QUANTUM

13 August 2024

QUANTUM SMART-1 CLOUD

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

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

Certifications

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

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

Security Management is a unified experience for all your Quantum Managements that manages your Smart-1 Cloud environment and all your Self-Hosted Management Servers in one place.

Smart-1 Cloud a best-in-class management solution is now available as a service. Check Point Security Management Architecture for the Cloud provides you with full management capabilities such as policy management, log analysis, reporting log retention, and Check Point's SmartConsole as a web console. With the Smart-1 Cloud application, you can manage your on-premises or CloudGuard Network Security Gateways from a single pane of glass.

Best Practice

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

Key Benefits

- **Always the Latest Security Management** - Newest features automatically updated in a unified management platform.
- **Zero Maintenance** - No need to monitor or for back up operations in your security management server.
- **On-demand Expansion** - Seamlessly expand capacity with support of more gateways and storage.

Use Case

A typical Use Case is a company looking to increase operational efficiency and lower the complexity of their Security Management platform. With the Smart-1 Cloud application, companies can focus and invest more effort in managing their security.

Tasks such as maintenance efforts, keeping up to date with the latest software version and security updates, running backups, and health status checks all require quality effort and time. In addition, as companies expand, it is necessary to align the security solutions correctly, which may need new hardware and migration procedures. A transfer of these, and other, IT management tasks to Smart-1 Cloud application significantly improves a company's security management, and let you focus on what is really important - your business.

The deployment process of a new Management Service in Smart-1 Cloud takes about 1 minute. After the deployment is complete, you receive a new Management with the latest version - ready to connect gateways. An existing customer can select to migrate their on-premises environment to Smart-1 Cloud. After the migration, you can continue to work from the exact same point that you stopped working before the migration (your on-premises management). See *"Migrate" on page 49*.

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

Supported Gateways and Versions

Category	Appliance Models	Software Version
Quantum Spark Security Gateways	3000 2000	R80.10 and higher
	1800 1600	R80.20.25 and higher R80.20.25 and higher
	1500	R80.20.05 and higher
	CloudGuard Edge	R80.20.05 and higher
Quantum Security Gateways	23000 21000 16000 15000 13000 12000 9000 7000 6000 5000 4000	R80.10 and higher
CloudGuard Network	CloudGuard Network Security Gateway	R80.20 and higher
	Auto Scaling solutions	▪ Azure VMSS ▪ AWS ASG ▪ GCP MIG
Security Gateways	Open Servers	R80.10 and higher
Quantum Maestro	All Maestro supported appliances	R81.10 and R81.20

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

Roadmap - Support for Security Gateways in the VSX mode.

Getting Started with Smart-1 Cloud

The *Check Point Infinity Portal* hosts the Smart-1 Cloud application.

To start, you must first create an account in the portal to use the application.

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

1. *"Step 1: Creating an Account in the Infinity Portal" below*
2. *"Step 2: Accessing 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" on page 43*.
5. Connect Gateways, see *Connecting Gateways*.

Step 1: Creating an Account in the Infinity Portal

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

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

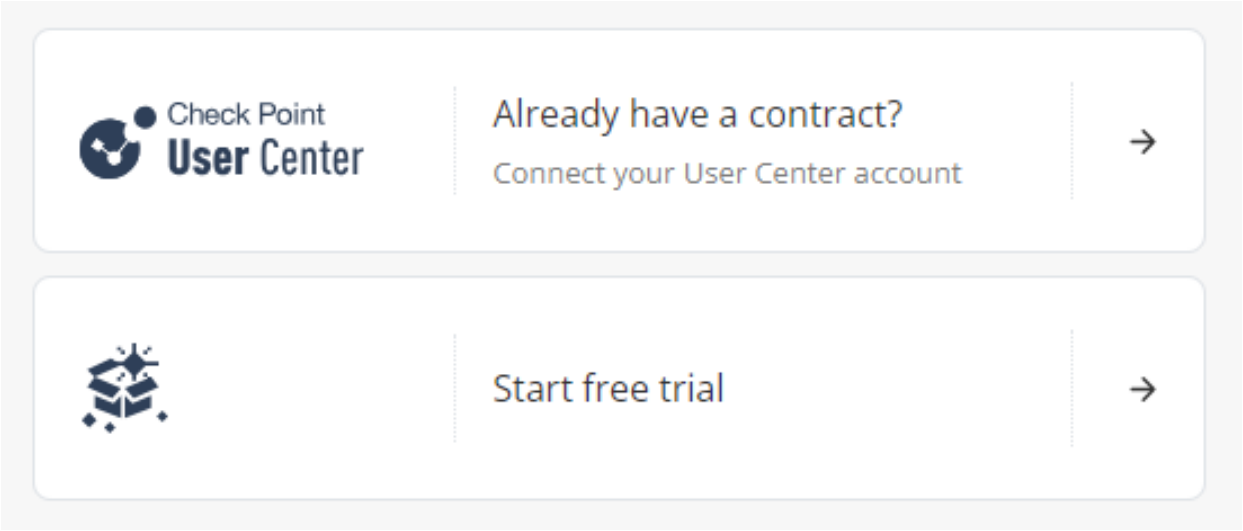
To create an Infinity Portal account, see the Infinity Portal Administration Guide.

Step 2: Accessing the Infinity Smart-1 Cloud 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**.

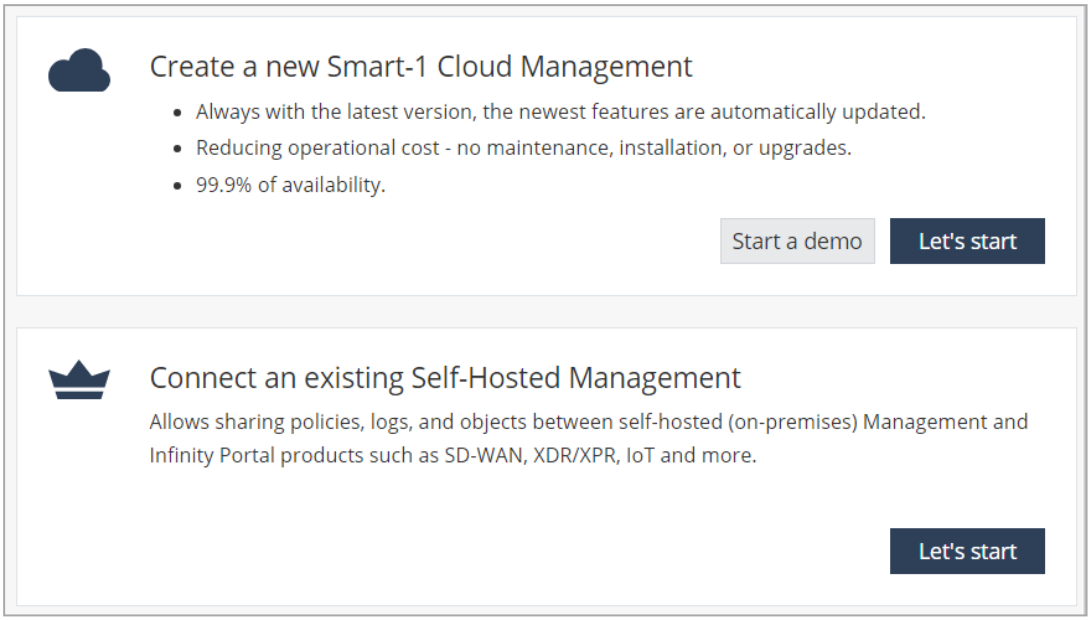
   Note - Security Management is a unified experience for all your Quantum Management solutions.
   You can connect multiple self-hosted (on-premises) Management Servers and manage one Smart-1 Cloud environment in one Infinity Portal tenant.

4. If you access the Smart-1 Cloud portal for the first time, select one of the options below:



   - 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.

- Start a free trial if you do not associate Smart-1 Cloud with a user account. When you select this option, you can use Smart-1 Cloud for a 30-day period.
  - When 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 how to connect your existing Self-Hosted Management Servers to the Infinity Portal, refer to [R81.20 Quantum Security Management Administration Guide] > Connecting On-Premises Management Servers and Security Gateways to the Infinity Portal.
  - In **Create a new Smart-1 Cloud Management** you can select to:
    - **Start a demo**.
    - Click **Let's start**.

      An email with confirmation of your registration is sent to your email account.

      After you approve your registration, the page automatically refreshes, and you can start to use the application.

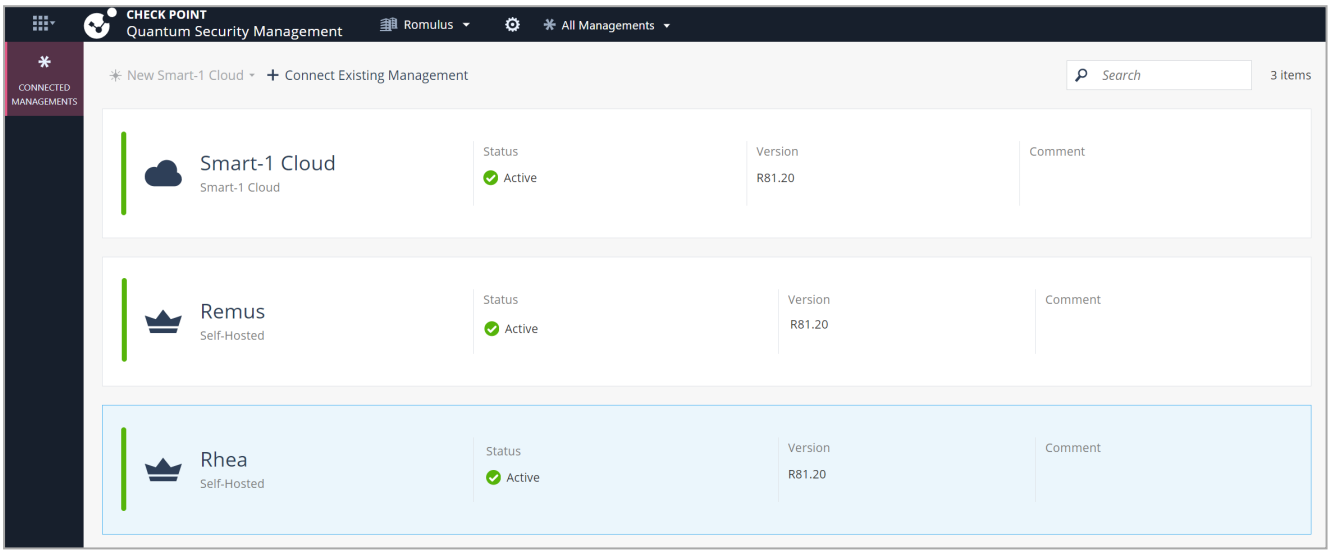
For **existing accounts**, the main screen shows a dashboard (by default, Security Policies dashboard) of your environment.

Navigating the Smart-1 Cloud Portal

The Smart-1 Cloud Portal table gives a brief overview of each button and their action.

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

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



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

Common Smart-1 Cloud Tasks:

- Create a new Smart-1 Cloud environment.
- Log in into SmartConsole.
- Connect Gateways.
- Obtain more information and run advanced options.

Additionally, you can do this:

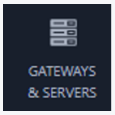
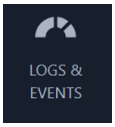
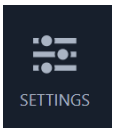
- Update and change the Global Settings.

  The information in the Global Settings and Profile contain the initial default values and effect all the system.

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

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

Overview of the Smart-1 Cloud Portal options:

To do this:	Click this:
▪ Security Policies Page is the new home page when 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, Streamed 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 you register to the Smart-1 Cloud application, you can start on-boarding 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 30 days of free trial. You can extend the trial period with EVAL license. Contact your Check Point representative for this license.
- **Demo**
  For demonstrations only and cannot be used in production. This environment terminates after 24 hours without option to extend it.

