a DAIP Security Gateway in Smart-1 Cloud, on the initialize SIC sequence, you must enter the tunnel IP address as the Gateway IP address.

ICA Management Tool and Smart-1 Cloud

For support of the ICA Management Tool contact *Check Point Support*.

Does Smart-1 Cloud support Compliance Blade?

Yes, the Compliance blade is supported. You can see it from the Streamed SmartConsole. Refer to *"Log in to SmartConsole from Smart-1 Cloud" on page 38*

How do I add/attach a VPN license to Smart-1 Cloud management?

To add or attach a VPN license to Smart-1 Cloud, contact Check Point Support and open a service request.

Does Smart-1 Cloud support ElasticXL?

Yes, ElasticXL is supported starting from R82. This is a new clustering technology that simplifies operations by using a single management object, offering automatic configuration and software synchronization across all cluster members.