QUANTUM

01 July 2025

# QUANTUM SPARK 1500, 1600, 1800, 1900, 2000 APPLIANCES

## R81.10.X

Locally Managed

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 R81.10.X Quantum Spark 1500, 1600, 1800, 1900, 2000 Appliances Locally Managed 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.

## Revision History

| Date | Description |
|---|---|
| 1 July 2025 | Updated:<br>- *"Configuring Authentication Servers for Remote Access" on page 384*.<br>- *"Working with the Firewall Access Policy" on page 258*.<br>- *"SSL Inspection Exceptions" on page 322*. |
| 08 June 2025 | Updated:<br>- *"Advanced Settings" on page 246*<br>- *"Configuring Advanced Site to Site Settings" on page 419*<br>- *"Configuring High Availability" on page 219*<br>- *"SD-WAN" on page 275* |
| 23 March 2025 | Added new content for R81.10.17 (see sk183153) |
| 12 February 2025 | Updated:<br>- *"Working with User Awareness" on page 431* |
| 28 January 2025 | Updated:<br>- *"SSH Authentication" on page 531* |
| 16 January 2025 | Updated:<br>- *"Configuring Internet Connectivity" on page 87* |
| 12 December 2024 | Updated:<br>- *"Configuring Authentication Servers for Remote Access" on page 384*<br>- *"Configuring the Firewall Access Policy and Blade" on page 250*<br>- *"Using System Tools" on page 507*<br>- *"Configuring Internet Connectivity" on page 87* |
| 01 October | Updated:<br>- *"Configuring Internet Connectivity" on page 87* |
| 19 September 2024 | Updated:<br>- *"IoT Protect" on page 300* |
| 11 September 2024 | Added new content for R81.10.15 (see sk182438) |

| Date | Description |
|---|---|
| 17 June 2024 | Updated:<br>- *"Configuring High Availability" on page 219* |
| 12 May 2024 | Updated:<br>- *"IoT Protect" on page 300* |
| 16 April 2024 | Added:<br>- *"Important Links" on page 22* |
| 18 March 2024 | Updated:<br>- *"Dr. Spark" on page 504* |
| 04 March 2024 | Updated:<br>- *"Using System Tools" on page 507*<br>- *"Configuring Advanced Site to Site Settings" on page 419* |
| 26 February 2024 | Added new content for R81.10.10 |
| 27 November 2023 | Updated:<br>- *"Viewing Security Logs" on page 473* |
| 31 August 2023 | Added new content for R81.10.08 |
| 18 May 2023 | Added new content for R81.10.07 |
| 09 May 2023 | Updated *"Configuring the Routing Table" on page 202* |
| 06 March 2023 | Merged the information about R81.10.00 and R81.10.05 into a single document<br>Updated:<br>- *"Configuring High Availability" on page 219*<br>- *"Configuring VPN Sites" on page 407* |
| 15 February 2023 | Updated:<br>- *"Configuring the Remote Access Blade" on page 355* |
| 24 January 2023 | First release of this document |

# Table of Contents

# Overview of Quantum Spark 1500, 1600, 1800, 1900 and 2000 Appliance Series

## 1500 Appliances

Quantum Spark 1500 appliance series includes the 1530, 1550, 1570, 1590, and 1570R appliances. These appliances support the Check Point Software Blade architecture and provide independent modular security building blocks. You can quickly enable and configure the Software Blades to meet your specific security needs. The 1535, 1555, 1575 and 1595 and 1595R appliances, which support WiFi6 and 5G, are available starting from R81.10.05.

Quantum Spark 1500 appliances deliver integrated unified threat management to protect your organization from today's emerging threats. Based on proven Check Point security technologies such as Stateful Inspection, Application Intelligence, and Security Management Architecture, the appliances provides simplified deployment while delivering uncompromising levels of security.

These appliances run an embedded version of the Gaia operating system. The appliances include core configuration elements such as Gaia Clish interface, SNMPv2/v3 and routing stack implementations. In addition to the Gaia features, Gaia Embedded operating system contains support for built-in network switches, wireless networks, 4G LTE Internet connectivity, multiple Internet connections (more than 2) in High Availability or Load Sharing mode, Policy Based Routing, and DDNS support. Quick deployment with USB is supported for all appliances, and with SD card and Dual SIM card for the 1570 / 1590 appliances.

This Administration Guide describes all aspects that apply to the Quantum Spark 1530 / 1550, 1570R, and 1570 / 1590 Appliances.

# 1600 and 1800 Appliances

The Quantum Spark 1600 / 1800 Security Appliances, part of the 1600 / 1800 Appliance family, deliver enterprise-grade security, run the R81.10 code base in an all-in-one security solution to protect Medium Business employees, network and data from cyber-theft.

The 1600 / 1800 Security Gateways offer integrated, multi-layered security in a 1U form factor, a high performance platform which is easy and simple to configure and manage. The Security Gateway offers firewall, VPN, Anti-Virus, Application Visibility and Control, URL Filtering, Email Security, and SandBlast Zero-Day Protection.

Quantum Spark 1600 / 1800 Security Appliances can be managed either locally in a Web interface, or centrally by means of a cloud-based Quantum Spark Security Management Portal (Quantum Spark Portal).

# 1900 and 2000 Appliances

The Quantum Spark 1900 and 2000 Security Appliances deliver enterprise-grade security in simple, affordable, all-in-one security solutions in a 1U Rack Unit (RU) form factor to protect mid-size business employees.

The two appliances offer the same amount of network ports (the difference is only in their Threat Prevention performance throughput). The appliances feature four 10GbE fiber ports as well as 18 x 1GbE and 2 x 2.5GbE copper ports

| Appliance | Model | Appliance Homepage |
|---|---|---|
| 2000 | V94 (wired only) | sk181924 |
| 1900 | V94 (wired only) | sk181924 |
| 1800 | V-83 (wired only) | sk168880 |
| 1600 | V-82 (wired only) | sk168880 |
| 1570R | V-81R, V-81WLR | sk166654 |
| 1595R | V91R, V91RC | sk157412 |
| 1575R | V85RWL, V85R<br>V-81R (1575R Maritime) | sk182056 |
| 1575 / 1595 | V91, V91W, V91WC, V91WLTE | sk157412 |
| 1570 / 1590 | V-81 Wired, V-81W WiFi, V-81WL WiFi-LTE, V-81WD WiFi-DSL | sk157412 |

| Appliance | Model | Appliance Homepage |
|---|---|---|
| 1535 / 1555 | V91, V91W, V91WC<br>V-80*, V90W | sk157412 |
| 1530 / 1550 | V-80 Wired, V-80W WiFi | sk157412 |

For front, side, and back panel details for each appliance, see the relevant *Getting Started Guide*:

- *Getting Started Guide for 1900 / 2000 Appliances*
- *Getting Started Guide for 1600 / 1800 Appliances*
- *Getting Started Guide for 1595R Appliances*
- *Getting Started Guide for 1570R Appliances*
- *Getting Started Guide for 1575 / 1595 Appliances*
- *Getting Started Guide for 1570 / 1590 Appliances*
- *Getting Started Guide for 1535 / 1555 Appliances*
- *Getting Started Guide for 1530 / 1550 Appliances*

# Important Links

**Important** - Review these materials before configuring your Quantum Spark appliance.

## Video

*Check Point Quantum Spark - YouTube Playlist*

## SK Articles

- *sk179615 - Quantum Spark Appliances - Releases R81.10.X*
- *sk178604 - Quantum Spark R81.10.X Known Limitations*
- *sk181134 - Quantum Spark R81.10.X Resolved Issues*
- *sk181924 - Quantum Spark Appliances 1900 and 2000 Models*
- *sk168880 - Quantum Spark Appliances 1600 and 1800 Models*
- *sk157412 - Quantum Spark Appliances 1500 Models*

## Documents (in English)

**Note** - Some topics in an Administration Guide only apply to specific appliances or models.

- *R81.10.X Quantum Spark Release Notes for 1500, 1600, 1800, 1900, 2000 Appliances*
- *R81.10.X Quantum Spark Locally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*
- *R81.10.X Quantum Spark Centrally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*
- *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances*
- *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*
- *Quantum Spark FAQ*

# Getting Started with 1500, 1600, 1800 1900 and 2000 Appliance Series

**This Administration Guide describes:**

- Installing the appliance and connecting the cables.
- Configuring Security Policies.
- Configuring local users and administrators.
- Configuring VPN.
- Configuring a cluster.
- Configuring advanced settings.
- Logging and monitoring.

**Workflow:**

1. Install the Quantum Spark appliance and connect all cables.

   See the:

   - *Getting Started Guide for 1900 / 2000 Appliances*
   - *Getting Started Guide for 1600 / 1800 Appliances*.
   - *Getting Started Guide for 1570R Appliances*.
   - *Getting Started Guide for 1570 / 1590 Appliances*.
   - *Getting Started Guide for 1530 / 1550 Appliances*.
   - *"Setting Up the Quantum Spark Appliance" on page 25*.
2. Follow the applicable First Time Deployment option.

   See *"First Time Deployment Options" on page 27*.
3. Install the required licenses.

   See *"Managing Licenses" on page 57*
4. Configure the required users and objects.

   See *"Managing Users and Objects" on page 431*.

5. Configure required appliance settings.

   See *"Managing the Device" on page 87*.

6. Configure and install the required Security Policies.

   See:

   - *"Managing the Access Policy" on page 250*.
   - *"Managing Threat Prevention" on page 324*.

7. Make sure the appliance works as required.

   See *"Logs and Monitoring" on page 473*.

8. Configure other required settings, such as:

   - VPN (see *"Configuring VPN" on page 349* and *"Managing VPN" on page 348*).
   - Clusters (see *"Configuring High Availability" on page 219*).
   - QoS (see *"Configuring QoS" on page 309*).

# Setting Up the Quantum Spark Appliance

**To set up the Quantum Spark Appliances:**

1. Remove the Quantum Spark Appliance from the shipping carton and place it on a tabletop.
2. Identity the network interface marked as **LAN1**.

   This interface is preconfigured with the IPv4 Address 192.168.1.1 and Subnet Mask 255.255.255.0.

**Connecting the Cables:**

1. Connect the power cable to the appliance. The appliance is connected directly to the power source.

   1530 / 1550 appliances only: Turn on the power switch located on the back panel.
2. When the appliance is turned on, the Power LED on the front panel lights up in red for a short period.

   The LED then turns blue and starts to blink. This shows a boot is in progress and firmware is being installed.

   When the LED turns a solid blue, the appliance is ready for login.

   **Note** - The LED is red if there is an alert or error.

   - **If you use an external modem:**

     Connect the Ethernet cable to the WAN port on the appliance back panel and plug it into your external modem or router's PC/LAN network port. The Internet LED on the appliance front panel lights up when the Ethernet is connected.
   - **If you do not use an external modem:**

     Connect the telephone cable to the DSL port on the appliance back panel and plug it into the DSL line socket. The DSL LED as well as the Internet Link LED remains off until you configure the appliance, including setting up the DSL as an internet connection.
3. Connect the standard network cable to the LAN1 port on the appliance and to the network adapter on your PC.

**Note** - Wait 10 seconds between power cycles (off and on).

# Using Default WiFi

Starting in version R81.10.07, you can use the default SSID for a WiFi connection.

**Note** -

- This option is only available when connecting the appliance for the first time and the First Time Configuration Wizard did not yet run.
- Only available for one hour.

1. Connect the appliance cable and the WAN cable.
2. Use the SSID and password printed on the appliance sticker to connect to WiFi.

   **Note** - Skip this step if you are connecting through LAN.

3. Browse to default gateway IP address: https://192.168.1.1:4434

   The **Welcome** screen of the First Time Configuration Wizard appears.

4. Click **Fetch Settings from the Cloud**.
5. In the new window, click **Yes** to confirm that you want to proceed.
6. The **Internet connection** page of the First Time Configuration Wizard
7. From the **Connection type** drop-down menu, select **Static IP**.
8. Click **Connect**.

   The One Touch status bar is running.

**Note** - If you were connected to WiFi: After the One Touch script finishes running, the WiFi network you were connected to is deleted. As a result, you are disconnected from the appliance.

# First Time Deployment Options

There are different options for first time deployment of your Small and Medium Business (SMB) gateways:

- First Time Configuration Wizard - For more information, see the *Getting Started Guide* for your appliance model.
  - *Getting Started Guide for 1900 / 2000 Appliances*
  - *Getting Started Guide for 1600 / 1800 Appliances*.
  - *Getting Started Guide for 1570R Appliances*.
  - *Getting Started Guide for 1570 / 1590 Appliances*.
  - *Getting Started Guide for 1530 / 1550 Appliances*.
- *"Zero Touch Cloud Service" on page 28*
- *"Deploying from a USB Drive or SD Card" on page 30*

**Note** - SD card deployment is supported only in 1570 / 1590 appliances.

# Zero Touch Cloud Service

The Zero Touch Cloud Service lets you easily manage the initial deployment of your gateways in the *Check Point Zero Touch Portal*.

**Note** - You cannot use Zero Touch if you connect to the Internet through a proxy server.

Zero Touch enables a gateway to automatically fetch settings from the cloud when it is connected to the internet for the first time.

**Note** - The appliance is fully configured after you complete the First Time Configuration Wizard (click **Finish** on the final screen or click **Quit** on an earlier screen after you enter a username and password). To use the Zero Touch Cloud Service after this point, you must first restore the factory defaults.

If the gateway connects to the internet using DHCP, the gateway fetches the Zero Touch settings without any additional action. If no DHCP service is available, you must run the First Time Configuration Wizard, configure the Internet Connection settings, and then fetch the settings from the Zero Touch server.

**Note** - You can run the Zero Touch configuration on DMZ over the SFP port. Connect the cable to the DMZ/SFP port as for WAN.

**To connect to the Zero Touch server from the First Time Configuration Wizard:**

1. In the **Welcome** page of the First Time Configuration Wizard, click **Fetch Settings from the Cloud**.
2. In the window that opens, click **Yes** to confirm that you want to proceed.
3. The **Internet connection** page of the First Time Configuration Wizard opens. Configure your Internet connection and click **Connect**.
4. The settings are automatically downloaded and installed.
5. A new window opens and shows the installation status. It may take several minutes until the installation is complete.