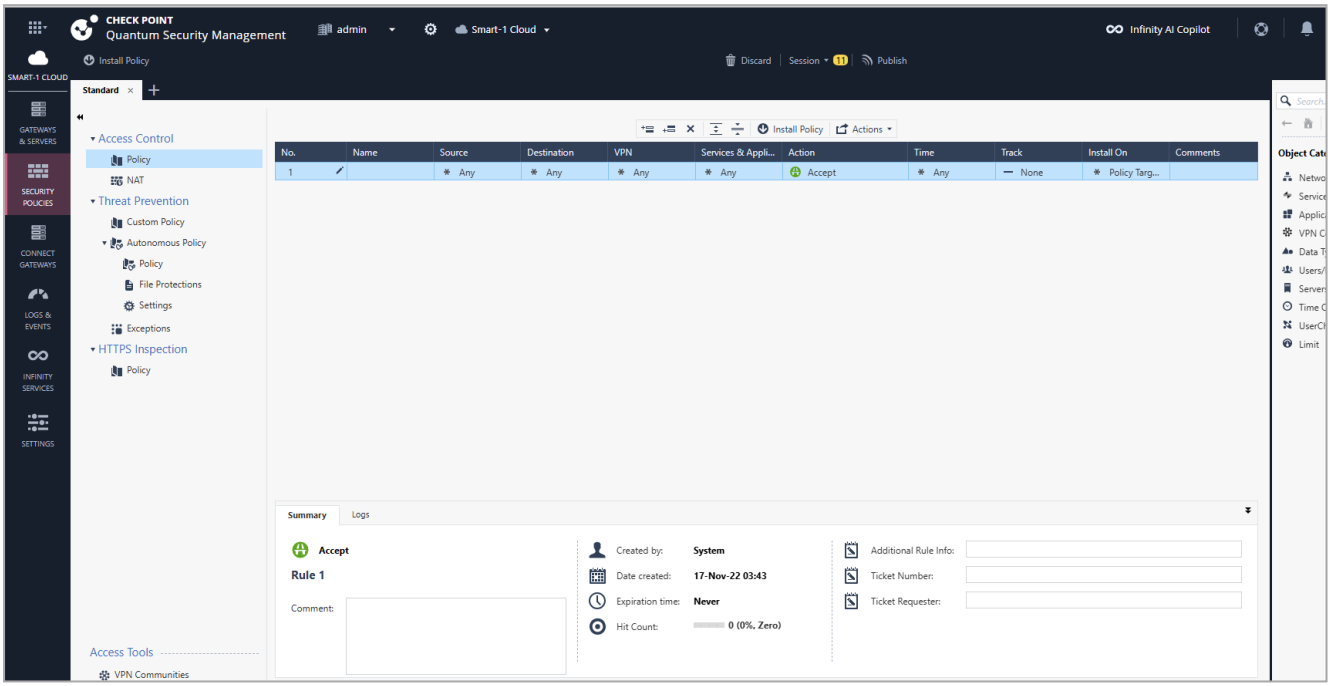
The **Preparing Account** window opens. It takes 1-2 minutes to create a new service.

After the process is complete, an email is sent to your account.

Understanding the Home Page

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

Example:

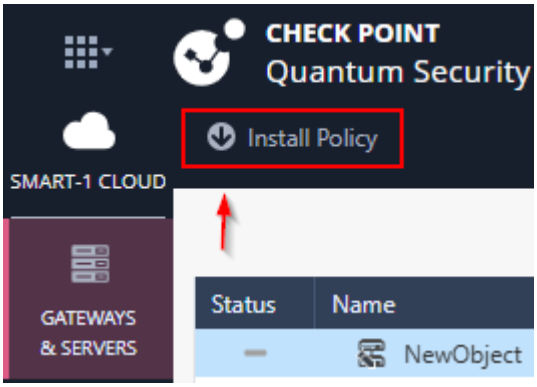


On the Smart-1 Cloud home page, you can:

- 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.
- Enter session details to view the number of changes made in the session.

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

You can install policy from the **Install Policy** button on the top left of the home page.

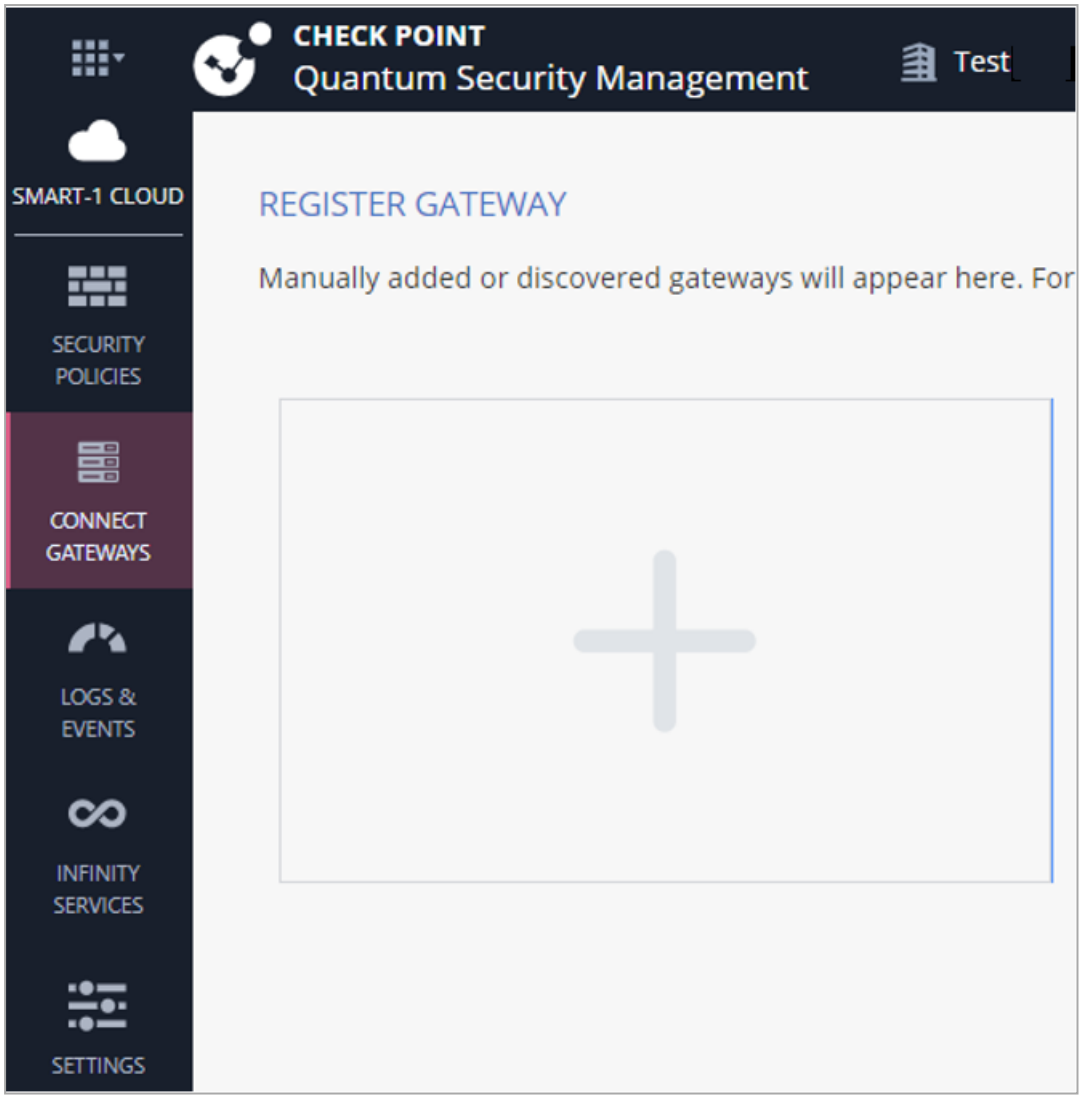

CHECK POINT
Quantum Security
Install Policy
SMART-1 CLOUD
GATEWAYS
& SERVERS
Status
Name
NewObject

Connecting Gateways and Clusters

Connecting a Security Gateway/CloudGuard Network Security Gateway

Procedure

1. From the left navigation panel, click **Connect Gateways**.
2. Click the large plus icon.



The **Register Security Gateway** window opens.

Note - The server detects if there are existing gateway objects in the database.
For existing gateway objects, the server asks:
`Do you want to create a new gateway object, or use an existing gateway`

3. Create a New Gateway:

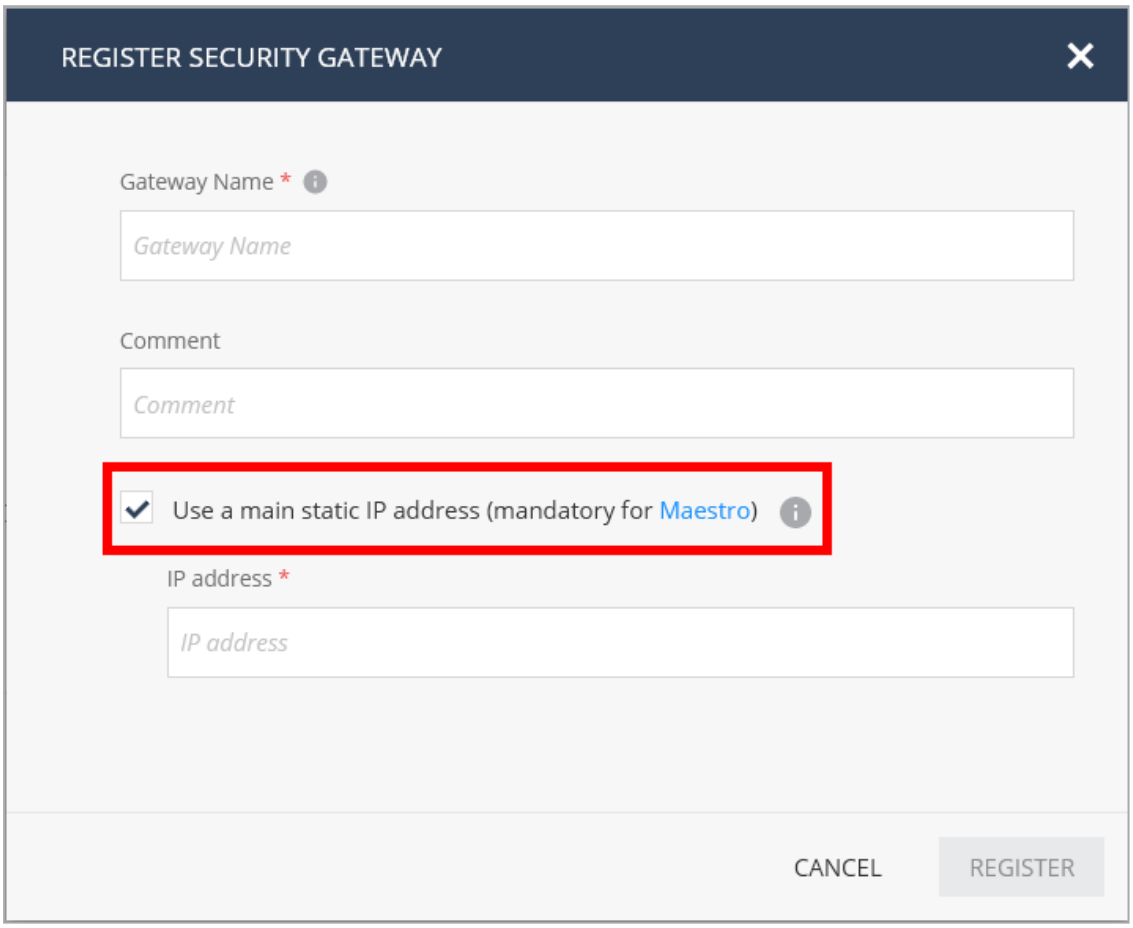
a. In the **Gateway Name** field, enter the name for this object.

b. **Optional:** In the **Comment** field, enter the applicable text.

c. To configure the Security Gateway with a static IP address, check the **Use a main static IP address** checkbox.

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

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



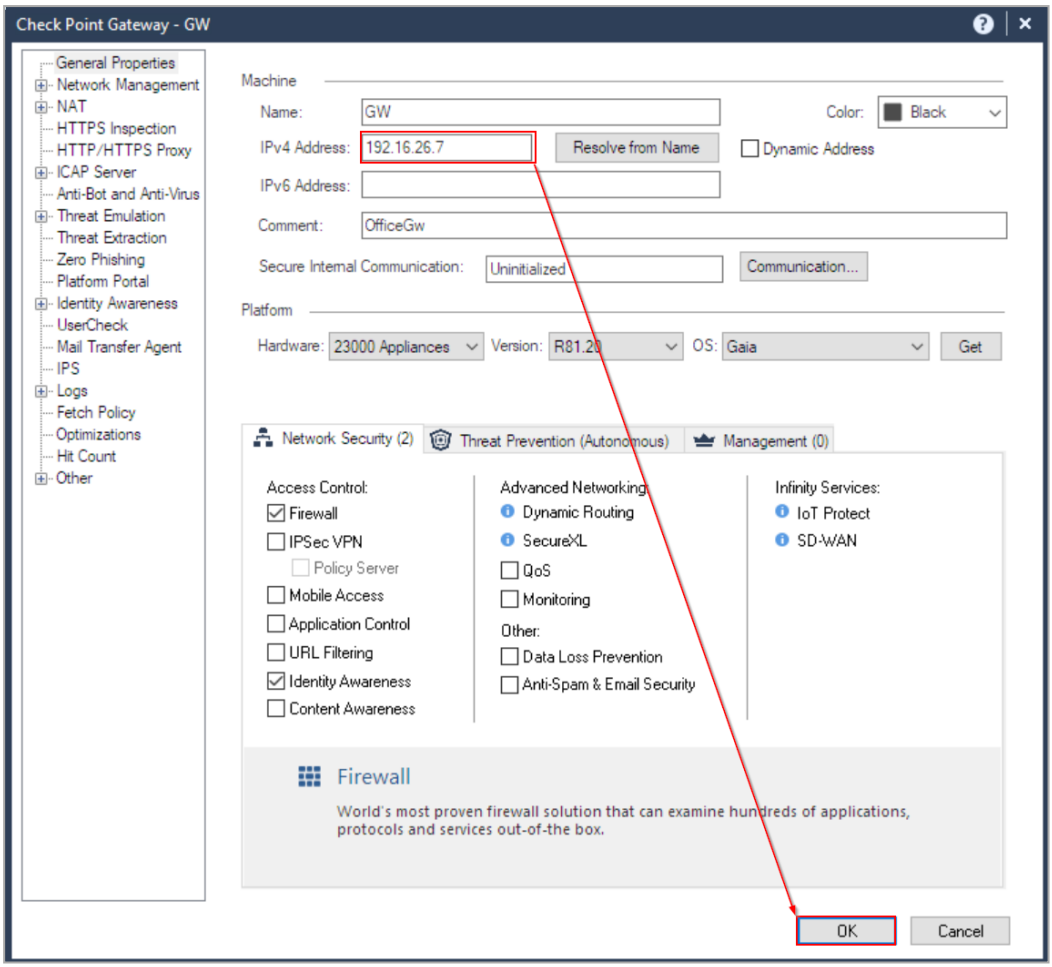
Note - We recommend configuring the main static IP address if you have a static IP address and it is not a SD-WAN Gateway.
This approach simplifies the configuration for functions such as UserCheck, NAT rules, and VPN configuration.