**Note** - If a collision is detected between an internal network (LAN) and an IP returned via DHCP (WAN), the conflicting LAN address is changed automatically. If a colliding LAN IP address is changed, a message appears in the system logs.

When you reconnect to the WebUI or click **Refresh**, the browser opens to show the status of the installation process.

After the gateway downloads and successfully applies the settings, it does not connect to the Zero Touch server again.

For more information on how to use Zero Touch, see sk116375 and the *Zero Touch Administration Guide*.

# Deploying from a USB Drive or SD Card

You can deploy the Quantum Spark Appliance configuration files from a USB drive or SD card (1570 / 1590, 1600 / 1800 appliances only) and quickly configure many appliances without using the First Time Configuration Wizard. The configuration file lets you configure more settings and parameters than are available in the First Time Configuration Wizard.

**Note** - SD card deployment is not supported for 1530 / 1550 appliances.

You can deploy configuration files in these conditions:

- An appliance with default settings is not configured at all.
- An appliance that already has an existing configuration.

The Quantum Spark Appliance starts, automatically mounts the USB drive, and searches the root directory for a configuration file.

**Note** - The USB drive must be formatted in FAT32. SD cards are formatted with ext4.

## Sample Configuration File

This is a sample Quantum Spark 1530 / 1550 Appliance configuration file for USB deployment.

```
set time-zone GMT+01:00(Amsterdam/Berlin/Bern/Rome/Stockholm/Vienna)
set ntp server primary 10.1.1.10
set ntp server secondary
set user admin type admin password aaaa
set interface WAN ipv4-address 10.1.1.134 subnet-mask 255.255.255.192 default-gw 10.1.1.129
delete interface LAN1_Switch
set dhcp server interface LAN1 disable
set interface LAN1 ipv4-address 10.4.6.3 subnet-mask 255.255.255.0
add interface LAN1 vlan 2
set dhcp server interface LAN1:2 disable
set interface LAN1:2 ipv4-address 10.4.3.3 subnet-mask 255.255.255.0
set dhcp server interface LAN2 disable
set interface LAN2 ipv4-address 192.168.254.254 subnet-mask 255.255.255.248
set interface LAN2 state on
set admin-access interfaces WAN access allow
set hostname DEMOgw01
```

## Preparing the Configuration Files

The Quantum Spark Appliance Massive Deployment configuration files are composed of Gaia Clish commands.

These are the file names that you can use:

- `autoconf.clish`
- `autoconf.<MAC Address>.clish`

*<MAC Address>* is the specified MAC address in this format: *XX-XX-XX-XX-XX*

You can create multiple configuration files for Quantum SparkAppliance gateways. The gateways run both files or only one of them. First the `autoconf.clish` configuration file is loaded. If there is a configuration file with the same MAC address as the gateway, that file is loaded second.

Use the **#** symbol to add comments to the configuration file.

# Deploying the Configuration File - Initial Configuration

This section describes how to deploy a configuration file on a USB drive to Quantum Spark Appliance. You must configure and format the file correctly before you deploy it. You can insert the USB drive in the front or rear USB port. Make sure the USB drive is formatted in FAT32.

You can deploy the configuration file to the Quantum Spark Appliance when the appliance is off or when it is powered on.

**Important** - Do not remove the USB drive or insert a second USB drive while the configuration script runs. This may cause a configuration error.

To deploy the configuration file from a USB drive for the initial configuration:

1. Insert the USB drive into a Quantum SparkAppliance.
   - Quantum SparkAppliance is OFF - Turn on the appliance. The Power LED is red when the appliance is first turned on.It blinks blue while the boot is in progress and then turns solid blue when the process is complete..
   - Quantum Spark Appliance is ON - The appliance automatically detects the USB drive.
2. The Quantum SparkAppliance locates the USB configuration file and begins to run the script. The USB LED blinks blue while the script runs.
3. The configuration script finishes and the Quantum Spark Appliance Power LED is a constant blue.
4. Remove the USB drive from the Quantum SparkAppliance.

**Note** - The USB LED is red when there is a problem running the configuration script. Turn off the Quantum Spark Appliance and confirm that the configuration files are formatted correctly.

# Deploying the Configuration File - Existing Configuration

To edit or upgrade the existing configuration of a Quantum Spark Appliance, deploy a configuration file. Use the `set property` command to set the appliance to use a configuration file on a USB drive. The USB drive can be inserted in the front or the rear USB port.

You can deploy the configuration file to the Quantum Spark Appliance either when the appliance is off or when it is powered on.

**Important** - Do not remove the USB drive or insert a second USB drive while the Quantum Spark Appliance configuration script runs. This may cause a configuration error.

To deploy the configuration file from a USB drive to a configured appliance:

1. From the CLI, enter the command:

   ```
   set property USB_auto_configuration once
   ```

   The appliance is set to use a configuration script from a USB drive.

2. Insert the USB drive in the appliance (the appliance automatically detects the USB drive).

   The USB LED comes on and is a constant orange.

3. The appliance locates the USB configuration file and begins to run the script. The USB LED blinks blue while the script runs.

4. The configuration script finishes.

   The USB LED is a constant blue and the screen displays: `System Started`.

5. Remove the USB drive from the appliance.

**Note** - The USB LED is red when there is a problem running the configuration script. Turn off the appliance and confirm that the configuration files are formatted correctly.

# Viewing Configuration Logs

After the Quantum Spark Appliance is successfully configured from a USB drive, a log is created.

- The log file is called: `autonconf.<MAC Address>.<timestamp>.<log>`
- The log file is created in the USB root directory and in `/tmp` on the appliance.

# Troubleshooting Configuration Files

This section discusses the scenario where the configuration file fails and the Quantum SparkAppliance is not fully configured.

## Configuration File Error

If there is an error and the configuration file fails, the appliance is not fully configured and is no longer in the initial default condition. The commands in the configuration file that show before the error are applied to the appliance. You can examine the configuration log to find where the error occurred.

When the appliance is not fully configured, the First Time Configuration Wizard shows in the WebUI. However, not all of the settings from the failed configuration file show in the First Time Configuration Wizard.

**Best Practice** - Check Point recommends that you do not use the First Time Configuration Wizard to configure an appliance when the configuration file fails. Restore the default settings to a partially configured appliance before you use the First Time Configuration Wizard to ensure that the appliance is configured correctly.

## Suggested Workflow - Configuration File Error

This section contains a suggested workflow that explains what to do if there is an error with the configuration file on a USB drive. Use the `set property USB_auto_configuration` command when you run a configuration file script on a configured appliance.

1. The USB drive with the configuration file is inserted into a USB port on the Quantum Spark Appliance.
2. The USB LED on the front panel blinks red. There is a problem with the configuration file script.

   **Sample console output displaying an error:**

   ```
   Booting Check Point RD-6281-A User Space...
   INIT: Entering runlevel: 3
   ........sd 2:0:0:0: [sda] Assuming drive cache: write through
   sd 2:0:0:0: [sda] Assuming drive cache: write through
   .....................................................
   System Started...
   Start running autoconfiguration CLI script from USB2 ...
   Error.
   autoconf.00-1C-7F-21-07-94.2011-07-21.1248.log was copied to
   USB2
   ```

3. The log file is created and contains the configuration details.
   - The log file is called: `autonconf.<MAC Address>.<timestamp>.<log>`
   - The log file is created in the USB root directory and in `/tmp` on the appliance.
4. Analyze the log file to find the problem.

**If you cannot repair the configuration file:**

1. Remove the USB drive.
2. Run the CLI command:

   ```
   restore default-settings
   ```

3. Connect to the WebUI and use the First Time Configuration Wizard to configure the appliance.

**If you understand the error and know how to repair the configuration file:**

1. Remove the USB drive.
2. Run the CLI command:

   ```
   restore default-settings
   ```

3. Insert the USB drive and run the repaired configuration script again.

## Sample Configuration Log with Error

This is a sample configuration log file for a configuration script that fails.

```
set hostname Demo1
set hostname: Setting hostname to 'Demo1'
OK
set interface WAN internet primary ipv4-address 66.66.66.11
Error: missing argument 'subnet-mask' for a new connection
Autoconfiguration CLI script failed, clish return code = 1
```

# Using the set property Command

The `set property` CLI command controls how the Quantum Spark Appliance runs configuration scripts from a USB drive.

These commands do not change how the First Time Configuration Wizard in the WebUI configures the appliance:

- `set property USB_auto_configuration off`

  The appliance does not run configuration scripts from a USB drive.

- `set property USB_auto_configuration once`

  The appliance only runs the next configuration script from a USB drive.

- `set property USB_auto_configuration always`

  The appliance always runs configuration scripts from a USB drive.

# Configuration and Upgrade Scenarios

This chapter contains workflows for common configuration and upgrade scenarios.

## Configuring Cloud Services

### Introduction

Cloud Services lets you connect your Quantum Spark Appliance to a Cloud Services Provider that uses a Web-based application to manage, configure, and monitor the appliance.

### Prerequisites

Before you connect to Cloud Services, make sure you have:

- Received an email from your Cloud Services Provider that contains an activation link. When you click the link , your Check Point Appliance automatically connects to Cloud Services.

  Or

- The Service Center IP address, the Quantum Spark Appliance gateway ID, and the registration key. Use these details to connect manually your Quantum Spark Appliance to Cloud Services.

**To automatically connect to Cloud Services:**

1. Make sure the Quantum Spark Appliance was configured with the First Time Configuration Wizard. See the relevant Getting Started Guide.
2. In the email that the Security Gateway owner gets from the Cloud Services Provider, click the **activation link**.

   After you log in, a window opens and shows the activation details sent in the email.
3. Make sure the details are correct and click Connect.

   For more details, see *"Configuring Cloud Services" on page 51*.

**To connect manually to Cloud Services:**

1. In the WebUI, go to the **Home** > **Cloud Services** page.
2. Follow the Connect to Cloud Services procedure in *"Configuring Cloud Services" on page 51*.

# Configuring a Guest Network

In some situations, you need to allow guest access to the Internet from within your organization. At the same time, you may want to restrict access to internal network resources. When you configure a guest network with a Hotspot, you can control network access. If you set user authentication options, you can then monitor the users that connect to the network.

### Prerequisites

- You must have a wireless network enabled on your appliance. The guest network is actually a Virtual Access Point (VAP).
- You must define the network interfaces that redirect users to the Hotspot portal when they browse from those interfaces.

### Configuration

1. Go to **Device** > **Wireless Network**.
2. Click **Guest** and follow the wizard instructions. See *"Configuring the Wireless Network" on page 116*.
    - Set the network protection (unprotected or protected network).
    - Set the access and log policy options in the **Access Policy** tab.
3. Make sure that the **Use Hotspot** checkbox is selected in the wizard.
4. Make sure you defined the network interfaces for Hotspot. See *"Configuring the Local Network" on page 125*.
5. Configure the Hotspot - Go to **Device** > **Hotspot** and set the options. See *"Configuring a Hotspot" on page 145*.
6. If necessary, you can limit access to the Hotspot for specified user groups in the Access section.

### Monitoring

Connect to the network and open a browser session. You see the customized Hotspot portal.

**Note** - You see the Hotspot portal one time in the given timeout period. The default timeout period is 4 hours.

User activity on this network is logged with user names if the Log traffic option was selected.

# Introduction to the WebUI

This chapter provides instructions for how to configure special features of the Quantum SparkAppliance with its web application interface (WebUI).

See the Quantum Spark*Appliance Getting Started Guide* for your appliance model. After you run the First Time Configuration Wizard , you connect to the appliance with a browser (with the appliance's IP or, if the appliance is used as a DNS proxy or DHCP server, to `http://my.firewall`). It redirects to a secure HTTPS site and asks for administrator credentials. When you log in, you can select the **Save user name** checkbox to save the administrator's user name. The name is saved until you clear the browser's cookies.

When you log in successfully, the WebUI opens to **Home** > **System**. From the left pane you can navigate between the different pages of each tab:

- **Home**
- **Device**
- **Access Policy**
- **Threat Prevention**
- **VPN**
- **Users & Objects**
- **Logs & Monitoring**

At the top of every WebUI page, the toolbar displays these buttons:

| Icon | Description |
|---|---|
| Search | Enter text in the search field. |

| Icon | Description |
|---|---|
| >_ | Starting in R81.10.15: Click to open a **Command Line Interface** window. After you log in with your user name and password, you can run any command in Gaia Clish or Expert mode without the need to leave the appliance WebUI or connect via SSH.<br>**Use case** - Technical users or developers can use this command line interface to debug directly from the WebUI during remote sessions.<br>ⓘ **Notes**:<br>■ This tool is only available for Super Administrators.<br>■ After you open the Command Line Interface, there is a 60 second idle period before you are logged out of the command line. Click **Connect** to log in again.<br>■ To minimize the Command Line Interface, click the "-" in the top right corner. The session remains active. To restore the minimized interface, click the icon again.<br>■ To terminate the Command Line session, click the "X" in the top-right corner of the command line interface screen. |
| 🛟 | Click to contact Support. |
| ⇦ | Click to log out of the WebUI session. |
| ? | Click to open the online Help (located below the toolbar). |

**To log in to the WebUI in a language other than English:**

On the browser page that shows the Login window, select the language link at the bottom of the page.

- Japanese
- Simplified Chinese
- Traditional Chinese

The log in page changes immediately to the selected language. The next login from the same computer is in the selected language (saved in a browser cookie). The language preference is kept until you clear the browser's cookies.

ⓘ **Note** - If the user's locale matches a localized WebUI, the Login window automatically loads in the specified language. Only English is supported as the input language.

# The Home Tab

This chapter describes the **Home** tab of the WebUI application.

# Viewing System Information

The **Home** view > **Overview** section > **System** page shows an overview of the Quantum Spark Appliance.

Starting in R81.10.15, when you access the **System** page, a popup shows what is new in the latest upgrade.

The Quantum Spark Appliance requires only minimal user input of basic configuration elements, such as IP addresses, routing information, and blade configuration. The initial configuration of the Quantum Spark Appliance can be done through a First Time Configuration Wizard. After the initial configuration is completed, every entry that uses `http://my.firewall` shows the WebUI **Home** > **System** page.

The **System** page shows these sections:

| # | Section | Description |
|---|---|---|
| 1 | Top section | This section shows these fields:<br>▪ **Model**<br>The Quantum Spark appliance model.<br>Example: *1900/2000 Appliance*<br>▪ **Version**<br>The firmware version and build.<br>Example: *R81.10.10 (996002845)*<br>▪ **MAC address**<br>The MAC address of the WAN port.<br>Example: *00:1C:7F:B6:91:53*<br>▪ **Management**<br>The management type - Centrally Managed or Locally Managed.<br>Example: *Local*<br>▪ **License**<br>The installed license.<br>Example: *Trial license*<br>▪ **Capabilities**<br>Additional important hardware features.<br>Example: *SSD*<br>In addition, this section shows the link **WatchTower mobile app** to connect the Check Point WatchTower to this Quantum Spark appliance. |

| # | Section | Description |
|---|---|---|
| 2 | **Internet connections** | This section shows:<br>■ The names of the configured Internet connections<br>■ The link "**Internet connections**" that opens the **Device** view > **Network** section > **Internet** page.<br>■ The status of the wireless connection. |

| # | Section | Description |
|---|---|---|
| 3 | Interactive front panel view | **Notes**:<br>- This section appears in R81.10.15 and higher versions.<br>- This section is displayed on Locally Managed appliances only.<br>This section shows an image of the front panel and the status of each physical port - network ports, USB ports, console ports.<br>The status of all ports is refreshed every 2 seconds.<br>If a cable (or USB device) is connected to a port to a configured port, or disconnected from a configured port, then it shows a corresponding icon (see the **Status** sub-section at the bottom).<br>Hover the mouse cursor over the physical **network** port with a connected cable to see the applicable information:<br>- **Status**<br>- **Operation**<br>- **IPv4 address**<br>- **Cluster IPv4 address**<br>- **Cluster mode**<br>- **Assignment**<br>- **Throughput**<br>In a cluster configuration, you can click the link **More information** to see a popup with a summary information for each cluster member (some of these are links to the corresponding page in WebUI):<br>- **Appliance name**<br>- **Version**<br>- **MAC address**<br>- **Uptime**<br>- **Sync method**<br>- **Role / Status**<br>- **High Availability mode**<br>- **Blade license status**<br>- **Enabled blades**<br>- **Throughput**<br>- **Connections**<br>- **Assets**<br>This section shows these sub-sections at the bottom:<br>- **Status** - Shows the legend for port icons.<br>- **Operation** - Show the Quantum Spark Gateway operation mode. |

| # | Section | Description |
|---|---|---|
| | | - **Relation (click to view)** |
| 4 | **Assets** | This section shows the infected devices on the internal networks.<br>This section shows the links to these pages:<br>- **Manage assets** - **Home** view > **Monitoring** section > **Assets** page.<br>- **IoT** - **Access Policy** view > **Firewall** section > **IoT** page. This link appears in R81.10.10 and higher versions. |
| 5 | **Monitoring** | This section shows live data graphs for throughput and packet rate.<br>This section shows the links to these pages:<br>- **Internet** - **Device** view > **Network** section > **Internet** page.<br>- **SD-WAN** - **Access Policy** view > **Firewall** section > **SD-WAN** page. This link appears in R81.10.05 and higher versions. |
| 6 | **Notifications** | This section shows system and security events, and their severity.<br>The link **All notifications** opens the **Home** view > **Monitoring** section > **Notifications** page. |

To monitor your device's internet connection from your mobile device, you must first configure this on the WebUI **Home** > **System** page.

**To configure connection monitoring:**

1. In the WebUI, go to **Home** > **System** > **Internet connections** and click **Edit**.

   The **Edit Internet Connection** window opens.

2. In the **Connection Monitoring** tab, check or clear:

   - **Automatically detect loss of connectivity to the default gateway**. This pings the default gateway to detect if connectivity is lost.

   - **Monitor connection state by sending probe packets to one or more servers on the Internet**. This uses other methods and servers to detect connectivity loss.

     **Important** - In versions R81.10.10 and higher, it is supported to disable probing in an Internet connection only if you clear the option, "This Internet connection will be a part of SD-WAN" (on the "Advanced" tab > section "SD-WAN Settings").

3. If you selected **Monitor connection state**, select the **connection probing** method:

   - Probe DNS servers
   - Ping addresses

4. If you selected **Ping addresses**, enter the IP address(es).
5. Select the settings for:
   - **Recovery time** (seconds)
   - **Max latency allowed** (milliseconds)
   - **Probing frequency for active connections** (seconds)
6. Click **Apply**

When you log in to your appliance for the first time after completing the First Time Configuration Wizard, the **Sending Data to Check Point** pop up window appears, with these checkboxes:

- **Help us improve product experience by sending data to Check Point** - The data sent includes session durations, how long the system is running, logs, etc.

  **Note** - Check Point does not upload data that contains private or sensitive information.

- **Help us improve product stability by getting critical updates from Check Point** - Pushes critical updates outside of the regular update notification and upload schedule.

  Available starting from R81.10.08.

Selecting these checkboxes is optional, but highly recommended.

# Controlling and Monitoring Software Blades

The **Home** > **Security Dashboard** page shows you the active blades and lets you quickly navigate to the blade configuration page.

It also gives you:

- Access to the basic settings of the blades with the **Settings** button (cogwheel icon) and lets you activate the blades.
- Access to statistics for each blade (graph icon)
- Alerts you if there are blades that are missing licenses, service blades which are not up-to-date, and active blades which require additional configuration (for example, site-to-site VPN where the user did not configure any sites). When applicable, there is a triangle in the upper right hand corner of the specified blade.

The software blades are shown in these groups on this page based on where they are configured in the WebUI:

- **Access Policy** - Contains the Firewall, Application & URL Filtering, User Awareness, and QoS blades.
- **Threat Prevention** - Contains the Intrusion Prevention (IPS), **Anti-Virus**, **Anti-Bot**, **Threat Emulation**, and **Anti-Spam** blades.
- **VPN** - Contains the Remote Access and Site to Site VPN blades. It also contains certificate options.

You can click the tab name link or Software Blade link to access the tab for further configuration.

**To enable or disable a Software Blade:**

1. Slide the lever of the specified blade to the necessary **ON** or **OFF** position.
2. When you turn off the Firewall blade, click **Yes** in the confirmation message.

**Note** - Software Blades that are managed by Cloud Services show a lock icon. You cannot toggle between on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

**To see or edit setting information:**

1. Click the cogwheel icon next to the **On**/**Off** lever.

   The blade settings window opens.

2. View the details or select options to change current settings.
3. Click **Apply**

**To view statistics:**

1. Click the bar graph icon.

   The blade statistics window opens.

2. If the blade is turned on:
   - View the graph and details.
   - To go to other blade statistics, click the arrows in the header.
3. If the blade is turned off:
   - Click **View demo** to see an example of the statistics shown
   - Click the **X** icon to close the demo.

**To view an alert:**

1. Hover over the alert triangle.
2. Click the applicable link.

# Setting the Management Mode

The **Home** > **Security Management** page shows information for the management mode of the appliance. You can also test Internet Connectivity from this page.

**To set the management type:**

Select one of the options:

- **Locally** - To manage the appliance using the local web application (WebUI). Click **Apply** and then **Yes** when asked to confirm.
- **Centrally** - To manage the appliance using the Security Management Server.

When centrally managed, it shows the trust status between the appliance and the Security Management Server. When a policy is prepared in SmartConsole you can fetch the policy from this window.

### Security Management Server

In this section you can view the status of the management connection, last policy installation, adjust trust settings, and initialize a connection.

1. In the Security Management Server section, click **Settings** to adjust trust settings or **Setup** to initialize a connection.

   The **Welcome to the Security Management Server Configuration Wizard** opens.

   Click **Next**.

2. In the **One Time Password (SIC)** page, select an option for authenticating trusted communication:

   - **Initiate trusted communication securely by using a one-time password** - The one-time password is used to authenticate communication between the appliance and the Security Management Server in a secure manner.

     Enter a one-time password and confirm it. This password is only used to establish the initial trust. When established, trust is based on security certificates.

     ⓘ **Important** - This password must be identical to the Secure Communication authentication one-time password configured for the appliance object in the SmartConsole of the Security Management Server.

   - **Initiate trusted communication without authentication (not secure)** - Select this option only if you are sure that there is no risk of imposture (for example, when in a lab setting).

   Click **Next**.

3. In the **Security Management Server Connection** page, select a connection method:

- To connect to the Security Management Server now, select **Connect to the Security Management Server now**, enter the Security Management Server IP or name and click **Connect**. When you successfully connect to the Security Management Server, the security policy is automatically fetched and installed.

  If the Security Management Server is deployed behind a 3rd party NAT device, select **Always use this IP address** and manually enter the IP address the appliance used to reach the Security Management Server. This IP address overrides, from this point on, the automatic calculating mechanism that determines the routeable IP address of the Security Management Server for each appliance.

  If trust was established but the gateway could not fetch the policy, you can investigate the issue with the Security Management Server administrator. When the issue is resolved, click the **Fetch Policy** button that shows instead of the **Connect** button.

- To connect to the Security Management Server later, select **Connect to the Security Management Server later**.

4. Click **Finish**.

**To reinitialize trusted communication with the Security Management Server:**

1. In the Security Management Server section, click **Advanced** to reinitialize trusted communication.
2. Click **Reinitialize Trusted Communication**.

   A warning message appears.
3. Click **Yes**.

   **Note** - You need to coordinate this operation with the Security Management Server administrator, as reinitialization is necessary on both sides.

### Security Policy

To obtain the security policy from the Security Management Server, click **Fetch Policy**. This option is available only if trust is established with the Security Management Server.

### Internet

To test connectivity, click **Test Connection Status**. A status message shows the results of the test. You can click **Settings** to configure Internet connections.

# Configuring Cloud Services

On the **Home** view > **Overview** section > **Cloud Services** page, you can connect the appliance to a Cloud Service.

The Cloud Services Provider uses a Web-based application to manage, configure, and monitor your appliance.

### Initial steps to connect the appliance to Cloud Services

1. Click the activation link in the email that the Security Gateway owner gets from the Cloud Services Provider.
2. Log in.

   A window opens and shows the activation details sent in the email.
3. Make sure the activation details are correct and click **Connect**.

If the appliance is connected to a different Cloud Services Provider, you are asked if you want to continue.

Alternatively, follow the connection procedure below.

When you successfully connect, a security policy and other settings are pushed to the appliance. The settings defined by Cloud Services contain your activated blades, security policy, and service settings.

After Cloud Services are turned on, these identification details are shown in the WebUI:

- At the bottom of the login page - The name defined by the Cloud Services Provider for your Security Gateway and the MAC address of the Quantum Spark Appliance.
- At the top of the WebUI application (near the search box) - The name of your Quantum Spark Appliance.

### The page shows these sections

#### Section "Cloud Services"

In this section, you connect the Quantum Spark Appliance to the Quantum Spark Management cloud service.

- In versions R81.10.15 and higher:
  - **Manage with Spark Management**

    Use this option to manage this Quantum Spark Appliance as one of multiple gateways in the Quantum Spark Management cloud service with full cloud capabilities.

    See the *Quantum Spark Management Administration Guide*.
  - **Use Cloud Capabilities**

    Use this option to onboard this Quantum Spark Appliance to Infinity Portal.

    You manage this Quantum Spark Appliance locally, but it store logs and reports in the cloud (in the Quantum Spark Management service).
- In versions R81.10.00 - R81.10.10:

  Use the **Configure** option to manage this Quantum Spark Appliance as one of multiple gateways in the Quantum Spark Management cloud service with full cloud capabilities.

When an Quantum Spark Appliance is connected to a Cloud Service, you can:

- Click **Details** to see the connection details.
- Click **Fetch now** to get updated activated blades, security policy, and service settings.
- Click **Refresh** to reconnect to the Cloud Service.

### Section "Managed Security Blades"

This section shows icons for defined security blades.

You can click the icon text to open the corresponding page in the WebUI.

- **Dark blue icon**

  Appears for a blade that is remotely managed by Cloud Services. The blade is turned on in the plan.

  Remotely managed blade pages show a lock icon.

  You cannot toggle between the on and off states.

  If you change other policy settings, the change is temporary.

  Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.
- **Gray icon**

  Appears for a blade that is remotely managed by Cloud Services.

The blade is turned off in the plan.

Note - If no blades are remotely managed, all of the blade icons are gray.

- **No icon**

  Appears for a security blade that is locally managed in the Quantum Spark Appliance.

  The blade is not managed by Cloud Services.

#### Section "Available Services"

This section shows the services that are managed by the Cloud Services Provider.

If a service has a **Settings** button, you can click it to see the settings.

You cannot change these settings.

Services that appears with a gray font are not provided by the Cloud Services Provider.

These are the available services:

- **Reports** - Periodic network and security reports sent by email. Click **Settings** to see the time frames set for your gateway.
- **Logs** - Logs are stored with the Cloud Services Provider.
- **Dynamic DNS** - A persistent domain name is set by Cloud Services.
- **Firmware Upgrades** - Firmware upgrades are managed remotely by Cloud Services.
- **Periodic Backup** - Backups are scheduled by Cloud Services.

### Workflow to connect to Cloud Services

1. Connect to Cloud Services Provider.
2. Get the security policy and settings.
3. Install the security policy and settings.

When you connect for the first time, the appliance must verify the certificate of the Cloud Services Provider against its trusted Certificate Authority list. If verification fails, you get a notification message. You can stop or ignore the verification message and continue.

## Connecting to Cloud Services

### In versions R81.10.15 and higher - onboarding to Infinity Portal

Use this procedure to onboard this Quantum Spark Appliance to Infinity Portal.

You manage this Quantum Spark Appliance locally, but it store logs and reports in the cloud (in the Quantum Spark Management service).

1. Click **Use Cloud Capabilities**.

   The **Configure Cloud Services** window opens.

   Follow the instructions in this window.
2. In a web browser, go to *Check Point Infinity Portal*.
   - If you do not have an account / tenant yet, then sign up and create a new tenant.

     See the *Infinity Portal Administration Guide*.
   - If you already have a tenant, then select the required tenant at the top.
3. In WebUI, click the link to retrieve a token from Infinity Portal.
4. In the window that opens, select the required tenant and click **Continue**.
5. Infinity Portal shows the required token.