If the Security Gateway object already exists with a tunnel IP, use these steps to change it to a static IP:

i. Open SmartConsole or Streamed SmartConsole.

ii. Change the IP address in the Security Gateway object properties to static IP address.

iii. Click OK.



iv. Open the Security Gateway object again and click **Test SIC Status** to test SIC communication.

d. Click **Register**.

This creates a new Security Gateway object in the Service with the name that you entered.

e. Click **Connect Gateway**

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

  Note - The connection of a new Security Gateway includes two steps:

  i. Connect the Security Gateway to the service.
  Here, it is necessary to perform a step on the Security Gateway (according to the instructions) to connect the Gateway to the service.
  When the process is finished, the status in the portal shows: **Pending SIC**.

  ii. Connect the Management to the Security Gateway.
  After you connect to the service, log in to SmartConsole and start the SIC between the Management and Gateway.
  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 applicable field in the deployment template.

    b. Complete all other fields in the template and start the deployment.

    c. When the CloudGuard 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.

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

To use an Existing Security Gateway:

1. Select the Security Gateway you would like to use.

   Note - The object's IP address is changed to an IP address from the service allocated subnets below:
   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

   A new card is created with instructions about how to connect the Security Gateway to the service.

2. Click **Connect Gateway** and follow the instructions to complete the connection.

   When you connect an existing Security Gateway to the service, you must (on the gateway side) connect the gateway to the service. When this process completes, the status in the portal shows: **Registration complete**. Do not restart the SIC between the Management Service and the Security Gateway (unless you changed the SIC on the Security Gateway).

Connecting a Cluster

Procedure

For on-premises Security Cluster:

1. In SmartConsole or Web SmartConsole:
   a. From the left navigation panel, click **Gateways & Servers**.

      Create a new Cluster object, make sure to select the **Classic mode** (and **not** the **Wizard mode**).

      If you already have a cluster configured open the existing Cluster object.

      The Cluster Virtual IP address is not populated automatically. It is necessary to enter the Cluster Virtual IP address.

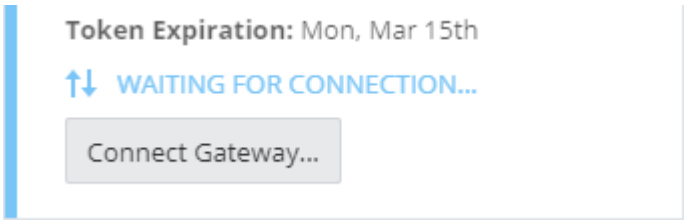
      Make sure not to give an IP address from this subnet: 100.64.x.x

   b. Create the cluster members:
      i. Navigate to **Cluster Members**.
      ii. Click **Add** > **Add New Cluster Member**.
      iii. Enter the cluster member name.
      iv. Enter a dummy IP address (later, this IP address changes automatically).

   c. Perform steps 1-b and 1-c again for all Cluster Members.
   d. Click **OK**.
   e. Publish the SmartConsole session.

2. In Smart-1 Cloud:
   a. From the left navigation panel, click **Connect Gateways**.
   b. Click the large plus icon. The **Register Security Gateway** window opens.
   c. Select **Use an existing Gateway object**.
   d. Select one of cluster members from the list and click **Register**.
   e. A **Gateway** card is created.

      Example:

   f. Click **Connect Gateway** and follow the instructions.
      i. In SmartConsole - Initiate SIC to the Cluster Member.
      ii. In SmartConsole - Publish the SmartConsole session.
   g. Perform steps 2-b - 2-d again for other Cluster Members.
3. In SmartConsole or Streamed SmartConsole:
   a. From the left navigation panel, click **Gateways & Servers**.
   b. Open the Cluster Object.
   c. Navigate to the **Network Management** tab.
   d. Click **Get Interfaces** > **Get Interfaces With Topology**.
   e. Click the MaaS Tunnel interface, and in **General** > **Network Type**, select **Private**.
   f. Finalize the topology definitions for the cluster.
   g. Install policy.

For CloudGuard Network Security Cluster

1. In the Smart-1 Cloud portal:

   For each Cluster member:

   a. Click **Connect Gateways** on the left navigation panel.
   b. Click the large plus icon. The **Register Gateway** window opens.

c. In the **Gateway Name** field, enter the name for this object.

   Optional: In the **Comment** field, enter the applicable text.

d. Click **Register**.

   This creates a new Security Gateway object in the Service with the name that you entered.

e. Click **Connect Gateway**.

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

2. In the Security Cluster deployment template:

   a. Paste the Tokens you copied from the Smart-1 Cloud portal for each member into the applicable fields in the deployment template.

   b. Fill all the other 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.

3. In SmartConsole or Web SmartConsole:

   Follow the admin guide applicable to the solution you are deploying to configure the Cluster object and Cluster members in SmartConsole.

   Notes::
   - When you enter the Cluster Virtual IP address, make sure not to give an IP address in the subnet 100.64.x.x.
   - When you add the cluster members to the cluster object, use the existing members from step 1.

Onboarding a new Quantum appliance using Zero Touch deployment

Procedure

Run this procedure to on-board a new appliance in Zero Touch and configures it as a Security Gateway or a Cluster Member.

1. Remove your new appliance from the shipping carton, connect the power cable and turn on the appliance.
2. The light on one of the network interface ports starts blinking.
   - **With a DHCP Server:**

     Connect the network cable to that interface port.

     Your connection must lead to the environment with a working DHCP server.
   - **Without a DHCP Server:**

     Configure one of the interfaces with the applicable networking information:

     a. Connect to the command line on the appliance.

     b. In the Expert mode, disable the Zero Touch DHCP:

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

     c. In Gaia Clish, configure the applicable 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 applicable 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 the applicable 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 that interface port.
3. Navigate to **Connect Gateways** page in the Smart-1 Cloud portal.

4. A card that represents your appliance appears.

   This may take 2-3 minutes.

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

5. Click the card for your appliance and enter all applicable information, then click **OK**.

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

6. Follow the instructions in the portal.

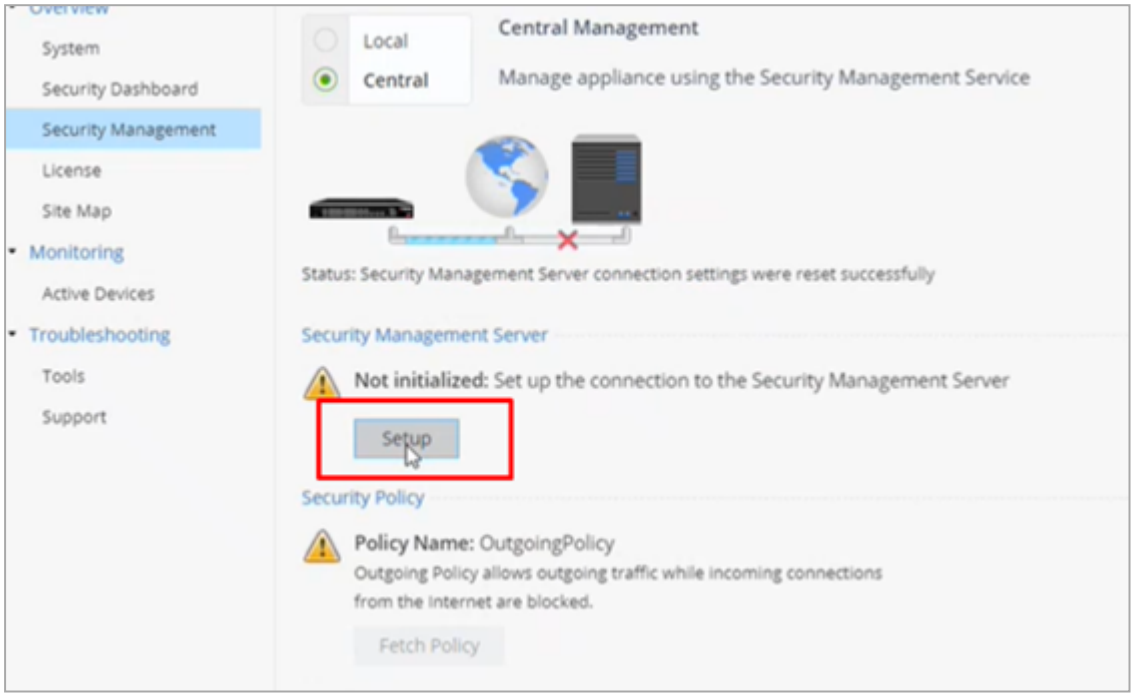
7. After the card status changes to **Registration completed**, you can configure your new Security Gateway in SmartConsole.

Connecting a Quantum Spark Appliance

Procedure

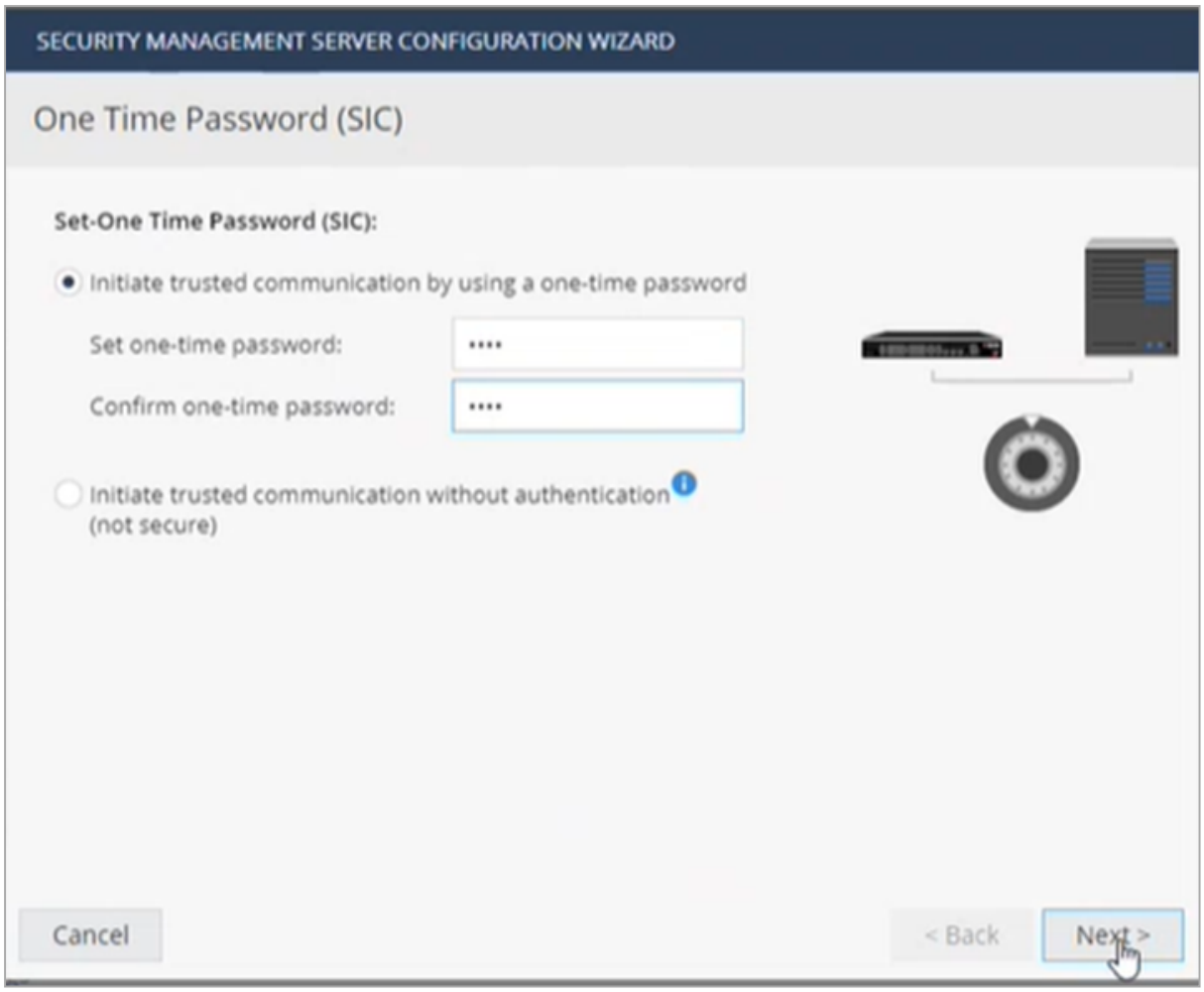
To connect Quantum Spark to Smart-1 Cloud, follow these steps:

1. Connect to the Quantum Spark WebUI and in the Security Management tab, click **Setup**.

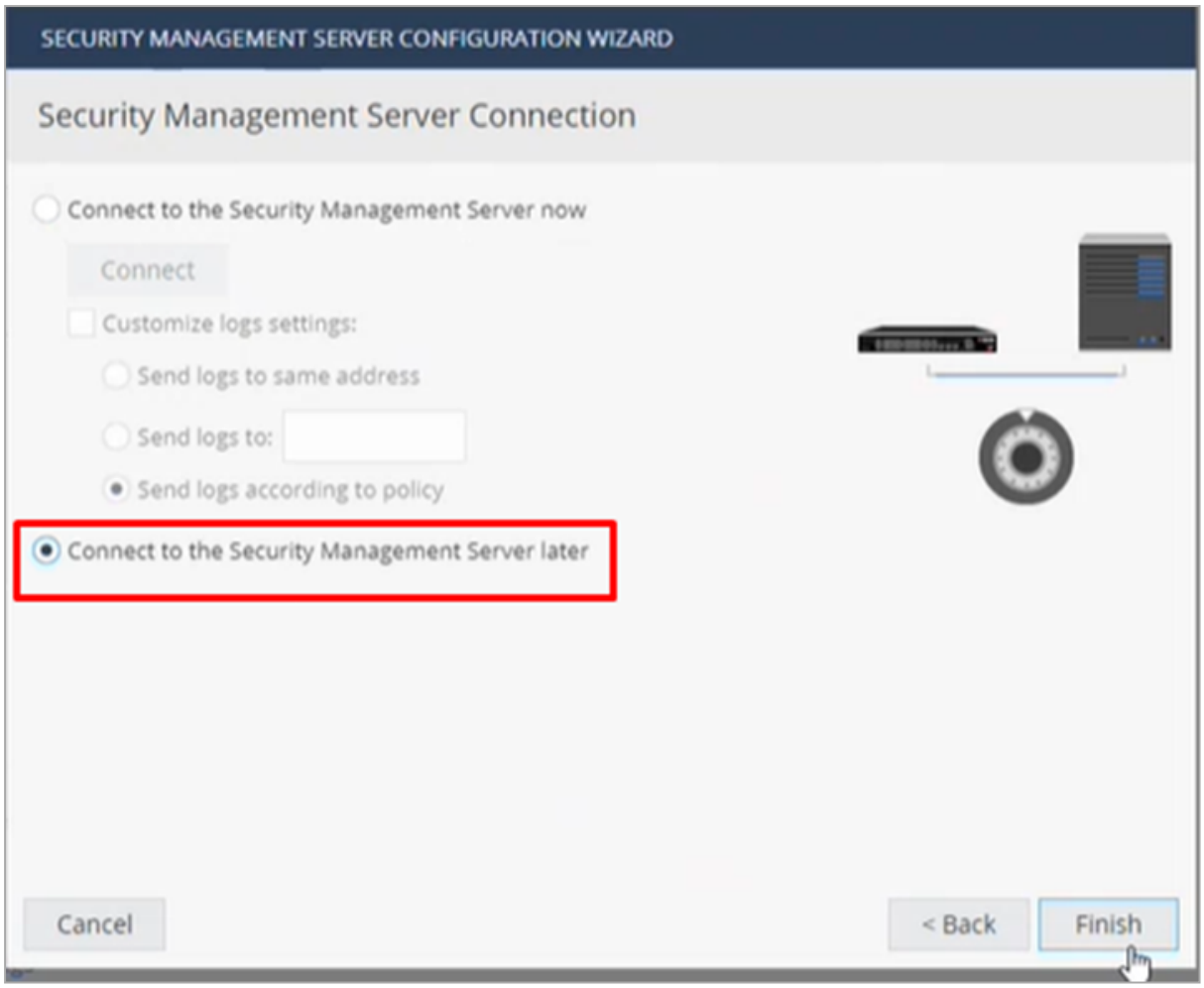


2. Check the **Use Security Management service** check box and click **Next**.
3. Click **Use the Infinity Portal to generate a new authentication token** and add the token.
4. The status changes to: Connected successfully to the Security Management Server. Click **Next**.

5. Add the one-time password and click **Next**:



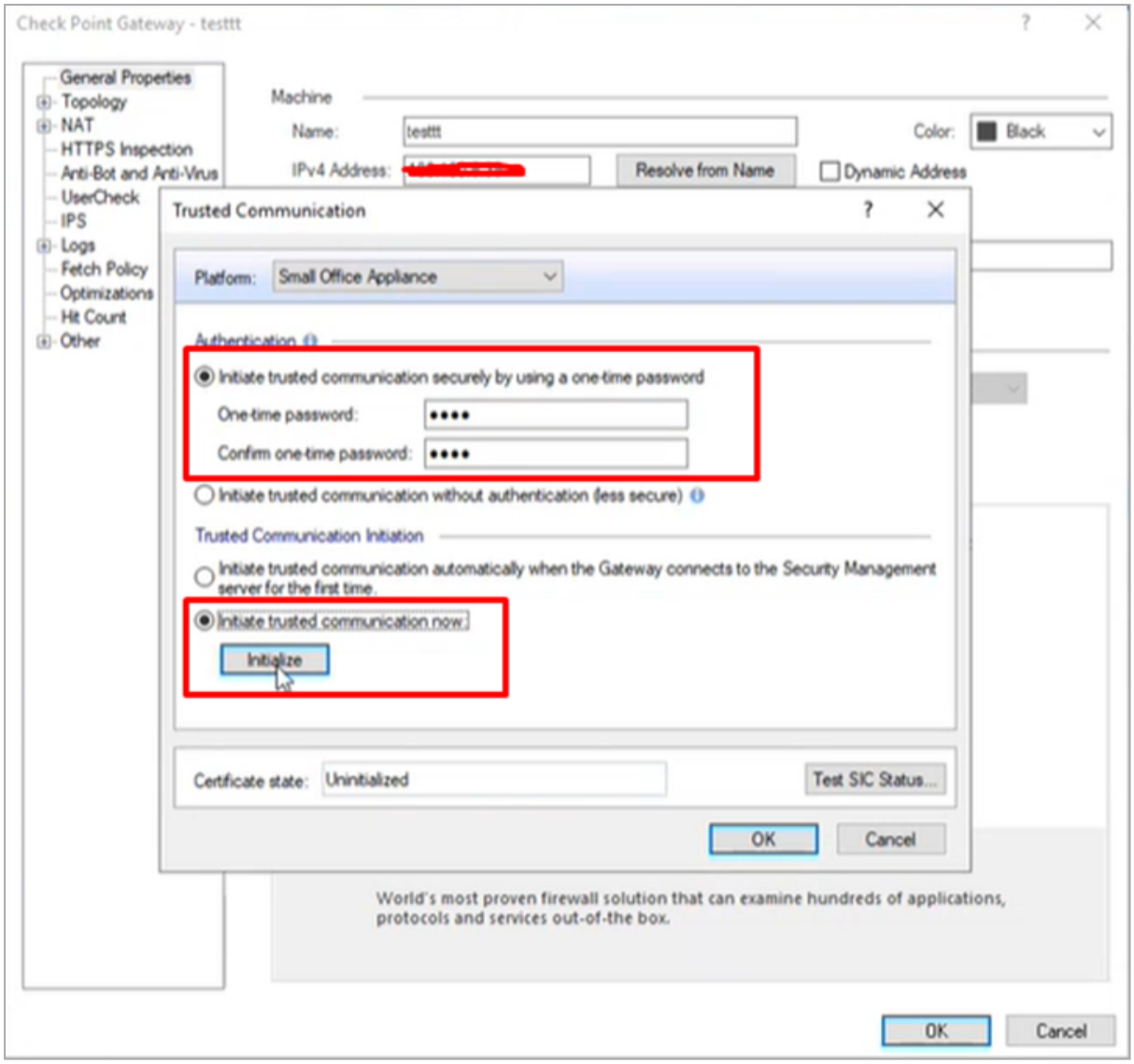
6. Check **Connect to the Security Management Server Later** and click **Finish**.



You can see in the WebUI that it is waiting for a connection from The Security Management.

7. Open the Security Gateway object in SmartConsole and ensure the Hardware type is correct.

8. Enter a one-time password, check the **Initiate trusted communication now** check box and click **Initialize**.



9. Save the object in SmartConsole and publish the changes.

Connecting a Maestro Security Group

Important - This procedure supports only Maestro Security Groups that runs 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.

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.

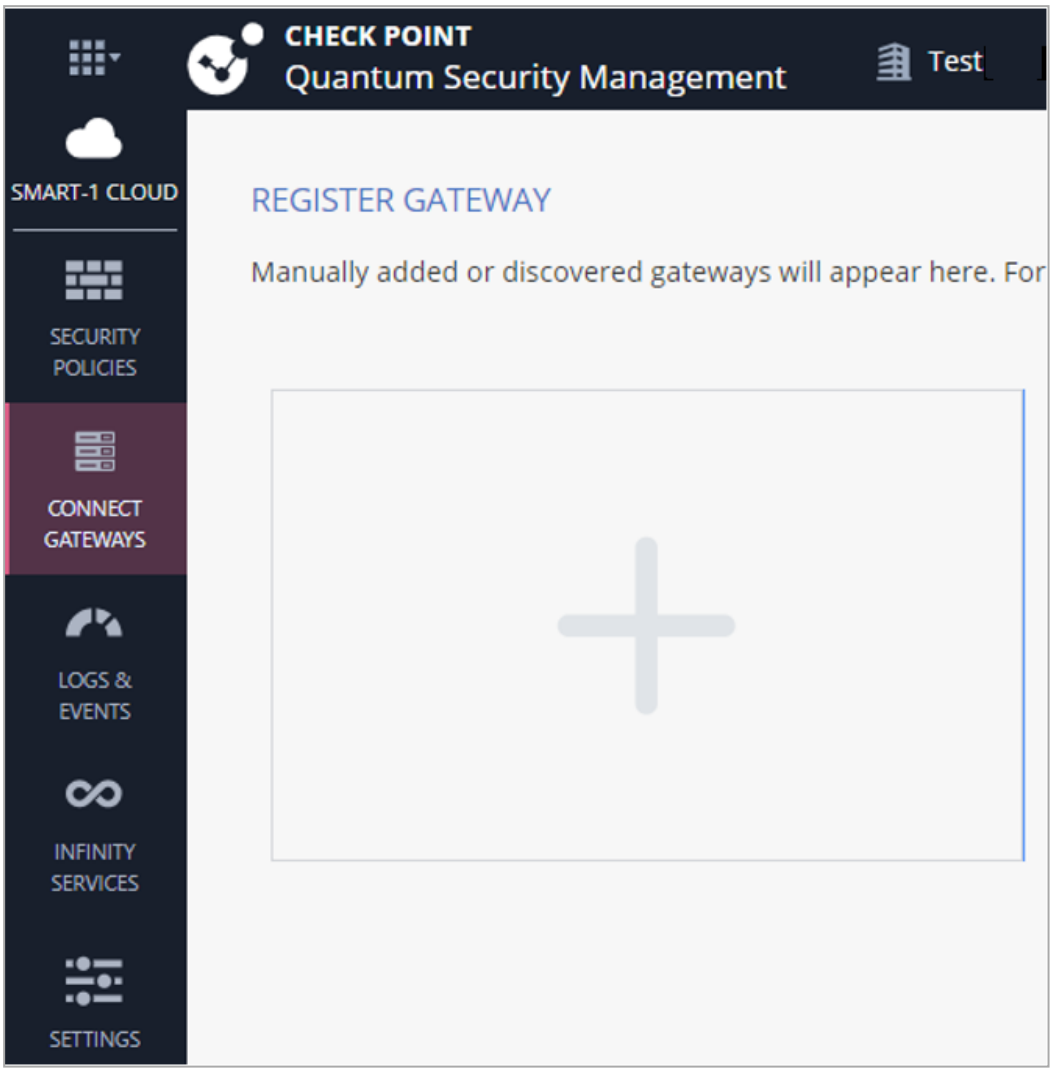
2. Install the required Hotfixes on the Security Group: For details, refer to sk181495.
3. Connect to the Smart-1 Cloud Portal.

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

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

   i. From the left navigation panel, click **Connect Gateways**.

   ii. Click the large plus icon.



The **Register a New Security Gateway** window opens.

Note - The server detects if there are existing gateway objects in the database.
For existing gateway objects, the server asks:
`Do you want to create a new gateway object, or use an existing gateway`

iii. Create a New Gateway object:

i. In the **Gateway Name** field, enter the name for this object.

ii. **Optional:** In the **Comment** field, enter the applicable text.

iii. Select **Configure as Maestro**.

iv. 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).

v. Click **Register**.

This creates a new Security Gateway object in the Service with the name that you entered.

vi. Click **Connect Gateway** and follow the instructions to complete the connection.