   Copy this token.
6. In WebUI, paste the token.
7. Click **Save**.

   The appliance tries to connect to the Cloud Services Provider.

   The **Cloud Services** section shows a progress indicator and shows the connection steps.

   When the appliance connects to Infinity Portal, the required Gateway object is created in the Quantum Spark Management services, and the applicable Plan is assigned to that Gateway object.

### In versions R81.10.15 and higher - connecting to the Quantum Spark Management cloud service

Use this procedure to manage this Quantum Spark Appliance as one of multiple gateways in the Quantum Spark Management cloud service with full cloud capabilities.

For more information, see the *Quantum Spark Management Administration Guide*.

1. Click **Manage with Spark Management** or **Edit**.

   The **Configure Cloud Services** window opens.

2. Select **Activation key** or **Activation details** and enter the specified information.
3. Click **Apply**

   The appliance tries to connect to the Cloud Services Provider.

   The Cloud Services section shows a progress indicator and shows the connection steps.

**Note** - If you see a message that the identity of your Cloud Services Provider cannot be verified but you are sure of its identification, click **Resolve** and then **Ignore and reconnect**.

#### In versions R81.10.00 - R81.10.10 - connecting to the Quantum Spark Management cloud service

Prerequisite to connect to Quantum Spark Management:

Get an email from your Cloud Services Provider that contains these details:

- An activation key for your appliance,

  or

- The Service Center IP address, the Gateway ID, and the registration key.

Procedure:

1. Click **Configure** or **Edit**.

   The **Configure Cloud Services** window opens.

2. Select **Activation key** or **Activation details** and enter the specified information.
3. Click **Apply**

   The appliance tries to connect to the Cloud Services Provider.

   The Cloud Services section shows a progress indicator and shows the connection steps.

**Note** - If you see a message that the identity of your Cloud Services Provider cannot be verified but you are sure of its identification, click **Resolve** and then **Ignore and reconnect**.

When connectivity is established, the **Cloud Services** section shows these details:

- The date of the synchronization
- The **On**/**Off** toggle shows that Cloud Services is turned on.

A **Cloud Services Server** widget appears on the status bar and shows **Connected**. If you click this widget, the Cloud Services page opens.

### Test connectivity to the Cloud Services

1. Connect to the command line on the appliance.
2. Log in.
3. If your default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```

4. Run this command:

   ```
   runCliCommand.lua testcloudconnectivity [<IP Address or FQDN>]
   ```

### Getting an updated security policy, activated blades, and service settings

Click **Fetch now** in the **Cloud Services** section.

The appliance gets the latest policy, activated blades, and service settings from Cloud Services.

# Managing Licenses

The **Home** > **License** page shows the license state for the Software Blades. From this page, the appliance can connect to the Check Point User Center with its credentials to pull the license information and activate the appliance.

In most cases, you must first register the appliance in your Check Point User Center account or create one if you don't already have one. A User Center account is necessary to receive support and updates.

If you have Internet connectivity configured:

1. Go to **Home** > **License**.
2. Click **Activate License**.

   You are notified that you successfully activated the appliance license.

If you were not able to activate the license, it may be because:

- There is a connectivity issue such as a proxy between your appliance and the Internet.

  Or

- Your appliance is not registered.

If there is a proxy between your appliance and the Internet, you must configure the proxy details before you can activate your license.

**To configure the proxy details:**

1. Click **Set proxy**.
2. Select **Use proxy server** and enter the proxy server **Address** and **Port**.
3. Click **Apply**
4. Click **Activate License**.

### If your appliance is not registered:

1. Browse to: https://smbregistration.checkpoint.com
2. Enter the **MAC address** and **Registration key**. These values can be found on the **Home** > **License** page.
3. Select **Hardware Platform**.
4. Select **Hardware Model**.
5. Click **Activate License**.

   You are notified that you successfully activated the appliance license.

After initial activation, the **Activate License** button shows as **Reactivate**. If you make changes to your license, click **Reactivate** to get the updated license information.

### If you are offline while configuring the appliance:

1. Browse to *Check Point User Center*.
2. Enter the appliance's credentials, MAC address, and registration key from the **Home** > **License** page.
3. After you complete the registration wizard, you are prompted to download the activation file. Download it to a local location. This is needed for the next step.
4. In **Home** > **License**, click **Offline**.

   The Import Activation File window opens.
5. **Browse** to the activation file you downloaded and click **Import**.

   The activation process starts.

The region is set when the license is installed. The region determines the wireless frequency and parameters, as the regulations vary according to region.

If you are using a trial license, only **basic radio settings**, are allowed in all zones. A warning that selected wireless radio settings are not applied shows on the **Summary** page of the First Time Configuration Wizard and also on the **Device** > **License** page. For more information on basic wireless radio settings, see sk159693.

If you select a country and install a valid license, but the wireless region of the device does not match the selected country, a warning message shows and you must edit the country information. When the country and wireless region match, you see the full settings.

# Viewing the Site Map

The **Home** > **Site Map** page shows a site map of the WebUI. It shows all of the tabs and the pages they contain.

Click the link to any page directly from the Site Map page.

# Notifications

In the **Home** tab > **Monitoring** section > **Notifications** page, recent system and security events are displayed in a table.

For each you can see:

- **Time** - The time when the event occurred.
- **Severity** - **Security Alert**, **Attention Required**, or **Informative Event**
- **Type** - What occurred. Examples of an Informative Event include "An administrator is logged in" or "Firmware upgrade is complete"
- **Message** - A description of the event. For the example, "Firmware upgrade is complete", the message includes the version and build of the upgrade.

### To filter the table:

Select the relevant tab:

- **All**
- **IoT & Assets**
- **Internet & SD-WAN**
- **Remote Access VPN**
- **Access**
- **Security Incidents**

### To view the details of a security event:

Click the event row in the table and click **View Details**.

**To configure the notification settings:**

1. Click **Settings**.
2. In the **Notification Settings** window, for **Notification language**, use the down arrow in the field to select the desired language.
3. To set the maximum number of notifications to receive within a specific time period (in minutes), select the checkbox **Limit notifications by time range** and use the arrows to enter the desired values. The defaults are a maximum of 3 notifications every 60 minutes.
4. To receive aggregated notifications instead of multiple single notifications, select the checkbox **Send aggregated notifications**.
5. To receive push notifications of a specific severity on your mobile device, select the checkbox **Send mobile push notifications of severity [blank] and higher**. Use the down arrow in the severity field to select **Security Alert**, **Attention Required**, or **Informative Event**.
6. For previews of WatchTower push notifications, select the checkbox **Show previews for WatchTower push notifications**.
7. Starting from R81.10.08, you can select how to receive the notifications. Select one or both of these options and use the down arrow in the field to select the severity:
   - **Send email notifications of severity [blank] and higher**
   - **Send SMS notifications of severity [blank] and higher**

   **Notes:**
   - To receive these notifications, an admin must define an email address **or** a mobile phone number.
   - If an admin did not define either a phone number **or** an email address, a warning appears when the admin logs in.
8. In the list of Notifications, select the checkbox and severity for the ones you want to receive.
9. Click **Save**.

# Assets

Starting from R81.10.10, the **Home** >**Monitoring** > **Assets** page replaces the **Active Devices** and **Wireless Active Devices** pages.

The **Assets** page displays devices in the internal networks. When an asset is connected to the gateway, it automatically appears here.

The top of the page shows multiple counters:

- **Assets** - Total number of connected devices.
- **IoT Assets** - Relevant only when the IoT protection is enabled. For more information, see the *"IoT Protect" on page 300* page.
- **Manually blocked**.
- **Infected**.
- **Assets attempted to access unauthorized domains** - Assets which accessed or attempted to access a domain that is not under IoT policy in the last 7 days.
- **Not under IoT policy** - Relevant only when the IoT protection is enabled. For more information, see the *"IoT Protect" on page 300* page.

The graph icon on the far right shows the breakdown of the device types, such as IP camera, Media player, Scale, SmartTV, and Other.

You can filter to show a specific type of assets. For example, if you filter for IP camera, you see the number of IP camera types and the relevant vendors. You can see general information about the asset such as the traffic upload and download, and the policy. In the **Asset Details** tab, you can set the asset to bypass by Smart Accel, or bypass by SSL inspection. You can also create a network object directly from the **Assets** page.

All connected assets are displayed in a table with these columns:

- **Name** - Name of the device. The vendor icons appear next to the name.
- **IP Address**
- **Interface**
- **Vendor**
- **Device Type**

For each asset, click one of these options:

- Refresh
- **Actions**

  - **TCpdump Tool** - Opens a popup window in which you can capture traffic that passes through appliance interfaces. For more information, see *"Using System Tools" on page 507*.
  - **Reserve IP address** - Click **Add** to reserve an IP address for this asset. This creates a network object with the asset name.
  - **Export assets to a csv file** - Click the **Export to csv** button to create a csv file with all asset data.
  - **Block** - Prevent this asset from sending traffic.
  - **Delete** - Delete this asset from the list of connected devices.
  - **Monitoring** - Receive notifications if the asset is not answering to ping. You can do this per function or per asset.
  - **Recognize** - Run the recognition process for a single asset , all assets, or for unrecognized assets.
  - **Scan** - Scan the asset with one of these options: Ping, ARP, SNMP.
- Show WiFi data

On the **Assets** page, IoT assets that are **Not under IoT policy** are marked with this icon 💎 (relevant if the IoT blade is turned on).

**To see the Asset Details:**

1. Go to the **Home** > **Monitoring** > **Assets** page.
2. Click the table row with the asset name.
3. The **Asset Details** open in a popup window with these tabs:
   - **Asset Details** - Shows these fields: **Vendor**, **Model**, **Interface**, **Last seen**, **Download speed**, **Upload speed**, **View security logs**.
   - **IoT** - **Access from the Internet** (domains allowed to access your device) and **Policy**. If these options are grayed out, you cannot make any changes. Otherwise select from the pulldown menu).
   - **Override/Bypass** - Describes override and bypass behavior: **Asset description**, **Override** (select **Asset type** and **Vendor** from the pulldown menu), **Bypass** (select the applicable checkboxes to bypass by Smart Accel and to bypass by SSL Inspection.

**To see an asset's status:**

1. Go to the **Home** > **Monitoring** > **Assets** page.
2. Double -click the table row with the asset name.
3. Click the arrow next to **Status** to expand the section.
4. Select the **Filters** icon to see the number of assets in this category/rank:
   - **IoT** - Number of connected IoT devices.
   - **Manually blocked**
   - **Infected**
   - **Unauthorized** - Attempts to access unauthorized domains.
   - **Unprotected** - Number of devices not protected by the IoT protection policy,
   - **Low confidence** - You can protect an asset from the Assets page only if the Low confidence rank is less than 10. This means that the recognition service is not sure, for example, if the device is an IoT device.
   - **Override**
5. Click the arrow to expand the **Functions** section.
6. Click the arrow to expand the **Interface** section.

# Managing Active Devices

**Important** - This page is only relevant for versions up to R81.10.08. Starting in R81.10.10, **Active Devices** and **Wireless Active Devices** are replaced by the **Home** > **Assets** page.

The **Active Devices** page shows a list of the devices identified in internal networks. You can access this page from the **Logs and Monitoring** tab > **Status** section and from the **Home** tab > **Monitoring** section.

The table shows these columns:

- **Name** - Hostname of the device.
- **IP address** - IP address of the device.

  **Note** - If a device has both IPv4 and IPv6 addresses, there is a single entry in the table.
- **MAC Address** - MAC Address of the device.
- **Device Details** - Type of the device.
- **Blocked** - Indicates whether the device is blocked from network activity.
- **Interface** - Name of the appliance interface, to which the device is connected.

## Blocking a Device Manually

Click the device to select it and click **Block**.

# Toolbar Buttons

- **Filter** - Filter the list by servers, active devices, or known devices.
- **Refresh** - Refresh the information in the list.
- **Details** - Select a row in the list and click **Details** to show additional properties of the device.
- **Save as** - Save a selected device as a network object or server.

  When you select this option, the **New Network Object** (see *"Network Objects and Groups" on page 466*) window or **New Server Wizard** (see *"Defining Firewall Servers" on page 267*) opens.

  Enter the information in the fields and click **Apply**. Use these objects to reserve IP addresses to MAC addresses in the DHCP server and also add this object name as a device in the local DNS service. Network objects and server objects can be used in the security configurations, for example in the Access Policy and IPS exceptions

  A server object also allows you to configure access and NAT if applicable as part of the object. If access and/or NAT are configured, automatic access rules are created in the Access Policy Rule Base.
- **Start/Stop Traffic Monitor** - Gather upload and download packet rates for active devices.

  This operation may affect performance. To stop, click **Stop Traffic Monitoring**.
- **Revoke Certificate** - Revokes the certificate assigned to the device.

# Revoking the Hotspot Access

The display shows the devices connected to the gateway through a Hotspot.

You can revoke the Hotspot access for one or more devices.

This disconnects the device from the gateway and requires the device to log in again through the Hotspot.

**To revoke the Hotspot access:**

1. Click the record for the relevant device.
2. Click **Revoke Hotspot Access**.

   The access for that device is revoked. You must log in again through the Hotspot to reconnect the device to the gateway.

**Notes:**

- This page is available from the **Home** and **Logs & Monitoring** tabs.
- If there is no IPv6 activity in a dual stack host, the Active devices do not show the IPv6 address.

# Adding a New Network Object to Bypass SSL Inspection Based on the Host MAC Address

1. Click the device to select it.
2. From the toolbar, click **Save as** and select **Device type Network Object**.
3. For **Host MAC address**, enter a custom value or select from the menu.
4. Select **Bypass host with this MAC by SSL inspection**.
5. In **Object name**, enter the applicable text.
6. Click **Apply**

**Note** - You can also do this from the **Users & Objects** > **Network Objects** page. Click **New**, and then for **Type**, select **Device**.

# Viewing Monitoring Data

The **Monitoring** page shows network, security, and troubleshooting information. When you enter this page, the latest data appears.

You can click **Refresh** to update information.

To see a sample monitoring report, click **Demo**.

To close the sample reports, click **Back**.

The number of current connections in the system is shown for **VPN Tunnels**, **Active Devices**, and **Connections**.

You can click the links to open the corresponding WebUI pages.