Note - The connection of a new Security Gateway includes two steps:

i. Connect the Security Gateway to the service.
Here, it is necessary to perform a step on the Security Gateway (according to the instructions) to connect the gateway to the service.
When the process is finished, the status in the portal shows: **Pending SIC**.

ii. Connect the Management to the Security Gateway.
After you connect to the service, log in to SmartConsole and start the SIC between the Management and Gateway.
The portal shows **Registration complete**.

4. Connect with SmartConsole to the Smart-1 Cloud Portal.

   See *"Log in to SmartConsole" on page 43*.

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

6. Open the Security Gateway object for this Maestro Security Group.

7. From the left, click the **General Properties** page.

8. Establish SIC:

   a. In the Secure Internal Communication field, click Communication.
   b. Enter the one-time password you configured on the Maestro Orchestrator when you created the Security Group.
   c. Click **Initialize**.
   d. Click **OK**.
9. Publish the session.
10. Install the Access Control policy on the Security Gateway object.
11. Install the Threat Prevention policy on the Security Gateway object.

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

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

- Web browser (Web SmartConsole).
- Desktop SmartConsole with Windows.
- Streamed SmartConsole
- Desktop Portable SmartConsole (does not require administrator credentials to install on a Window's computer).

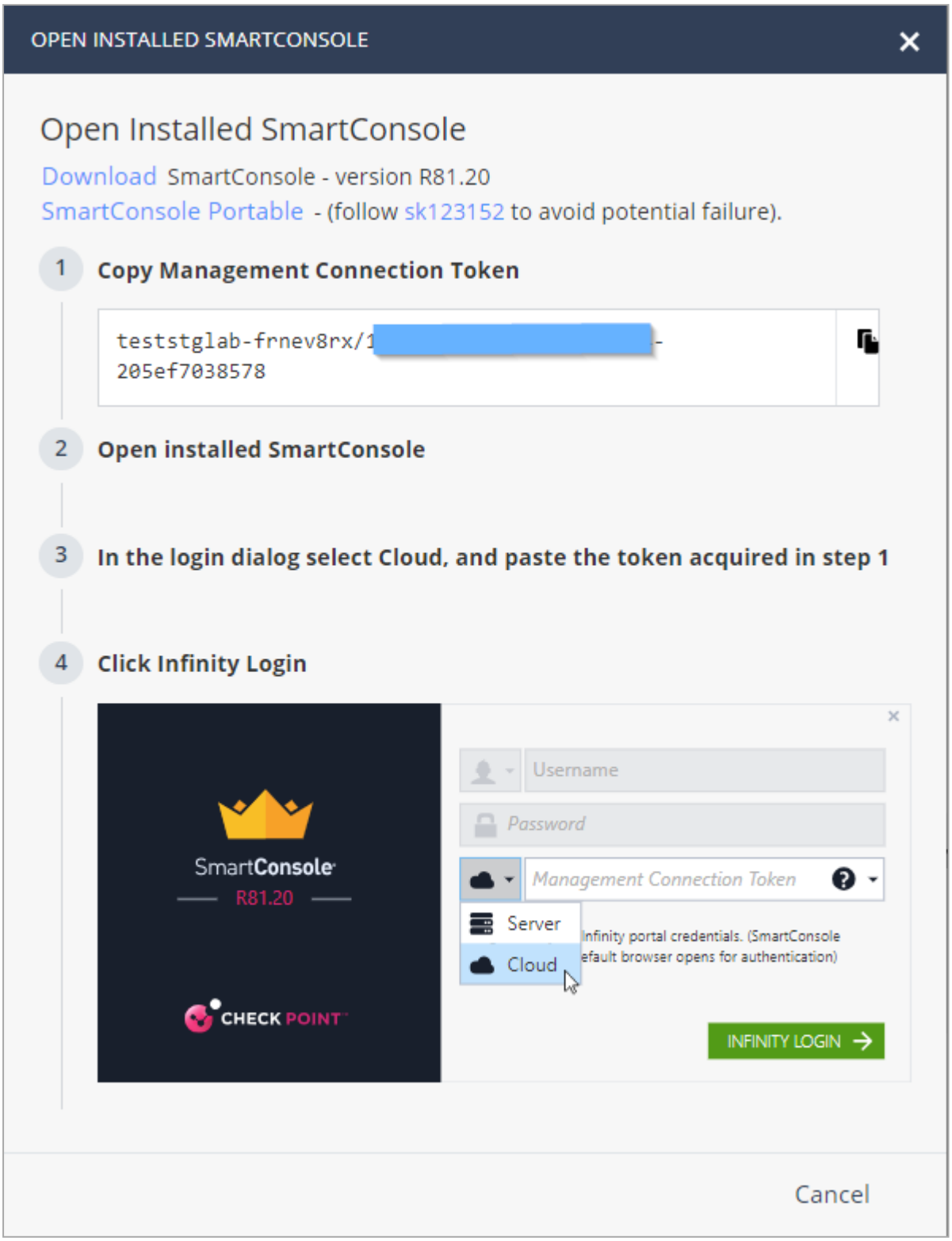
Note - Because of port tunnelling, a desktop SmartConsole can only establish one connection to a Smart-1 Cloud tenant on the same PC.
As an alternative, you can use Web SmartConsole or Streamed SmartConsole.

Log in to SmartConsole from a web browser

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

Using the Desktop SmartConsole application

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



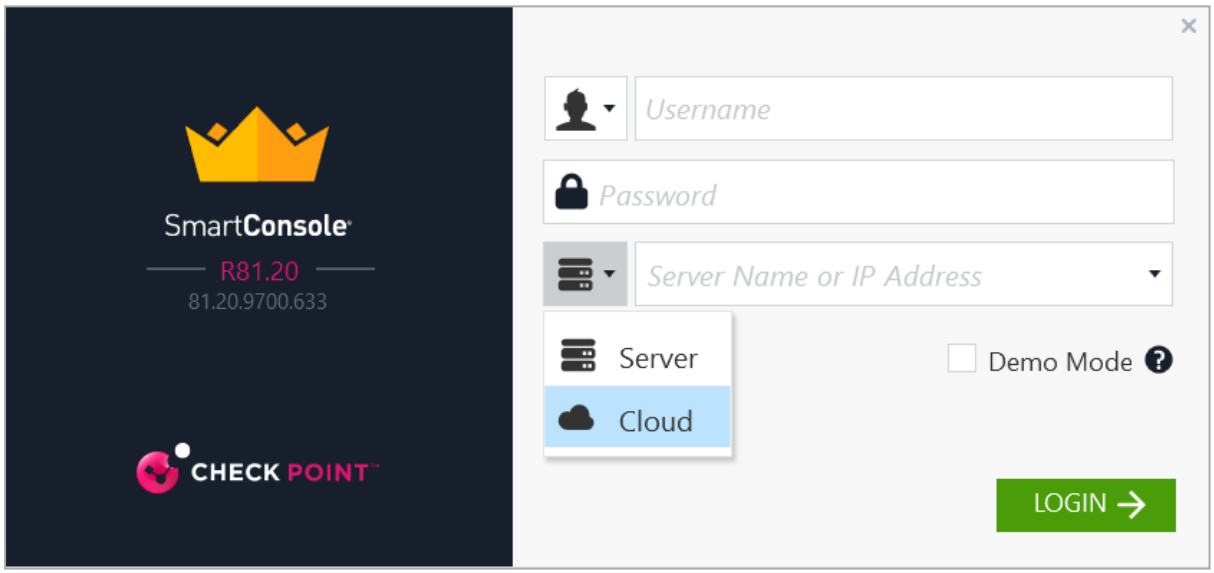
Note - Download SmartConsole as a Windows installation or as a Portable (ZIP) version.

1. Download SmartConsole from the **Open Installed SmartConsole** window.
2. Select the desired 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 instructions on the screen.

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

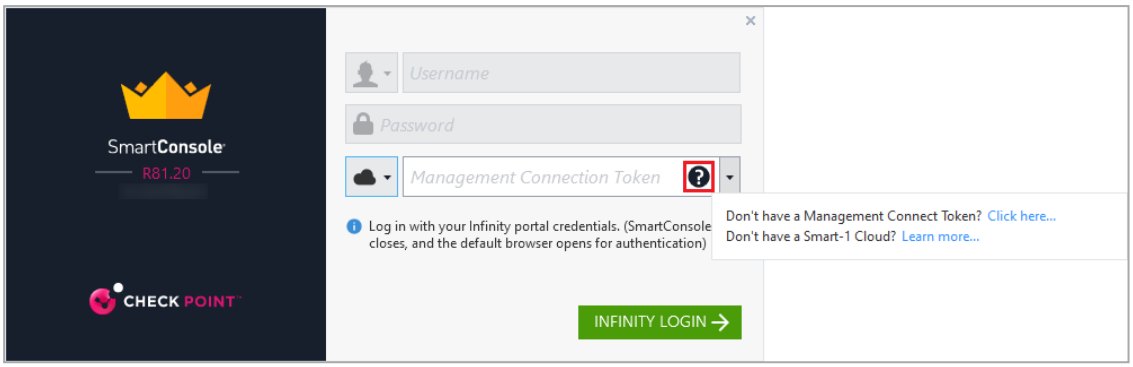
   See the R81.20 SmartConsole Online Help Guide for more information about how to use SmartConsole.
5. From the **server** drop-down list, select **Cloud**.



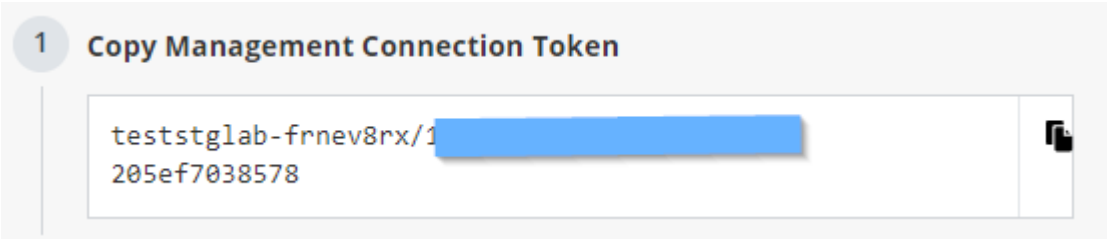
6. Enter the Management Connection Token.

   Notes:

- You can hover over the help icon to see the applicable links:



- Get the token on the **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** and let the browser open Check Point's SmartConsole.

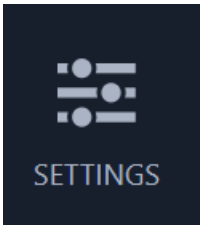
    SmartConsole opens for you to start work.

Log in to Streamed SmartConsole

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

The Streamed SmartConsole automatically opens. You are now logged in to SmartConsole, which runs on the web.

Using the Settings



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

General

It is possible to read information and send commands to the Check Point Management Server. Same as you create objects and Security Policies and deploy them in SmartConsole, you can do the same tasks with APIs.

Service Information:

- **Status**: Shows the service status.
- **Service Identifier**: Unique service identifier based on the prefix provided in the service creation. When you contact Check Point, you must use this service identifier.
- **Version**: Security Management software version.
- **License Status**: Active for customers who have purchased a Smart-1 Cloud license or a trial for customers who run in trial mode.

To change the required log retention period

To update the period, it is required to keep the logs:

1. On the Smart-1 Cloud home page, select **Settings** > **General**.
2. Click **Log Server Settings**.
3. In the **DESIRED LOG RETENTION PERIOD** enter number of months.

Logs are deleted after the defined period. If available storage cannot keep the desired log retention period, a notification is sent to your email.

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 web request structure at this time.

To copy these details to a clipboard, click the clipboard button.

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

To restart your service

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

   The **Restart Environment** confirmation window opens.
3. Click **Restart Environment** and follow the instruction on the screen.
4. Click **Restart**.

Note - **Restart Environment** restarts the Smart-1 Cloud environment as equivalent to cpstop and cpstart in an on-premises management environment.

Migrate

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

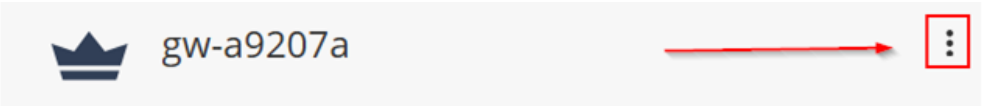
Note - The migration operation overwrites tenant information (the migration process does not merge tenant information).

Recommended option - To migrate a Self-Hosted (on-premises) Security Management environment that is connected to Infinity Portal

Note - For information on how to connect an On-Premises Management Server to Infinity Portal, refer to sk177205.

Important - You can migrate a self-hosted Security Managemen environment to Smart-1 Cloud only if Smart-1 Cloud was not already created in this Infinity Portal tenant.

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



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

   Important - The migration process can take a while. You do not have access to the Smart-1 Cloud application during the import process.
   When the import finishes, an email is sent to you, and the service unlocks.