The Monitoring page is divided into these sections:

- Network
- Security
- Troubleshooting

To expand or collapse the sections, click the arrow icon in the section's title bar.

## Network

By default, network statistics are shown for the last hour. You can also see statistics for the last day. Select the applicable option **Last hour** or **Last day** from the Network section's title bar.

The data is automatically refreshed for the time period:

**Last hour** - At one minute intervals. For example, if you generate a report at 10:15:45 AM, the report represents data from 9:15 to 10:15 AM.

**Last day** - At hourly intervals. For example, if you generate a report at 10:15 AM, the report represents data from the last 24 hours ending at 10:00 AM of the current day.

- **Bandwidth Usage** - The doughnut chart shows the top 10 applications or users that consumed the most bandwidth in the selected time frame (last hour or last day). Click the **Applications** or **Users** links to toggle between the statistics. To show user information the User Awareness blade must be activated.
- **Top Bandwidth Consuming** - Shows statistics for the top bandwidth consuming application, category, site, and user in percentages and the amount of traffic (MB or GB).
- **Traffic** - By default, shows the total amount of traffic received and sent in an area graph. The time axis reflects the time frame (last hour or last day) selected for the Network section. For last hour, the graph shows 5 minute intervals and for last day, hourly intervals. You can click the **Received** and **Sent** links to see only the amount of traffic received or sent. The orange area on the graph represents sent traffic. The blue area represents received traffic.

If you hover over a time interval, a popup box shows:

- The date and time
- The traffic sent or received
- The total traffic for that time interval
- Total traffic statistics - Next to the area graph you can see total traffic statistics for the last day or hour.

Security

**Infected devices** - Shows the number of:

- Infected devices
- Infected servers
- Recently active infected devices

You can click **All Infected Devices** to open the **Logs & Monitoring** > **Infected Devices** page.

**High risk applications** - Shows:

- The number of high risk applications
- The most used high risk applications
- The top users of high risk applications.

You can click **Applications Blade Control** to open the **Access Policy** > **Firewall Blade Control** page to see **Applications and URL Filtering** settings.

**Security events** - Shows the number of:

- Anti-Bot - Malwares detected by the Security Gateway.
- Anti-Virus - Malwares detected by the Security Gateway.
- Threat Emulation - Malicious files found since the last reboot and how many files scanned.
- The number of IPS attacks.

  You can click the links to open the **Threat Prevention** > **Blade Control** page.

# Troubleshooting

- **System Resources** - Click **CPU, memory and disk usage** to see CPU, memory, and disk usage information.
- **Device Info** - Shows Security Gateway information.
- Links to pages that can be useful for monitoring and troubleshooting purposes.

**Note** - This page is available from the **Home** and **Logs & Monitoring** tabs.

# Extended Monitoring

## Overview of Extended Monitoring

Quantum Spark Appliances do not have sufficient storage to keep all logs and monitoring data.

You can configure your Quantum Spark Appliance to upload the logs to Check Point cloud (the appliance uploads the logs to the Quantum Spark Management service in Infinity Portal).

When you need to review the data, your Quantum Spark Appliance download the applicable logs from Check Point cloud and shows them in WebUI.

## Requirements for Extended Monitoring

1. The Quantum Spark Appliance must run the firmware R81.10.15 or higher.
2. The Quantum Spark Appliance must be connected to Cloud Services with the option **"Use Cloud Capabilities"**.

   See *"Connecting to Cloud Services" on page 54*.

**Note** - If your Quantum Spark Appliance with the firmware R81.10.10 or lower was already connected to Quantum Spark Management, then after the firmware upgrade, the Extended Monitoring feature is available on your Quantum Spark Appliance.

## Description of the WebUI Page

The **Logs and Monitoring** view > **Monitoring** section > **Extended Monitoring** page shows three tabs with multiple sections:

- **Traffic** - with these sections:
  - **Sources by Bytes**
  - **Applications by Bytes**
  - **Destinations by Bytes**
  - **Services by Bytes**
- **Logs** - with these sections:
  - List of log records
  - **Statistics**
  - **Blade**
  - **Action**
  - **Interface Name**

  - **Origin**
  - **Service**
- **Remote Access** - with these sections:
  - Various widgets with data about the Remote Access VPN users and their traffic
  - **Top applications by traffic**
  - **Traffic over time**

## Viewing Log Records

You can review the logs in two places:

- In the Quantum Spark Management service > **Logs & Events** view.

  See the *Quantum Spark Management Administration Guide*.
- On your Quantum Spark Appliance > **Logs and Monitoring** view > section **Monitoring** > **Extended Monitoring** page.

  Each tab has the Search bar at the top:
  - On the left of the Search filed, you can click to select a preset time filter.
  - In the Search field, you can enter a string to filter the results in all sections (for example, enter an IP address).
  - On the right of the Search field, you can click the applicable button - to enable an automatic refresh or to refresh manually.

# Viewing Reports

The **Reports** page shows network analysis, security analysis, and infected devices reports by a selected time frame (monthly, weekly, daily, and hourly).

These elements influence the times shown in reports:

- Rounding off of time
- System reboot

### Rounding Off of Time

The times shown in generated reports are rounded down:

- For hourly reports - At one minute intervals. For example, if you generate a report at 10:15:45 AM, the report represents data from 9:15 to 10:15.
- For daily reports - At hourly intervals. For example, if you generate a report at 10:15 AM, the report represents data from the last 24 hours ending at 10:00 AM of the current day.
- For weekly reports - At four hour intervals, starting with 00:00, 04:00, 08:00 and so on. For example, if you generate a report at 11:55 AM, the report represents data from the last week ending at 08:00 AM of the current day.
- For monthly reports - At four hour intervals, starting with 00:00, 04:00, 08:00, 12:00 and so on. For example, if you generate a report at 11:15 AM, the report represents data from the last month ending at 08:00 AM of the current day.

### System Reboot

In the first 24 hour cycle after an appliance starts up (after installation or an update), the system adds one more time interval to the delta of the next applicable report interval.

For example, for weekly reports that are generated at pair hour intervals, the appliance requires 1 more hours plus the delta for the first applicable pair hour.

- For an appliance that started at 00:00 AM - The first weekly report is generated at 04:00 AM. The total of 4 hours derives from the first delta of the first applicable pair hour which is 02:00 and the added 2 hours. The total wait is 4 hours.
- For an appliance that started at 01:59 AM - The first weekly report is generated at 04:00 AM. The generated time derives from the delta of the first applicable pair hour which is 02:00 and the added 2 hours. The total wait is 2 hours.

After you start up an appliance, reports are generated:

- Hourly reports - 2-3 minutes from startup.
- Daily reports - 1-2 hours from startup.
- Weekly reports - 2-4 hours from startup.
- Monthly reports - 4-8 hours from startup.

**Note** - Only the last generated report for each report type is saved in the appliance. When you generate a new report, you override the last saved report for the specified type.

**To generate a report:**

Click the applicable time frame link at the top of the page (**Monthly**, **Weekly**, **Daily** or **Hourly**).

The line below the links shows the selected report and its time frame. To refresh the data shown, click **Generate**.

The report includes these sections:

- Executive Summary
- Table of Contents
- Report Pages

### Executive Summary

The first page of the report is the executive summary and shows:

- The number of Anti-Bot, Anti-Virus, and Threat Emulation malware detected by the Security Gateway and the number of IPS attacks.
- Top bandwidth consuming statistics by category, site, and user. You can click the **Top category**, **Top site**, or **Top user** link to get to the applicable report page. It also shows **Bandwidth Usage by Applications** statistics for the top 5 applications in a doughnut chart and total traffic received and sent.
- The number of infected devices, servers, and recently active infected devices.
- The number of high risk applications, the most used high risk applications, and the top users of high risk applications.
- The Security Gateway name, version, and MAC address.

### Table of Contents

The table of contents contains links to the network analysis, security analysis, and infected devices reports. Click a link to go directly to the selected section.

## Report Pages

Each report page shows a detailed graph, table, and descriptions.

**Note** - This page is available from the **Home** and **Logs & Monitoring** tabs.

# Using System Tools

On the **Tools** page you can perform various actions to diagnose problems with the appliance.

The same **Tools** page is available in:

- The **Home** view > **Troubleshooting** section.
- The **Device** view > **System** section.
- The **Logs & Monitoring** view > **Diagnostics** section.

| Action | Available From | Description |
|---|---|---|
| **Monitor System Resources** | R81.10.00 | Opens a popup windows that shows:<br>■ **CPU Usage History**<br>The information is refreshed automatically.<br>■ **Memory Usage History**<br>Memory usage is calculated without memory that was allocated in advance to handle traffic and without cache memory.<br>This gives a more accurate picture of the actual memory usage in the appliance but it may differ from figures you receive from Linux tools.<br>The information is refreshed automatically.<br>■ **Disk Usage**<br>Click the **Refresh** button for the most updated disk usage information.<br>Click the names of column to sort the output. |
| **Show Routing Table** | R81.10.00 | Opens a popup window that shows this information for each route:<br>■ **Source**<br>■ **Destination**<br>■ **Service**<br>■ **Gateway**<br>■ **Metric**<br>■ **Interface**<br>■ **Origin** |

| Action | Available From | Description |
|---|---|---|
| **Show Router Configuration** | R81.10.05 | Opens a popup window where you select one of the categories, and the window shows the corresponding Gaia Clish commands:<br>- **BGP**<br>- **OSPF**<br>- **Inbound route filters**<br>- **Route redistribution** |
| **Run Command** | R81.10.10 | Opens a popup window in which you can select a predefined CLI command and see its output:<br>- **Policy status** (shows the status of different security policies)<br>- **Scan network** (shows the connected IoT devices)<br>- **Show diagnostics** (runs the Gaia Clish command "`show diag`").) |
| **Test Cloud Services Ports** | R81.10.00 | Opens a popup window that shows the result of the Cloud Services Connectivity Test<br>(the output of the Gaia Clish command "`test cloud-connectivity`"). |

| Action | Available From | Description |
|---|---|---|
| **Tcpdump Tool** | R81.10.00 | Opens a popup window, in which you can capture traffic that passes through appliance interfaces.<br>❗ **Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window. |

| Action | Available From | Description |
|---|---|---|
| | | |

| Action | Available From | Description |
|---|---|---|
| **Firewall Monitor Tool** | R81.10.10 | Opens a popup window, in which you can capture traffic that passes through appliance interfaces.<br>**Warnings:**<br>■ When you use this tool, the CPU load increases. Schedule a maintenance window.<br>■ When you select the option "`-p all`", the CPU load increases significantly because this tool shows the information for each inspection chain module.<br>**Notes:**<br>■ The appliance runs the "`fw monitor`" command with the specified parameters.<br>See the:<br>• *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances* > Chapter "Miscellaneous Commands" > Section "fw commands".<br>• *R81.10 CLI Reference Guide* > Chapter "Security Gateway Commands" > Section "fw" > Section "fw monitor".<br>■ Compared to the **Tcpdump Tool**:<br>• This tool shows how each packet passes through the Security Gateway inspection chain modules.<br>• This tool saves the captured traffic only in the plain-text format (filename is "`fw_monitor.log`").<br>■ You can view the captured traffic in real time or save it into a plain-text file.<br>■ When you start a new traffic capture and save it into a file, and a file with such name already exists, the appliance adds a running number to the default filename (this way, it does not overwrite an existing file).<br>■ The appliance captures traffic only on interfaces with a configured IP address.<br>■ The packet capture stops automatically if the WebUI session ends.<br>**Procedure:** |

| Action | Available From | Description |
|---|---|---|
| | | 1. Click the **Firewall Monitor Tool** button.<br>2. **Optional:** Configure the applicable filters:<br>a. In the **Monitor outgoing packets** field, enter how many outgoing packets to capture before the tool must stop the traffic capture.<br>b. In the **Monitor incoming packets** field, enter how many incoming packets to capture before the tool must stop the traffic capture.<br>c. Select "**-p all**" to see the information for each inspection chain module.<br>**Warning** - The CPU load increases significantly.<br>d. Select "**grep**" to enter a free text filter.<br>■ This field is case-sensitive.<br>■ If the text must contains spaces, then you must enclose it in single quotes or double quotes.<br>■ The tool captures the specified number of packets, and then filters the output to show only the relevant lines.<br>3. To save the captured traffic into a plain-text file:<br>Note - If you selected "**grep**", then the saved file contains only the relevant lines you see on the screen.<br>a. Click **Save** to download the file.<br>b. Your web browser saves this file (`fw_monitor.log`) in the default download folder. |

| Action | Available From | Description |
|---|---|---|
| **Firewall Ctl Tool** | R81.10.10 | Opens a popup window, in which you can see the kernel debug that shows which packets the Security Gateway drops.<br>**Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window.<br>**Notes:**<br>- The appliance runs the "`fw ctl zdebug -m fw + drop`" command.<br>See the *R81.10 Quantum Security Gateway Guide* > Chapter "Kernel Debug".<br>- You can view the kernel debug output in real time or save it into a plain-text file.<br>- When you start a new kernel debug and save it into a file, and a file with such name already exists, the appliance adds a running number to the default filename (this way, it does not overwrite an existing file).<br>- The kernel debug stops automatically if the WebUI session ends.<br>**Procedure:**<br>1. Click the **Firewall Ctl Tool** button.<br>2. **Optional:** In the **Command timeout** field, enter the duration (in seconds) of the kernel debug.<br>3. **Optional:** In the "**grep**" field, enter the applicable filter:<br>- This field is case-sensitive.<br>- If the text must contains spaces, then you must enclose it in single quotes or double quotes.<br>- The tool captures the specified number of packets, and then filters the output to show only the relevant lines.<br>4. To save the kernel debug output into a plain-text file:<br>Note - If you entered a "**grep**" filter, then the saved file contains only the relevant lines you see on the screen.<br>a. Click **Save** to download the file. |

| Action | Available From | Description |
|---|---|---|
| | | b. Your web browser saves this file (`fw_ctl_zdebug_drop.log`) in the default download folder. |