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

6. When the migration is complete successfully, in Smart-1 Cloud, navigate to **Connect Gateway**.
7. Click the plus (**+**) icon below the existing Security Gateway, select the Gateway you want to connect and follow the on-screen instructions.
8. For a Security Gateway that runs a version lower than R80.40 with Jumbo Hotfix Accumulator Take 89, you must reset the Secure Internal Communication (SIC) on the Gateway before initializing the communication from SmartConsole to the Security Gateway. For more information, refer to 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, it is not necessary to reset SIC on the Security Gateway.

To migrate 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 the Infinity Portal, go to **Settings** > **Migrate**.
2. Below **Export Data**, click **Download** to download the migration tools for migrating on-premises Security Management to Smart-1 Cloud.
3. On the on-premises Security Management, run export.
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 can take a while. During the import process, you do not have access to the Smart-1 Cloud application.
   When the import finishes, an email is sent to you and the service is unlocked.

6. When the migration completes successfully, in Smart-1 Cloud navigate to **Connect Gateway**.
7. Click the plus (**+**) icon below the existing Security Gateway, select the Security Gateway you want to connect and follow the on-screen instructions.

8. For a Security Gateway that runs a version lower than R80.40 with Jumbo Hotfix Accumulator Take 89, you must reset the Secure Internal Communication (SIC) on the Gateway before initializing the communication from SmartConsole to the Security Gateway. For more information, refer to 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, it is not necessary to reset SIC on the Security Gateway.

Cloud Management Extension (CME) Configuration

Smart-1 Cloud lets administrators configure and directly show Cloud Management Extension (CME) status in the GUI.

CME enables cloud-native integration between Check Point CloudGuard Network solutions and Cloud platforms.

As a Service that runs on Smart-1 Cloud, it continuously monitors CloudGuard Network solutions deployed in Azure and Amazon Web Services (AWS) and synchronizes them.

Limitations:

- The GUI does not support the Google Cloud Platform (GCP).
- The GUI does not support the configuration of custom scripts on the Security Gateway.

How to enable CME in Smart-1 Cloud

1. In the Quantum Smart-1 Cloud view in the Infinity portal, go to **Settings** > **CME Configuration**.
2. In **General Information**, click **CME Status**, and it turns to On. The CME management name displays in the box below.

Add an account

1. To add an account, click **Accounts (Controllers)**.
2. Click **New**. The **Add Account** window opens.
3. Give the account a name.
4. In the Vendor box, select AWS or Azure.
5. Enter the parameters.

Parameters for AWS

Parameter	Description
Access Key	AWS Access Key ID.
Secret Key	AWS Secret Key.
Regions	The AWS regions in which the gateways are being deployed.
STS Role	The STS Role ARN of a role to assume.
STS External ID	An optional STS External ID to use when assuming a role in account.
Communities	List of VPN communities that the account can use. VPN community is used for Transit Gateway Auto Scaling Group solution.
Scans	Enable auto-provisioning of the objects you select.
Sub-Accounts	Configure the sub-account properties. The sub-account name must be unique. Enter Access Key Secret Key,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.

Add Security Gateway Configurations

1. To add Security Gateway configuration, in the CME configuration page, click **Gateway Configurations (Templates)**.
2. Give the Gateway a **Name**.
3. Select the applicable **Account** for the Gateway.
4. Select the Gateway Version.
5. Enter a One time password.

6. In Access Control, select the policy to install on the Security Gateway.
7. Select the checkbox near the Access Control and Threat Prevention blades you want to enable on the Security Gateway.

Advanced Configuration

To add support for AWS Transit Gateways, select the Transit Gateway checkbox.

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

Parameters for AWS Transit Gateway

Parameter	Description
VPN Community	A VPN Star community in which the VPN Gateway is the center.
TGW static routes	Enter network addresses (CIDR) separated by a comma to create a static route on each Gateway of the Transit Gateway auto-scaling group.
TGW spoke routes	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. Use a comma to separate multiple values.

For more information on CME, see the *Cloud Management Extension Administration Guide*.

Forwarding Events to SIEM

Event Forwarding is an easy and secure procedure to export logs. You can forward data, logs, events, and saved applications data from a Check Point environment to a SIEM (Security Information and Event Management) provider, such as Splunk, QRadar, or ArcSight. These SIEM providers process large amounts of data and show it for analysis in created dashboards or sent notifications.

Forward to SIEM vs. Event Forwarding

Forward to SIEM and event forwarding are used to send event logs to a monitoring system.

Currently, event forwarding supports only Syslog format, while Forward to SIEM supports Syslog, Splunk, LEEF, Generic, LogRhythm and RSA formats.

Forward to SIEM configuration

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

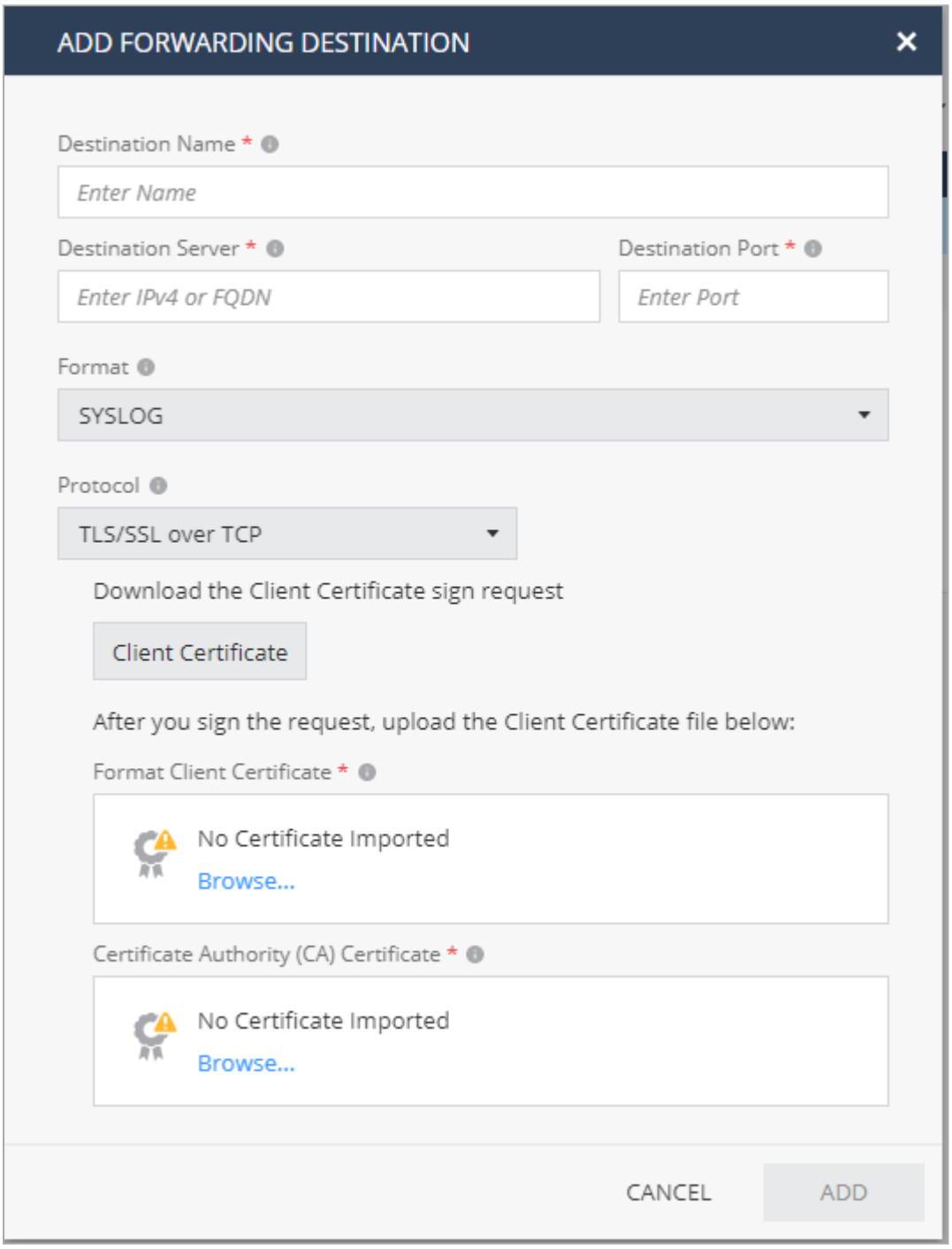
In the configuration page you see a table with forward to SIEM destinations, and information for the destination, such as status, encryption, name, target port, protocol and format.

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, ca 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:

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

Procedure:

- Click the **Client Certificate** box to download the certificate request (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 certificate.

  Important - In case some time has passed between making the certificate request and uploading the certificate, you can close the Add New Destination window, and in a later time open it again, fill all the details but do not click the Client Certificate box again, as this will create a new request.
  Just click **Browse** to upload the certificate and continue with the new destination creation.

- Upload the Certificate Authority (CA) certificate.

Editing the destination

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

You can change any one of the destination properties, except the destination name.

Deleting a destination

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

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

Start, stop or restart a destination

To start, stop or restart destination, on the Forward to SIEM Configuration screen select a destination or multiple destinations, click **More Actions**, and select the action you want to perform, and select **Yes**.

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

Troubleshooting

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

- Make sure that your Security Gateway does not block traffic from the Smart-1 Cloud. public FQDN:
  - `eu-west-1.g04.checkpoint.com`
  - `us-east-1.g04.checkpoint.com`
  - `ap-southeast-2.g04.checkpoint.com`
- Check that 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 3rd 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`

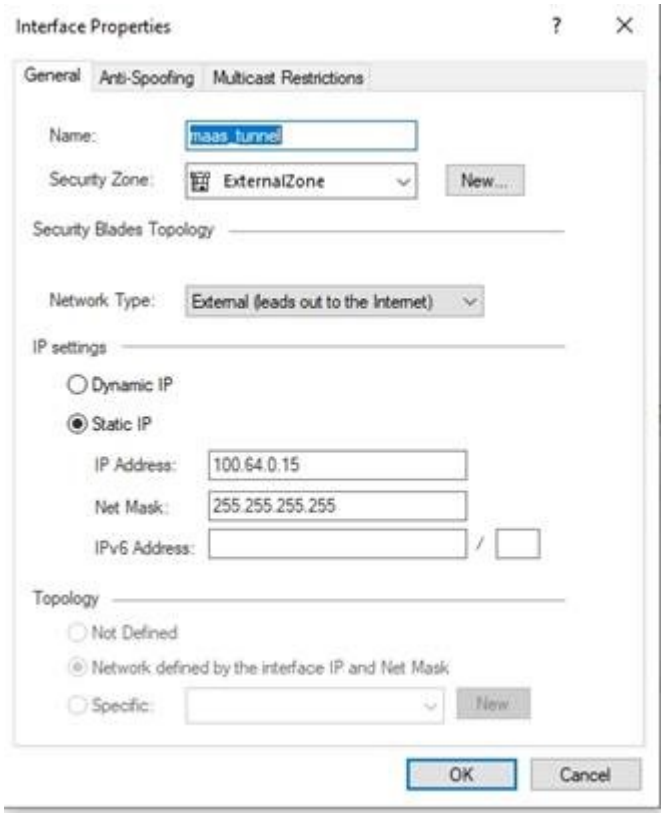
How to Connect a Quantum Spark Appliance with a Dynamic IP

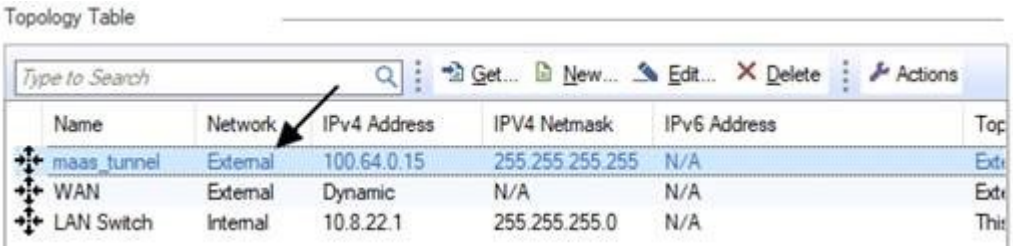
To connect a Quantum Spark Appliance with a Dynamic IP:

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 SmartConsole, navigate to the **Objects Management** tab.
2. On the **Server to connect** to field, select the host object you created for this Domain Controller.
3. Manually add the branch(es).