| Action | Available From | Description |
|---|---|---|
| **VPN Debug Tool** | R81.10.10 | Opens a popup window, in which you can start a VPN debug.<br>**Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window.<br>**Notes:**<br>■ The appliance runs the "`fw ctl zdebug -m fw + drop`" command.<br>See the *R81.10 Quantum Security Gateway Guide* > Chapter "".<br>• *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances* > Chapter "Miscellaneous Commands" > Section "fw commands".<br>• *R81.10 CLI Reference Guide* > Chapter "Security Gateway Commands" > Section "fw" > Section "fw monitor".<br>■ You can view the kernel debug output in real time or save it into a plain-text file.<br>■ When you start a new kernel debug and save it into a file, the appliance adds a running number to the default filename (this way, it does not overwrite and existing debug file).<br>■ The kernel debug stops automatically if the WebUI session ends.<br>**Procedure:**<br>1. Click the **VPN Debug Tool** button.<br>2. Click the **Start Debugging** button.<br>3. Wait until you see the line "`VPN debugging in progress`".<br>4. Do **not** close this popup window (it will stop the VPN debug).<br>5. Replicate the VPN issue:<br>■ Remote Access VPN connection to this appliance.<br>■ Site to Site VPN connection to / from this appliance.<br>6. Click the **Stop Debugging** button.<br>7. Click **Download File** to download the archive with the required log files. |

| Action | Available From | Description |
|---|---|---|
| | | 8. Your web browser saves the archive file (`vpn_<YYYYMMDDHHMM>.tgz`) in the default download folder.<br>9. To have more information, also collect the CPinfo file - see the **Generate CPInfo File** below.<br>For the complete debug procedure, refer to sk62482. |
| **Display DSL Statistics** | R81.10.00 | Opens popup window that shows the DSL statistics.<br>Available only on DSL models. |
| **Generate CPInfo File** | R81.10.00 | Collects outputs of many commands and contents of various log files into an archive package.<br>This data helps Check Point Support understand the configuration and troubleshoot issues.<br>**Procedure:**<br>1. Click **Generate CPInfo File**.<br>A message next to the button shows the progress.<br>2. When the task completes, the button changes to **Download CPInfo File**.<br>3. Click **Download CPInfo File** to download the file.<br>4. Your web browser saves this file (`R81.10<Build>_<MMDDHHMM>.cpinfo.gz`) in the default download folder.<br>5. When the download completes, the button changes to **Generate CPInfo File**. |
| **Ping** | R81.10.00 | Opens a popup window that shows the result of the ping command to the specified IP address / hostname.<br>The appliance sends ICMP Requests to the specified destination. |
| **Trace** | R81.10.00 | Opens a popup window that shows the result of the traceroute command to the specified IP address / hostname.<br>The appliance sends ICMP Requests to the specified destination. |
| **Lookup** | R81.10.00 | Opens a popup window that shows the result of the DNS lookup for the specified IP address / hostname (the output of the Gaia Clish command "`nslookup`"). |

| Action | Available From | Description |
|---|---|---|
| **Download** | R81.10.00 | Opens sk159712 to download the Windows driver for a USB-C console socket.<br>**Explanation:**<br>When the mini-USB is used as a console connector, Windows OS does not automatically detect and download the driver needed for serial communication.<br>You must manually install the driver.<br>For more information, see sk182035. |

# Managing the Device

This section describes how to set up and manage your Quantum SparkAppliance.

## Configuring Internet Connectivity

The **Device** view > **Network** section > **Internet** page shows how the appliance connects to the Internet.

On this page you can:

- Add new IPv6 and IPv4 connections and edit, delete, or disable existing connections.
- Configure a single Internet connection or multiple connections in High Availability or Load Sharing configurations. When multiple Internet connections are defined, the page shows them in a table.
- Monitor the servers and Internet connections (see *"Monitoring" on page 113*).

We recommend you contact your local Internet Service Provider (ISP) to understand how to configure your specific Internet connection.

**Note** - ADSL/VDSL settings are relevant only for devices that have a DSL port. In 1570 / 1590 appliances, you can also configure a DSL connection over the DMZ port (see *"To configure an Internet connection over the DMZ port:" on page 99*).

### Getting Started

1. Connect with WebUI on the Quantum Spark Appliance at this address:

   ```
   https://<IP Address>:4434
   ```

2. Go to **Device** view > **Network** section > **Internet** page.
3. Configure an IPv4 Internet connection.
   a. Click **New** or **Add an IPv4 Internet connection**.

      The **New Internet Connection** window opens.

   b. Configure the required setting on the **Configuration** tab:

**Procedure**

i. Expand the **Internet Configuration** section.

ii. In the **Name** field, do one of these:

- Enter a name for the connection (you can change it later).
- Leave the default "**Internet<N>**" label (where **<N>** indicates an incrementing number).

For 15XX appliances, you can create a maximum of 10 Internet connections. For 1600, 1800, 1900, and 2000, the maximum number is 20. This includes alias IP connections.

iii. In the **Interface** field, select the required interface.

| Interface | Notes |
|---|---|
| **WAN** | Suitable for most types of Internet connections.<br>You can configure multiple static IP addresses on the same WAN interface. |
| **VXLAN** | Creates a VXLAN connection. |
| **DMZ** | Suitable for most types of Internet connections.<br>The DMZ port has 2 inputs:<br>■ LAN (RJ45) and SFP.<br>■ In non-VDSL 1570 / 1590 appliances, you can use an external DSL modem connected to the DMZ SFP port.<br>Only Check Point Branded SFP DSL is supported. Third party SFP DSL is not supported.<br>DMZ is not supported in 1530 / 1550 appliances. |
| **LAN<N>** | You can use unassigned LAN ports with no VLANs configured.<br>When you delete the Internet connection, the port reverts to an unassigned LAN.<br>If you remove or disable a LAN, any assigned alias IPs are also removed.<br>**Unassigned LAN ports use case** - If your company is in a region where Internet connections supplied by ISPs are unreliable and experience multiple disconnections, you can connect your appliances to multiple Internet connections from different ISPs. |

| Interface | Notes |
|---|---|
| **New Link Aggregation (Bond)** | Creates a link between two or more physical interfaces.<br>This improves performance and redundancy by increasing the network throughput and bandwidth.<br>A WAN or LAN bond can act like a regular Internet connection in the cluster flow.<br>A WAN bond in a cluster can be a monitoring interface. |
| **ADSL/VDSL** | If you select the ADSL/VDSL interface, you must select one of these in the **Type** field: **PPPoE**, **IPoE - static IP**, **IPoE - dynamic IP**. |

iv. In the **Type** field, select the required connection type.

> **Warning** - When you change the connection type in an existing connection, the appliance may disconnect from the Internet.

See:

- *"IPv4 Connection Types" on page 97*
- *"IPv6 Connection Types" on page 98*

Based on the selected connection type, additional fields may appear.

| Connection Type | Additional Fields |
|---|---|
| **DHCP** | None |
| **VXLAN** | ■ `VNI`<br>■ `Peer address`<br>■ `Destination port`<br>■ `Internet connection` |
| **Static IP** | ■ `IP address`<br>■ `Subnet mask`<br>■ `Default gateway` |

| Connection Type | Additional Fields |
|---|---|
| **PPPoE** | ■ `ISP login username`<br>■ `ISP login password` |
| **PPTP**<br>or<br>**L2TP** | ■ `Server IP address`<br>■ `ISP login username`<br>■ `ISP login password` |
| **Bridge** | ■ `Bridge to`<br>■ `DHCP/Static IP`<br>■ `Default gateway` |

v. If applicable, select the option **Use connection as VLAN**.

vi. New in R81.10.15: **High Availability Settings** section.

> **Note** - This section is only visible if you configured a cluster.

**High Availability** is enabled by default.

Enter the **Cluster IP address** (the virtual IP address of the cluster) and the Peer physical IP address.

> **Note** - Changes made here appear in the list of **Configured Interfaces** on the High Availability page, including their status (**High Availability** or **Sync**). The **Cluster status** for an Interface also appears on the relevant **Edit Internet Connection** window of the **Local Network** page.

vii. **Optional:** Expand the **DNS Server Settings** section and configure the required DNS servers.

This section appears for specific connection types (for example, for **Static IP** and **Bridge**).

c. Configure the required settings on the **Connection Monitoring** tab:

**Procedure**

> **Note** - Based on the selected connection type on the **Configuration** tab, some options may not be available.

i. Expand the **Connection Monitoring** section.

ii. Select **Automatically detect loss of connectivity to the default gateway** to detect connectivity loss by sending ARP requests (pinging) to the default gateway and expecting responses.

> **Important** - If you use Dynamic Routing, you must clear this option to prevent probing of the default gateway.

iii. Select **Monitor connection state by sending probe packets to one or more servers on the Internet** to detect connectivity loss by using more methods and servers.

> **Important** - In versions R81.10.10 and higher, it is supported to disable probing in an Internet connection only if you clear the option, "This Internet connection will be a part of SD-WAN" (on the "Advanced" tab > section "SD-WAN Settings").

iv. In the **Connection probing method** section, select one of these:

- **Ping addresses** - To send pings to the servers configured on this tab (enter an IP address or a hostname).
- **Probe DNS servers** - To send pings to the DNS servers you configured on the **Configuration** tab.

d. Configure the required settings on the **Advanced** tab:

**Procedure**

> **Note** - Based on the selected connection type on the **Configuration** tab, different sections and options appear.

In the **IP Address Assignment** section (for PPPoE, PPTP, or L2TP), configure the applicable settings.

**Configuration**

- **Local tunnel IP address**

  Configures how this Internet connection (PPPoE, PPTP, or L2TP) gets its local IP address - automatically or uses the configured IP address.

- **Unnumbered PPPoE**

  Controls whether the appliance dials only one time and supports a range or IP addresses assigned by an ISP.

- **WAN IP assignment**

  Configures how this Internet connection (PPTP or L2TP) gets its WAN IP address - automatically or uses the configured IP address, Subnet mask, and Default gateway.

In the **Service Provider Assignment** section (for PPPoE, PPTP, or L2TP), configure the applicable settings.

**Configuration**

- **Service**

  Optional. Configures a name for the dial service name.

- **Authentication method**

  Configures the authentication method for the dial service (`Auto`, `PAP`, `CHAP`).

In the **Connect on demand** section (for PPPoE, PPTP, or L2TP), configure the applicable settings.

**Configuration**

**Connect on demand**

Controls whether to use the connect-on-demand feature.

Applies only when you are in a High Availability cluster of appliances.

In the **Port Settings** section, configure the applicable settings.

**Configuration**

- If necessary, select **Use custom MTU value** and configured the **MTU size** value.

  You can apply an MTU on:

  - LANs and DMZ – They must be separate networks, or assigned to a bridge network.
  - Switches - The MTU is assigned to the switch itself, not the LANs that are assigned to it.
  - Bonds
  - VLANs - The VLAN MTU must be lower or equal to its parent MTU.

  You **cannot** apply an MTU on:

  - Interfaces assigned to switches or bonds.
  - Bridges - Configure the MTU separately for each of their children.
  - Aliases
  - Virtual Access Points

  To avoid fragmentation (which slows transmission), set the MTU according to the smallest MTU of all the network devices between your gateway and the packet destination

  For static and DHCP mode, set MTU to 1500 or lower.

  For PPPoE connections, set MTU to 1492 or lower.

  **Note** - When the appliance is behind a modem that works as a NAT device, the MTU value of the connection must be the same as configured in the modem. If the modem has a PPPoE connection, configure the MTU in the connection to 1492 or lower.

- **MAC address clone**
  - **Use default MAC address** - This Internet connection uses the default MAC address of the selected physical port.
  - **Override default MAC address** - You can override the default MAC address for this Internet connection. This is useful when the appliance replaces another device and it is necessary to mimic its MAC address.
- **Disable auto negotiation**

  If you select this option, you can configure the link speed and duplex for this Internet connection.

  Different values are available for different appliance models.

In the **QoS Settings** section, configure the applicable settings.

**Configuration**

**Important:**

- This applies only to IPv4 Internet connections.
- To apply these QoS settings, you must enable the QoS Software Blade:
  Go to the **Home** view > **Overview** section > **Security Dashboard** page > in the **QoS** section, move the slider to the right position (enabled green).

- **Enable QoS (download)**

  Enables and configures the restriction for the inbound traffic (download on the internal networks behind the appliance).

- **Enable QoS (upload)**

  Enables and configures the restriction for the outbound traffic (upload on the internal networks behind the appliance).

In the **ISP Redundancy** section, configure the applicable settings.

**Configuration**

**Important:**

- This applies only to IPv4 Internet connections.
- Locally Managed - Starting from R81.10.10, ISP Redundancy is deprecated in Locally Managed appliances. For versions lower than R81.10.10, follow the instructions below.
- Centrally Managed - Follow the instructions below.

You can configure multiple IPv4 Internet connections in High Availability or Load Balancing modes. When you configure more two or more Internet connections, you can configure the ISP Redundancy mode on the **Device** view > **Network** section > **Internet** page (at the top of the page > below the line **Multiple Internet connections**).

In this **ISP Redundancy** section of each Internet connection you can configure the priority or weights of each Internet connection (based on the configured ISP Redundancy mode).

- **Route traffic through this connection by default**

  Controls whether the appliance sends all traffic through this Internet connection.

  The appliance sends traffic through this Internet connection device only if specific, usually service-based, routing rules exist for this Internet connection. This is commonly used when you have a connection that is used for dedicated traffic.

  When you clear this option, this connection does not participate in ISP Redundancy.

- **High Availability** > **Priority**

  Configures the priority for the Internet connection in ISP Redundancy. The appliance uses an Internet connection with a lower priority only if an Internet connection with a higher priority failed.

- **Load Balancing** > **Weight**

  Configures how to share the traffic between the Internet connections.

In the **NAT Settings** section, configure the applicable settings.

**Configuration**

**Do not hide internal networks behind this Internet connection**

Controls whether to disable NAT for traffic from your internal networks that goes through this Internet connection.

In the **Bond Settings** section, configure the applicable settings.

**Configuration**

- **Hash policy**

  Configures the Bond hash policy (how to assign connections to Active subordinate interfaces):

  - `Layer2` - Based on the XOR of hardware MAC addresses.
  - `Layer2+3` - Based on the XOR of hardware MAC addresses and IP addresses.
  - `Layer3+4` - Based on the IP addresses and Ports.

- **MII interval**

  Configures the Bond Media Monitoring Interval (MII) that specifies how much time in milliseconds to wait before checking the link on subordinate interfaces for a failure.