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

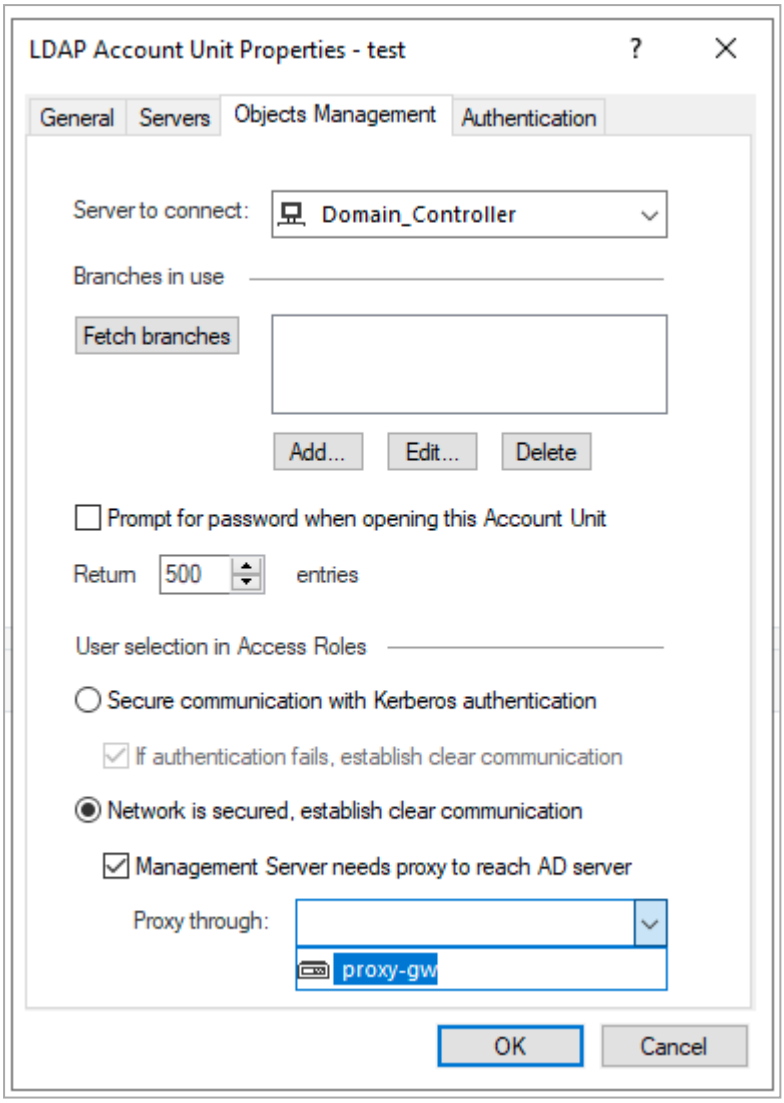
   The branch name is the suffix of the Login DN that begins with `DC=`.

   Example:

   If the Login DN is: `CN=John.Smith,CN=Userse,DC=mycompanyDC=com`

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

5. 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.

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.

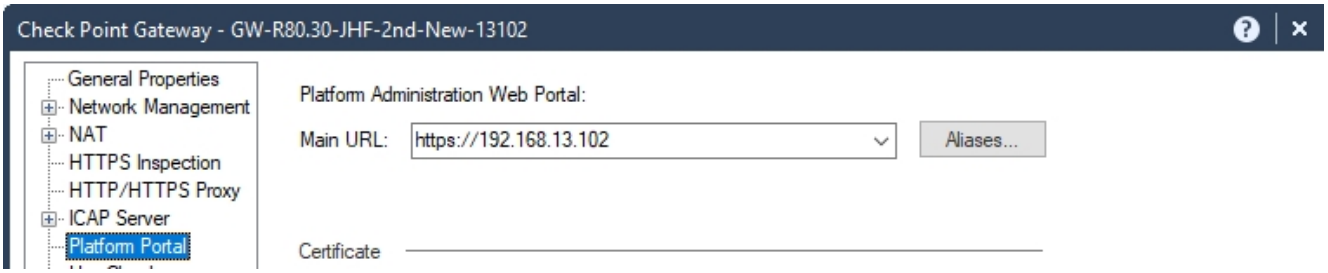
To allow access to the Security Gateway Gaia Portal:

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.



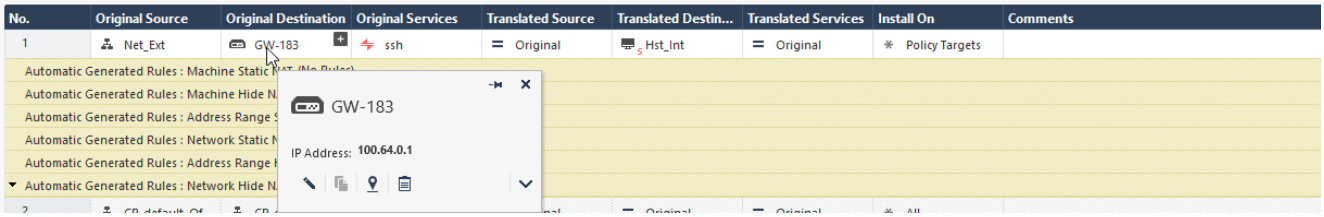
How to Configure Access from the Security Gateway External IP Address to the Internal Asset with Static NAT

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.

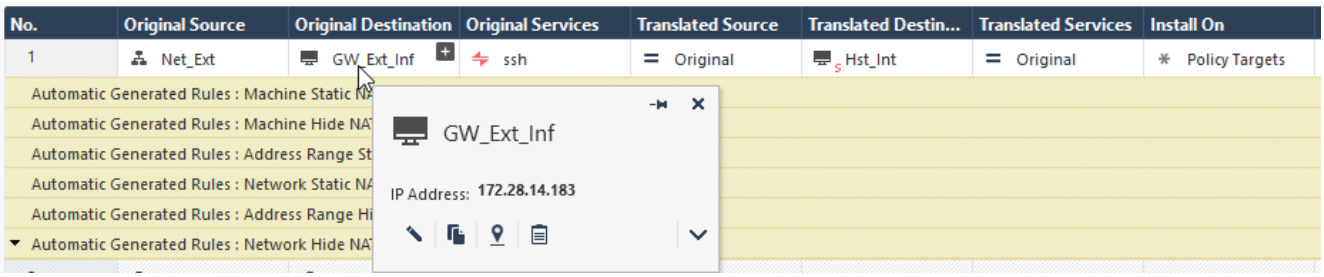
Consequently, the destination IP address of this rule is actually a virtual tunnel IP address, and not the Security Gateway's physical external interface.

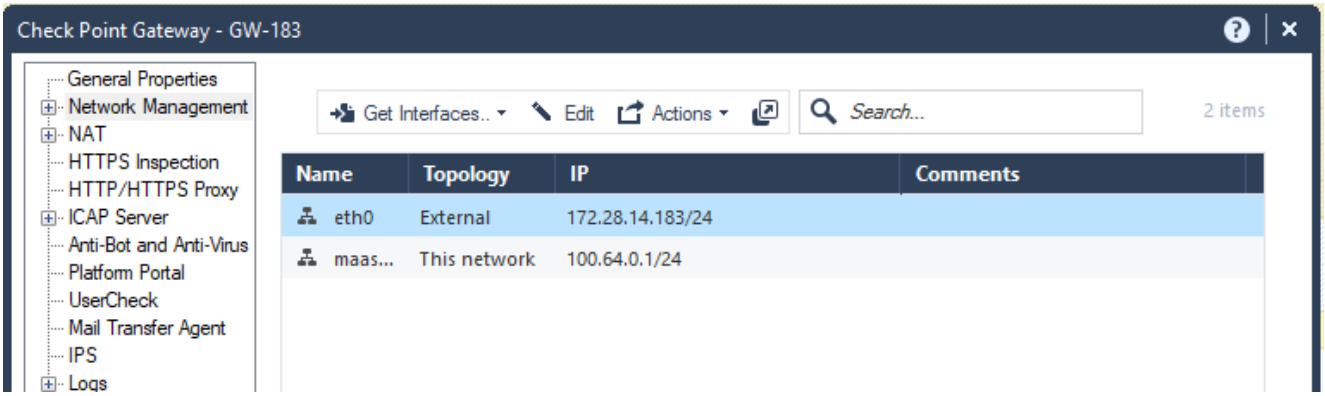
This screenshot shows the IP address in the tooltip:



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**.

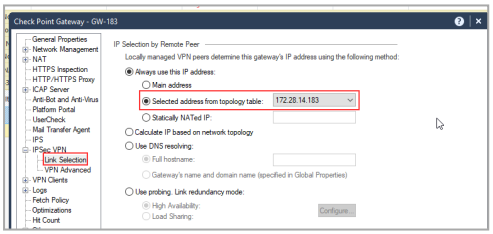
Note - If you create the Security Gateway object with a static IP address and not with the tunnel IP, link selection is not required. You can use the standard settings for VPN configuration on the Security Gateway.
We recommend configuring in Smart-1 Cloud a static IP address in the Security Gateway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

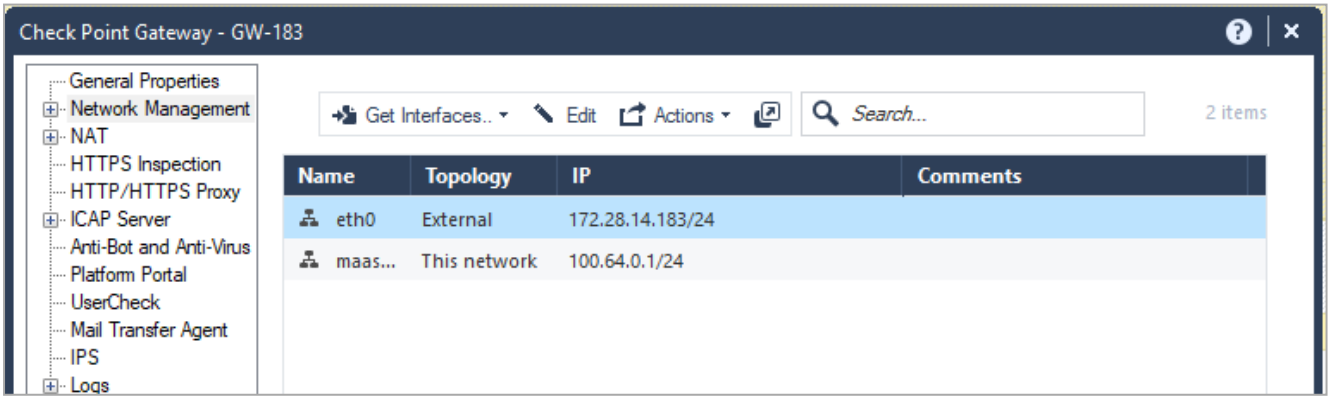
Consequently, you cannot use the **Main address** option.

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".

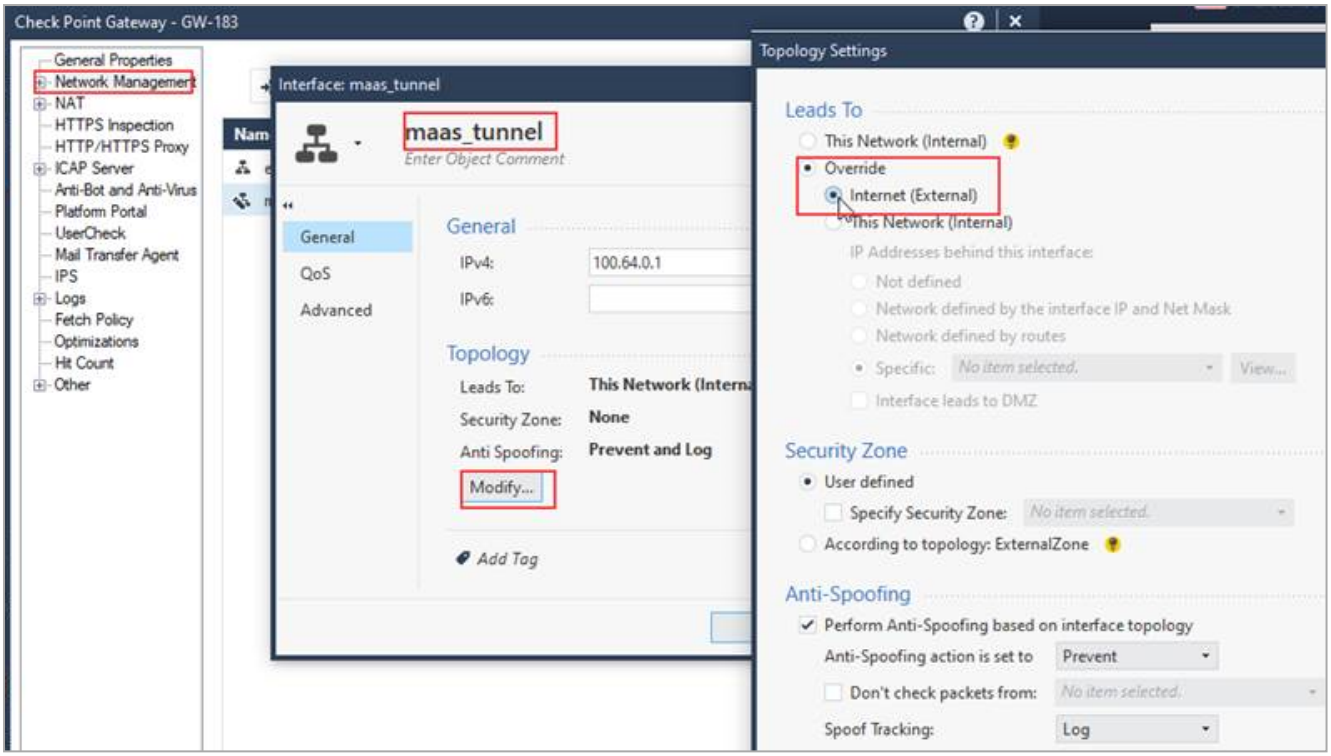
To resolve this issue, it is necessary to configure the topology of the `maas_tunnel` interface as" **Internet (External)**."

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

Expected Behavior and Known Limitations

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

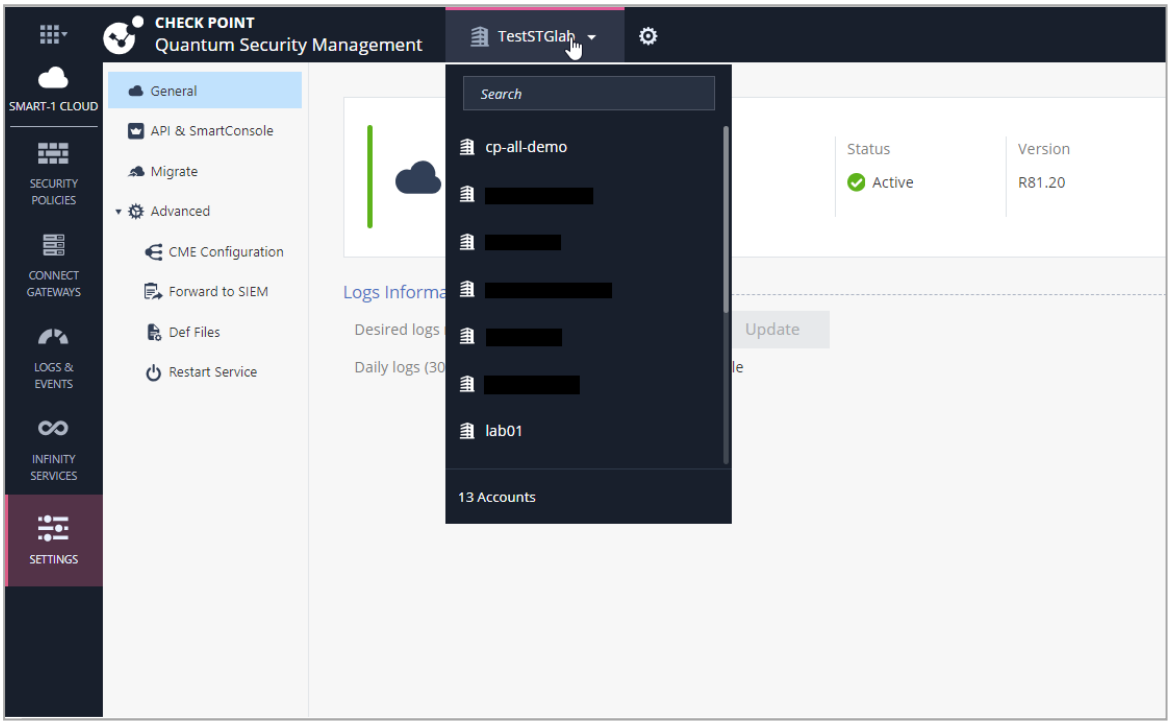
Smart-1 Cloud enables administrators to manage their security policies, network objects, and logs analysis similar to on-premises deployments from a web browser.

In some cases, there may be changes in behavior when you compare the cloud environment to the on-premises environment.

Below is a list of expected behavioral changes and current known limitations.

General 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.
  - Switching between the different environments in the portal is easy. This is done 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.
  - It is currently not supported to share global objects, global policies and global rules between the environments.
- **Management Objects**
  - The management object in Smart-1 Cloud is read-only and is not seen in the gateways and servers view. It is visible in the object explorer in read-only.
  - Running actions on the management object is not required. As part of the service, backups of the environment run on a regular basis - every 12 hours.
  - SSH access to the Management server is not possible, for actions that must have SSH access contact support.

- **Management Login - Supported Methods**
  - Log into SmartConsole (use the infinity portal credentials), examine the available Infinity Portal login methods. See the *Infinity Portal Administration Guide*.
- **Two-Factor Authentication**
  - For log in to the Infinity Portal - 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 of 99.9% up time, no additional HA solution is required.
- **Not Supported Features**
  - Managing of VSX Gateways and VSX Clusters.
  - SmartProvisioning.
  - In SmartTasks, the **Run Script** feature is not supported. (Smart-1 Cloud supports **Send Web Request** and **Send Mail** only).

    Note - To access the on-premises/cloud SMTP server, you must allow inbound traffic from Smart-1 Cloud FQDNs based on your region:
    - EU: eu-west-1.g04.checkpoint.com
    - US: us-east-1.g04.checkpoint.com
    - AP: ap-southeast-2.g04.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 popup suggestion bar stays empty).
  - Upgrading Quantum Spark Gateways from the CDT (Central Deployment Tool) is not supported.
  - SmartUpdate is not supported.
- **Management APIs that are *not* supported**

  Note - Running these APIs can cause unwanted behavior.
  - `run_script` on the Management Server object
  - `migrate-export-domain`
  - `put-file`
  - SmartTasks

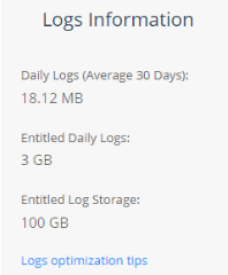
- **CloudGuard Edge**
  - CloudGuard Edge is supported with version R80.20.05 and higher.

    Best Practice - We recommend to always upgrade your CloudGuard Edge appliance to the latest available version.
  - For more information, see:
    - sk161272 - CloudGuard Edge
    - sk166513 - CloudGuard Edge Known Limitations
- **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* with 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*.
  - CME Automatic Hotfix Deployment is not supported.
  - Migration of an on-premises management database with CloudGuard Network Auto Scaling gateway is not supported. Issues can occur with the communication between Smart-1 Cloud and the existing CloudGuard Network Auto Scaling gateways. The connection of a CloudGuard Network Auto Scaling gateway as a new gateway is supported.
- **VPN**
  - Automatic MEP Topology is not 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
- The support of SmartEvent Views and Reports is for each purchased license - activation is done automatically based on the purchased license.
- SmartEvent Policies are not supported. Consequently, it is not possible to configure custom events or automatic reactions.

  Important - The SmartEvent Software Blades and Indexing mode checkboxes (in the Management Server object) must stay cleared - this is the expected behavior.

- Possible latency of maximum two minutes from the time the gateway creates the log until it is visible in **Logs & Events**.
- OPSEC and LEA are not supported.
- 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, this includes *action*, *type*, and *product*.

- To filter logs for only one value, when `Blade/Product` has some values, add wildcards before and after the Blade's name, such as "`blade:*Firewall*`."
- 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
- 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**.
- 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** - In some fields might cause "`query failed`" error - in this case, open a support ticket.
- Opening log file from **Logs & Events** is not supported.
- Tufin: Hostname or LogID = Service Identifier, (Logs from forward to SIEM configuration (Syslog)).

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

Migration

To migrate a Security Management Server to Smart-1 Cloud, when moving from on-premises to Smart-1 Cloud, before you start review these requirements.

In some cases, you must change the configuration before or after the migration.

Important to know before you start:

1. Migration is supported from version R81.10 and higher.
2. Reset SIC post the migration:
   a. Gateways running R80.40 Jumbo Hotfix Accumulator Take 89 or higher, it is not necessary to reset SIC post the migration.
   b. All others Gateways must reset the SIC on the gateway before you initialize the 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 appliances and or version	See the list of *"Supported Gateways and Versions" on page 9*. A Gateway that belongs to an unsupported appliance or 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 these changes are made: ▪ Remove NAT configuration ▪ Remove Proxy configuration ▪ It ignores old network configuration
Endpoint Manager	Before you run the export on the on-premises management, disable the Endpoint Policy Management Software Blade and install the database.
Consent flag - Automatically download Blade contracts and other important data	Enable: Flag is enabled by default during the 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 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. If your need to migrate from Standalone configuration to Distributed configuration before the migrate to Smart-1 Cloud, follow the instruction in sk179444 - Migration from a Standalone environment to a Distributed environment.

Configuration	Required Step
Authentication methods: OS Password, SecurID, RADIUS, TACACS, API Key	Change the authentication method to a Check Point password. If the administration 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, you must change the IP address to a different subnet.

Limitation

Migration from pre-R81 Multi-Domain Management server to a Smart-1 Cloud server fails, for details refer to sk180650.

Integrations with Other Services and 3rd Party Tools

- Integrations of 3rd party tools and Smart-1 Cloud are supported with the use of the Management APIs.
- Integration with 3rd party tools that use SSH access or OPSEC/LEA to the Management Server are not supported.
- Known integrations not supported:
    - ThreatCloud Managed Security Service

Troubleshooting

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 66*.
"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.

Best Practices

Management APIs

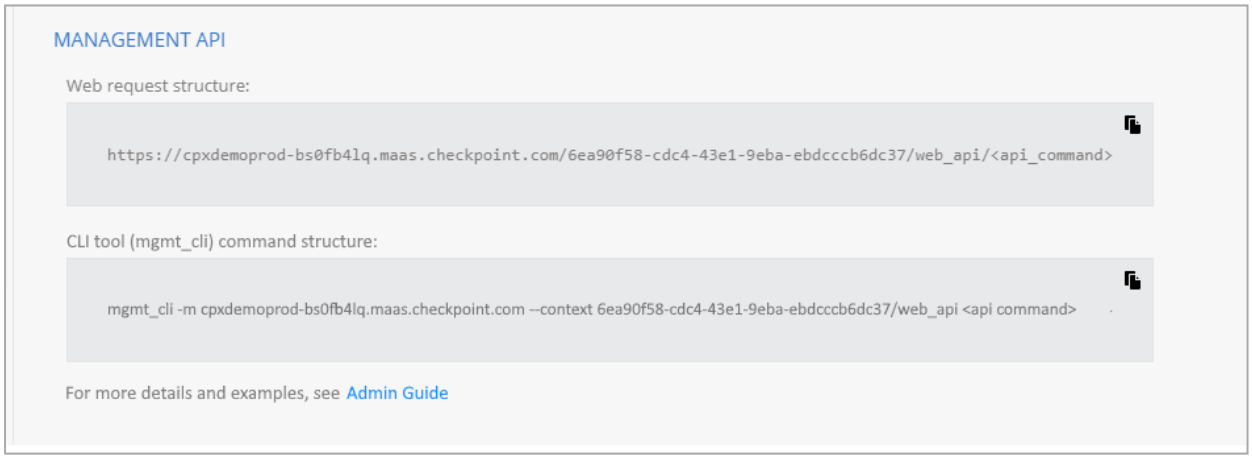
It is possible to read information and to send commands to the Check Point Management Server. In an equivalent procedure to creation of objects, Security Policy configuration, and use of the SmartConsole GUI, it is possible to do the same tasks with command line tools and web services.

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:

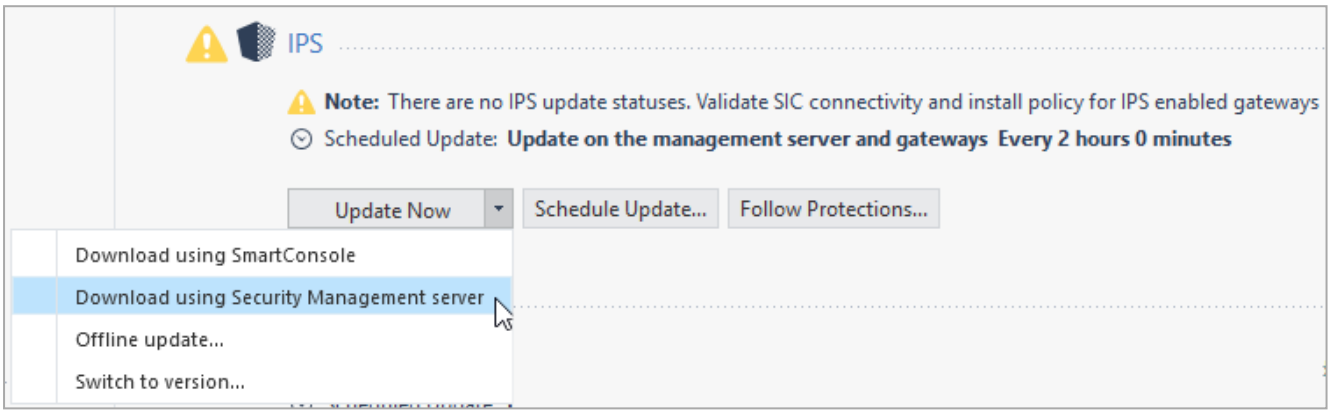
- Upload the files to a temporary folder in **my files**. Downloaded files are saved here. Use the folder icon, on the top toolbar, to download files to the local computer.

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.



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.

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

Frequently Asked Questions

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 58*.

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, *"Smart-1 Cloud License" on page 89*.

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 Retention

The Smart-1 Cloud counts log storage based on storage size rather than days. The license you purchase includes storage space and the maximum log rate. Therefore, the total number of retained days is derived from the daily log rate and the purchased storage.

For example, if you purchase 100 GB of storage and the actual daily log input is 5 GB, the number of days that data is saved is 100/5 = 20 days.

You can see the average daily log input on the Smart-1 Cloud home page.

An exclamation mark shows on the Smart-1 Cloud home page as a warning if the storage capacity exceeds the license limit.

Note - When the storage capacity is full, Smart-1 Cloud deletes the oldest log.

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 Streamed SmartConsole" on page 46*