In the **DHCP Settings** section, configure the applicable settings.

**Configuration**

**Hostname via DHCP**

Controls whether the appliance gets its hostname from your DHCP server.

In the **SD-WAN Settings** section, configure the applicable settings.

**Configuration**

- **Download speed (Mbps)**

  Configures the restriction for the inbound traffic (download on the internal networks behind the appliance) if this Internet connection participates in SD-WAN.

- **Upload speed (Mbps)**

  Configures the restriction for the outbound traffic (upload on the internal networks behind the appliance) if this Internet connection participates in SD-WAN.

- **This Internet connection will be a part of SD-WAN**

  Configures this Internet connection to participate in SD-WAN.

  Refer to the **Access Policy** view > **Firewall** section > **SD-WAN** page.

- **This Internet connection will be set as backup in SD-WAN**

  Configures this Internet connection to participate in SD-WAN as a backup for the main SD-WAN Internet connection. Select this only for links that are expensive or of poor quality. For example, Cellular networks have a plan, and if you exceed your limit it can be costly. In the MPLS network, you pay per use.

4. Click **Save**.

# IPv4 Connection Types

### IPv4 connection types

Select the connection type:

- **DHCP** - Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses within a specified range to devices on a network. The device retains the assigned address for a specified administrator-defined period. This does not apply to the ADSL/VDSL interface.
- **Static IP** - A fixed (non-dynamic) IP address. If you want an alias IP, configure another static IP type connection on the same internet port. Example: WAN and WAN:1 (WAN:1 is the alias IP).
- **PPPoE** - A network protocol to encapsulate Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly in DSL systems. PPPoE can run directly over the ADSL/VDSL interface as well as the DMZ interface with the SFP port. It can also run over WAN or DMZ interfaces that are typically connected to an external DSL modem. You must enter the **IP address**, the **subnet mask**, **default gateway** and **DNS Server Settings**.
- **IPoE - dynamic IP** (DSL only) - The Internet IP of the appliance is imported through DHCP.
- **IPoE - static IP** (DSL) **-** The Internet IP of the appliance is determined statically. You must enter the **IP address**, the **subnet mask**, **default gateway** and **DNS Server Settings.**
- **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
- **L2TP** - Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol. It does not provide any encryption or confidentiality but relies on an encryption protocol that it passes within the tunnel to provide privacy.
- **Bridge** - Connects multiple network segments at the data link layer (Layer 2).
- **Bridge DHCP** - The bridge is configured as a DHCP client and the DHCP settings (including IP and subnet) are removed.
- **Cellular** - This is for appliances with an internal LTE modem. Both SIM cards are used for the internet connection with a failover between them. The cellular connection can be over IPv4 or IPv6 and is configured the same way in both.
- **Cellular Modem** - Connect to the Internet with a cellular modem to the ISP through a 3G or 4G network. For this option, select the USB/Serial option in the Interface name.

ℹ **Notes**:

- Only one cellular modem is supported.
- Only customers with an approved RFE will be supported with the external modem specified in the RFE.

# Bridged Internet Connection in a Cluster

Starting from R81.10.15, you can configure a bridged internet connection in a cluster. The bridge is configured between an internet connection and a LAN interface.

**Procedure:**

1. On the **Internet** page, click **Add an internet connection**. In the **New Internet Connection** window, for **Type** select **Bridge**.
2. In the **Bridge to** field, select **New** This opens the **New Bridge** window.
3. For **Bridge children**, select any LAN interface.
4. Enter the IP address, Subnet mask and Default Gateway.
5. Click **Save**.

# IPv6 Connection Types

## IPv6 connection types

- **Static IPv6** - A fixed (non-dynamic) IP address.
- **Obtain automatically (DHCPv6/SLAAC)** - In both Dynamic Host Configuration Protocol (DHCP) and Stateless Address Auto Configuration (SLAAC) the user does not set the IP as this is handled by the router/DHCP server. DHCPv6 issues a full IP address. SLAAC issues an IP address prefix, and the gateway completes the rest of the address according to discovery protocols.
- **PPPoE (IPv6 only)** - A network protocol to encapsulate Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and Metro Ethernet networks.
- **PPPoE (IPv4/IPv6)** - Same as **PPPoE ( IPv6 only)**, but the user must first configure a type IPv4 PPPoE internet connection on the same interface. Use this option when the ISP provides both IPv4 and IPv6 addresses through the same PPPoE connection. This prevents the need to define the same dialer connection details more than once.
- **IPv6 Bridge** - A Layer 2 bridge between internal and external networks, containing both IPv4 and IPv6 addresses (or just IPv6) to make the gateway reachable through the bridge in a dual stack/pure IPv6 network.

  Supported as static WAN IP and DHCP.

**To configure an Internet connection over the DMZ port:**

1. On the **Configuring Internet Connectivity** page, click **New** to create a new Internet connection.

   The **New Internet Connection** window opens in the **Configuration** tab.

2. For **Interface**, select **DMZ**.

   - For a DSL over DMZ Connection, select **SFP-DSL**.
   - For a non-DSL connection, select **RJ45/SFP-Fiber**.

3. Click **Save**.

# IPv6 configuration

**To configure an IPv6 internet connection:**

**Step 1 - Enable IPv6**

1. Go to **Device** > **System** > **System Operations**.
2. In the section **IPv6 Settings**, click **Enable IPv6**.

This allows you to configure an IPv6 address in network and policy settings.

**Note** - The appliance reboots automatically after you enable IPv6.

**Step 2- Configure an IPv6 Internet connection**

1. Go to **Device** > **Network** > **Internet**.

   If you enabled IPv6 in Step 1, you now see an **IPv6 section** on this page.

2. Beneath the line **No IPv6 Internet connection is configured**, click **Configure Internet**.
3. In the **New IPv6 Internet Connection** window, configure the new IPv6 Internet connection settings and click **Save**.

   The **IPv6 section** on the Internet page now shows the new IPv6 connection.

4. On the **Local Network** page, the table of local interfaces shows a column for IPv6 in addition to IPv4

### Prefix delegation

When an Internet connection has prefix delegation enabled, the gateway can request a prefix (in addition to an IP address) from the server and configure an internal network DHCPv6 server that uses this prefix. Connected devices are then routable without the need to use NAT.

These connection types support prefix delegation:

- PPPoE-IPv6
- LAN-IPv6
- VLAN
- Switch
- Bridge

**To enable prefix delegation in an IPv6 connection:**

1. On the **Internet Connectivity** page, click **New** to create a new IPv6 connection.

   The **New IPv6 Internet Connection** window opens.
2. In the **Advanced** tab, select **Enable prefix delegation for this Internet connection**.
3. Click **Apply**.

   **Note** - Configure the settings for this Internet connection in the **Configuration** tab.

A network or bridge with prefix delegation enabled must have the **IPv6 Auto Assignment** set to **SLAAC**, **DHCPv6**, or **Disabled**.

For each delegated network, the behavior depends on the IPv6 Auto Assignment settings:

| IPv6 Auto Assignment setting | Delegation Action |
|---|---|
| Disabled | Address range is set according to the prefix and subnet. The DHCPv6 server is automatically enabled when it receives a prefix. |
| SLAAC | Addresses are provided via Stateless Address Auto Configuration, according to SLAAC rules. The prefix and subnet are provided. |
| DHCPv6 | Address range is set according to the prefix and subnet. |

### Neighbor Discover Protocol (ND-Proxy)

On some IPv6 networks, where prefix delegation is not supported, you can use the Neighbor Discover Protocol (ND proxy) to assign globally-routable IPv6 addresses to internal (LAN) interfaces and hosts.

**Workflow:**

1. The Security Gateway receives a globally-routable /64 IPv6 prefix from the ISP through a dynamic IPv6 Internet-connection, using RA (Router Advertisement).
2. Instead of assigning an IPv6 address to the Internet-connection interface (using SLAAC), the address is assigned to one of the internal interfaces(LAN, DMZ, Bridge, and so on).
3. SLAAC is enabled automatically on the internal network/bridge.

   Hosts behind this internal network/bridge receive a globally-routable IPv6 address automatically.
4. The Internet-connection interface is not assigned with any global IPv6 address, but still has a link-local IPv6 address.
5. A default-gateway route is created to the ISP's gateway link-local address (as with all IPv6 Internet-connection).
6. ND proxy is used to answer Neighbor Discovery requests from the ISP side to the internal network for hosts that were assigned addresses with IPv6 prefix received from the ISP.

**To enable ND proxy:**

1. In the **Configuring Internet Connectivity** page, click **New/Edit the IPv6 connection**.

   The Edit Internet Connection window opens in the **Configuration** tab.
2. For **Connection type**, select **Obtain automatically (DHCPv6/SLAAC)**.
3. In the **Advanced** tab, expand the **Neighbor Discovery proxy** section.
4. Select the **Enable Neighbor Discovery proxy** checkbox.
5. Select your **local network** from the drop down menu.
6. Make sure **NAT Settings** are disabled:
7. Expand the **NAT Settings** section and select the **Do not hide internal networks behind this Internet connection** checkbox.
8. Make sure **Prefix Delegation** is disabled:

9. Expand the **Prefix Delegation** section and make sure that **Enable prefix delegation for this Internet connection is not checked**.
10. Click **Apply**.

### IPv4 gateway option on IPv6 bridge

This feature is available starting from R81.10.15.

**Use Cases**:

You can configure the IPv4 gateway setting manually while the IPv6 still uses DHCP/SLAAC and add a default IPv4 gateway.

**Procedure:**

1. In the **Internet** page, click **New/Edit the IPv6 connection**.
2. The **Edit IPv6 Internet Connection** window opens in the **Configuration** tab.
3. For **Interface**, select **WAN**.
4. For **Type**, select **IPv6 Bridge**.
5. For **DHCPv6/SLAAC or Static IP**, select **Static IP**.
6. Enter the **Default gateway (IPv4)**.
7. Enter the **Default gateway (IPv6)**.
8. **Optional**: In the **DNS Server Settings** section, enter the **DNS server(s)** (first, second, and third).
9. Click **Save**.

### DS-Lite (Dual Stack Lite)

DS-Lite is a connection type used by ISPs to provide Internet access to IPv4 networks and services. It can be WAN, DMZ, or an unassigned LAN port. You can use DS-Lite to carry IPv4 traffic over an IPv6 tunnel between the gateway and a server.

IPv6 connection types:

- DHCPv6
- PPPoE
- Static IP - WAN, DMZ or unassigned LAN port.

The DS-Lite master WAN connection type must be one of these:

- Dynamic IPv6
- Static IPv6
- PPPoEv6
- Bridge IPv6

**To enable DS-Lite:**

1. In the **Configuring Internet Connectivity** page, click **New/Edit the IPv4 connection**.

   The Edit Internet Connection window opens.

2. For **Connection type**, select **DS-Lite**.

   **Note** - Make sure the interface type is the same for both IPv4 and IPv6. For example, if the IPv4 the interface is configured as WAN, the IPv6 interface must also be configured as WAN.

3. The **AFTR address** field is displayed.

   **Note** - This field is not mandatory when the IPv6 connection type is DHCPv6.

4. In the **Linked connection** field, select the IPv6 connection name.
5. In the **Advanced** tab:
   - Set the default **MTU** of the DS-Lite interface to 1460 (IPv4 default = 1500)
   - Set the size of the **IPv6 header** to 40.
6. Click **Apply**

### IPIP

IPIP, a variation of DS-Lite, is used to tunnel IPv4 traffic over IPv6-only networks. As in DS-Lite, the IPv4 traffic is tunneled over an existing IPv6 connection. The DS-Lite/IPIP tunnel is created between the client (gateway) and a peer (AFTR which resides on the ISP and is configured statically or acquired via DHCPv6).

IPIP uses the same IPv4-over-IPv6 tunnel as DS-Lite, but you can configure a static IPv4 address, which is globally routable.

The gateway first establishes an IPv6 connection to the ISP. The IPv6 address consists of:

- **Prefix** - Obtained using prefix delegation or RA messages (SLAAC).
- **Suffix** - Configured by the user

Comparison of DS-Lite and IPIP:

- Both DS-Lite and IPIP use an IPv6 internet connection to carry the IPv4 traffic.
- DS-Lite - The gateway address is non-globally-routable and automatically selected from the subnet 192.0.0.0/32.

  IPIP - The gateway address is globally-routable and you configure it manually.
- In both DS-Lite and IPIP, you can get the prefix of the IPv6 address dynamically using SLAAC.
- DS-Lite - The IPv6 address is automatically generated based on the acquired prefix and an auto-generated suffix, based on the interface Ethernet MAC address.

  IPIP - The IPv6 address must end with a manually configured suffix.
- When the prefix of the IPv6 carrying the IPIP connection is changed, you must notify the IPIP tunnel provider over HTTP.

The WAN connection type of the IPIP master must be **Dynamic IPv6**.

**To enable IPIP:**

1. Enable the IPIP feature in *"Advanced Settings" on page 246*.
2. Configure an IPv6 Internet connection.
3. In the **Configuring Internet Connectivity** page, click **New/Edit the IPv4 connection**.

   The **Edit Internet Connection** window opens.
4. For **Connection type**, select **IPv4 over IPv6 (IPIP)**.

   **Note** - Make sure the interface type is the same for both IPv4 and IPv6. For example, if the IPv4 the interface is configured as WAN, the IPv6 interface must also be configured as WAN.
5. The **AFTR address** field appears. This field shows the hostname or IPv6 address for DS-Lite/IPIP tunnel.

   **Note** - This field is optional when the IPv6 connection type is DHCPv6.
6. In the **Linked connection** field, select the IPv6 connection name.

   This is the IPv6 Internet connection index on which the DS-Lite/IPIP tunnel is defined.

   **Note** - The IPIP tunnel and its linked IPv6 connection must be on the same appliance port.
7. In the **VNE Settings** section:

   VNE is an added service that enables you to send an HTTP(S) request to your provider's server and update them that your IPv6 address changed.

   For **Service name**, select one of these:

- **Transix** - If you select this option, these fields appear:
  - **Update server URL** - The Server URL if your IPv6 changed. Default value: http://update.transix.jp/request
  - **User Name** - Your username for the updater service.
  - **Password** - Your username password for the updater service.
- **v6 Connect** - If you select this option, these fields appear:
  - **Update server URL** - The Server URL if your IPv6 changed. Default value: https://v6update.asahi-net.or.jp/prefix
  - **User Name** - Your username for the updater service.
  - **Password** - Your username password for the updater service.
- **Xpass** - Includes additional services such as DDNS and the ability to buy a prefix of IPv4. With Xpass, you can support 1/8/16 Static IPv4 address. If you select this option, these fields appear:
  - **Update server URL** - The Server URL if your IPv6 changed.
  - **User name** - Your username for the updater service.
  - **Password** - Your username password for the updater service.
  - **FQDN** - The URL in this contract (Example: 1234abcd.v4v6.xpass.jp this URL maps to the gateway).
  - **DDNS ID** - The ID for the DDNS service.
  - **DDNS Pass** - The password for the DDNS service.
  - **Unnumbered** - Select this checkbox if you want your IP1, IP8 or IP16 IPv4 address to be unnumbered for the option to assign the public IP from the WAN network on LAN.
- **General**

  When you select this option, you do not need to enter your credentials.

8. In the **Advanced** tab:

   a. In the **IPv4 over IPv6 (IPIP) Settings** section, select **Enable static IPv6 suffix**.

      ⓘ **Note** - This is configured in the IPv6 connection configuration window. Otherwise, IPIP is configured on the IPv4 connection.

   b. Configure the default **MTU** of the IPIP interface to 1460 (IPv4 default = 1500). The size of the IPv6 header is 40.

9. Click **Apply**.

### MAP-E

Mapping of Address and Port using Encapsulation (MAP-E), like DSLite, is a mechanism to facilitate the transition from IPv4 to IPv6. It relies on an IPv6 network backbone to carry IPv4 traffic. Both the address and port mapping information are embedded within the IPv6 address. Unlike DSLite, this method involves a direct mapping scheme without the need for a centralized CGNAT. IPv4 packets are encapsulated in IPv6 but use predefined mapping rules to determine the destination.

This feature is available starting from R81.10.15.

**Use Cases**:

MAP-E is a less expensive method for end users seeking a scalable, decentralized approach to manage IPv4 traffic over an IPv6 network, especially in environments with high traffic volumes that need efficient resource utilization.

**Procedure:**

1. On the **Internet** page, click **New** > **New Internet Connection**.
2. In the **New Internet Connection** window, enter the **Name** and select the **Interface** from the pulldown menu.

   Supported interfaces (must have the DHCPv6/SLAAC internet connection):

   - WAN
   - DMZ
3. For **Type**, select **Mapping of Address and Port**.
4. Select the **Linked connections** from the pulldown menu. This is the IPv6 connection that the MAP-E is routed over.
5. In the **MAP-E Settings** section, select the **MAP-E vendor**:
   - **OCN Virtual Connect** - Connection options: Dynamic or Static mode
   - **JPX** - Connection options: Dynamic mode only
6. For **MAP-E connection type**, select **Dynamic** or **Static**.
   - **Dynamic** - Gives the port range you can use within your IPv4 connection. This is a subset of all the available ports.
   - **Static** - You can use the entire port range. If you select this mode, enter the **Update server URL**, the **Username**, and the **Password**.
7. Select or clear the **Unnumbered IP address** checkbox. This is the option to allow assigning the WAN IP to the LAN IP.
8. Click **Save**.

On the Internet page, you now see the new Internet connection. Check that the status shows as **Connected** and probing is enabled.

**To see the available Port Ranges:**

1. Click the **MAP-E options** link.
2. **The MAP-E Options and Monitoring** page opens and displays the **Last update time**, the **Service name**, and the port ranges.
3. **Optional** - Click to **Refresh View** or to **Clear the MAP Table**. Clearing the MAP table deletes the current MAP-E rule (the IP address, and the port range) and fetches a new one. If the values of the new MAP-E rule are different, this results in a reconnection and a different IP address.

# Other configuration types

### Creating a new BOND (WAN)

1. In the **Internet Connection page**, to create a new internet connection, click **Configure internet**.

   The **New Internet Connection** window opens in the **Configuration** tab.

2. Under **Internet Configuration**, enter the **Connection name**.
3. For **Interface**, select **New link aggregation (Bond)**.
4. For **Ports**, select a minimum of 2 interfaces that are unassigned and disabled.

   **Note** - 1530 / 1550 appliances do not have a DMZ port.

5. Select the **Operation mode**:
   - **802.3ad** - Dynamically uses Active interfaces to share the traffic load.
   - **Round Robin** - Selects the Active interface sequentially.
   - **XOR** - All interfaces are Active for Load Sharing. Traffic is assigned to Active interfaces based on the transmit hash policy (Layer2 or Layer3+4).
   - **High Availability (Active/Backup)** - Gives redundancy when there is an interface or link failure. If you select this mode, you must select a **Master** i.e. the primary/default port for the traffic.
6. Select the **Connection type**.
7. In the **Advanced** tab, select the **Mii interval**. The Mii interval is the frequency (in ms) that the system polls the Media Independent Interface (Mii, the standard interface for fast Ethernet) to get status.
8. If you selected **802.3ad** or **XOR** as your operation mode, select the **Hash policy** from the dropdown menu.
   - `Layer2` - Based on the XOR of hardware MAC addresses.
   - `Layer2+3` - Based on the XOR of hardware MAC addresses and IP addresses.
   - `Layer3+4` - Based on the IP addresses and Ports.
9. Click **Apply**.

**To add a Bond as an additional internet connection:**

1. In the **Internet Connection** page, click **Add an internet connection...**

   The **New Internet Connection** window opens in the **Configuration** tab.

2. Configure the rest of the fields as for a new connection.

# Cellular Connections

### Configuring a Cellular Internet Connection

**Note** - The gateway can connect through IPv4, IPv6 or a mixed IPv4v6 service.

1. Click **Configure Internet** (if not configured at all), **Add** (for another Internet connection), or **Edit**.

   The New or Edit Internet Connection window opens.

2. In the **Configuration** tab, select **Cellular** for **Interface name**.
3. Click **Apply**

   **Note** - This closes the Edit Internet Connection window.

   The remaining steps are optional additional settings and are not essential for configuration.

4. In the **Cellular** tab, under **Cellular settings**, select the **Primary SIM** and which SIM to disable: **SIM 1**, **SIM 2** or **Neither**.
   - SIM 1 - Micro-SIM
   - SIM 2 - Nano-SIM
5. For each SIM, enter the **APN** and **PIN** number.

   **Note** - Some cellular carriers require a password to access the cellular Internet. In this case, the administrator must enter the credentials to connect to the appliance.

6. For Connection Type, select one of these values:
   - IPv4 - Both SIMs are configured to IPv4 only
   - IPv6 - Both SIMs are configured to IPv6 only

- IPv4v6 - There are two connections, one IPv4 and one IPv6. Select this if one of the SIM cards is configured as dual-stack, or if the two SIM cards are configured with different connection types

7. Configure the **Connection Monitoring** and **Advanced** tabs as for other interface connections.
8. Click **Apply**

### Linking the APN to a SIM card based on a specific MMCNMC number

1. Connect to the command line on the Quantum Spark appliance.
2. If your default shell is Bash, go to Gaia Clish:

   ```
   clish
   ```

3. Disable the use of the configuration file:

   ```
   set os-settings advanced-settings use-secondary-mccmnc-file
   false
   ```

4. Go from Gaia Clish to the Expert mode:
   - If your default shell is Gaia Clish:

     ```
     expert
     ```

   - If your default shell is Expert mode:

     ```
     exit
     ```

5. Back up the current configuration file:

   ```
   cp -v /pfrm2.0/etc/usb_dev/mcc_mnc_secondary_list.conf{,_BKP}
   ```

6. Edit the current configuration file:

   ```
   vi /pfrm2.0/etc/usb_dev/mcc_mnc_secondary_list.conf
   ```

7. Configure the required values.

   Format:

   ```
   [<SIM ID Number (MCC/MNC)>]
   apn=<STRING>
   carrier_package=<STRING>
   ```

   Example:

   ```
   [302220]
   apn=isp.telus.com
   carrier_package=TELUS
   ```

8. Save the changes in the file and exit Vi editor.

9. Go from the Expert mode to Gaia Clish:

   - If your default shell is Gaia Clish:

     ```
     exit
     ```

   - If your default shell is Expert mode:

     ```
     clish
     ```

10. Enable the use of the configuration file:

    ```
    set os-settings advanced-settings use-secondary-mccmnc-file
    true
    ```

### Switching the Active Image

For Security Gateways with cellular Internet connections, you can switch the active image between carrier-approved firmware configurations.

The image contains files used to configure the module for use with specific carriers. Multiple images can be stored on the device. During a firmware upgrade, you can add images packages to the module or replace an image with a newer version.

**Note** - You can only switch to an image already uploaded to the module.

The image package contains these files:

- **Firmware file** - Contains the module's firmware.
- **Carrier Configuration file** (the Product Release Information or PRI) - Contains custom settings for a specific carrier and is linked internally to a specific firmware file.

The module runs an active image which contains a single uncompressed copy of a firmware file and a single configuration file.

To see a list of available carriers and their image packages, go here.

- EM7455 - Global region
- EM7430 - APAC region

**Use cases:**

Some carriers require the module to run a specific carrier configuration file, and may also request this for the certification process. In addition, the carrier configuration file ensures the use of carrier-specific parameters when you register with that carrier.

### To select an active image for a SIM:

1. In **Device** > **Internet**, double click an existing cellular connection, or select the connection and click **Edit**. You can also click **New** to create a new cellular connection.

   The **Edit Internet Connection** window opens.

2. In the **Cellular** tab, for each SIM, select the new **Carrier configuration package** from the list of supported image package names. Each SIM can have a different carrier.

   **Note** - This list dynamic, based on the valid installed packages on the modem.

3. Click **Apply**

On the **Internet** page, the **Status** changes to **Connecting** with the message:

```
Switching carrier configuration package. This may take a few
minutes.
```

### To disable image switching:

In the **Cellular** tab, for each SIM, select **None** for the Carrier configuration package.

- For PPPoE over ATM over VDSL/ADSL or IPoE over ATM over VDSL/ADSL or for an ADSL interface:
  - Enter the **VPI number** and **VCI number** you received from your service provider, and the **Encapsulation type** (LLC or VC_MUX).
- For WAN/DMZ interfaces and static, DHCP, PPPoE, PPTP, and L2TP connection types

  or

  For VDSL/ADSL interfaces and IPoE - dynamic IP and IPoE - static IP connection types over PTM:
  - **Use connection as VLAN** - Select this checkbox to add a virtual Internet interface.
  - **VLAN ID** - Enter a VLAN ID between 1 and 4094.

If you are in an **Annex L** system, in **Advanced Settings**, you must enable the **Annex L** and disable the **Annex J/M**.

If you are in an **Annex M** system, in **Advanced Settings**, you must enable **Annex J/M** and disable the **Annex L**.

In all other Annex systems, no changes are needed to the default configuration.

**Notes:**

- Multiple Internet connections can be established over a single VDSL/ADSL connection carrying PTM traffic or in the case of WAN and DMZ interfaces.
- Only one Internet connection can be established over a VDSL/ADSL interface carrying ATM traffic or a USB interface.
- One IPoE or PPPoE connection can be established over ATM running over the DSL interface.
- A single IPoE connection or multiple PPPoE connections can be established over one untagged DSL interface carrying PTM traffic.
- A single IPoE connection or multiple PPPoE connections can be established over one VLAN tagged DSL interface carrying PTM traffic.
- A single DHCP or Static IP connection can be established over a USB interface.
- A single DHCP or Static IP connection or multiple PPPoE connections can be established over one untagged or one VLAN tagged WAN or DMZ interface.
- When all the ADSL standards are turned off in the Advanced Settings and you can only connect using the VDSL2 standard, the VPI, the VCI and the encapsulation options still appear even though they are not used to open an Internet connection.

# Monitoring

This section applies to both IPv4 and IPv6 connections.

On the **Internet Connectivity** page, click **Connection monitoring...**

**Procedure**

The Monitoring Servers table shows the configured connections:

- **Connection** - Name. For example, Internet1.
- **Server Name**
- **IP address**
- **Packet Loss**
- **Failures**
- **Avg. Latency**

- **Min Latency**
- **Max Latency**
- **Jitter**

Probing provides information about the quality of an internet connection and what action to take if there is no connectivity. You can configure separate probing settings for each internet connection.

**To configure probing for an internet connection (pings):**

1. In the **Internet Connectivity** page, select a connection and click **Connection Monitoring**.

   The **Edit Internet Connection** window opens.

2. In the **Connection Monitoring** tab, select **Monitor connection state by sending probe packets to one or more servers on the Internet**.

   Select this option to use more methods and servers to detect connectivity loss.

   ⓘ **Important** - In versions R81.10.10 and higher, it is supported to disable probing in an Internet connection only if you clear the option, "This Internet connection will be a part of SD-WAN" (on the "Advanced" tab > section "SD-WAN Settings").

3. For **Connection probing method**, select **ping addresses**.

4. Under **Advanced Probing Settings**, use the default values or enter new ones for:

   - **Recovery time** (in seconds)
   - **Max latency allowed** (milliseconds)
   - **Probing frequency** (seconds)
   - **Window size** (pings)
   - **Failover pings** (percent failures)

5. Click **Apply**.

**To monitor a connection by DNS probe:**

1. In the **Connection Monitoring** tab, select **Monitor connection state by sending probe packets to one of more servers on the Internet**.

   **Important** - In versions R81.10.10 and higher, it is supported to disable probing in an Internet connection only if you clear the option, "This Internet connection will be a part of SD-WAN" (on the "Advanced" tab > section "SD-WAN Settings").

2. For **Connection probing method**, select **DNS probe**.
3. Click **Apply**.

**To monitor Cellular connections (internal LTE modem):**

Click the **Monitor cellular modem** link to see this information in the **Cellular Modem Monitoring** window:

- Cellular radio
- Cellular modem
- Operator
- SIM cards - Which SIM is active, primary or disabled.

# Configuring the Wireless Network

The **Device** view > **Network** section > **Wireless** page shows the wireless network settings (if applicable). 802.1x is supported.

You can configure your main wireless network and also additional guest or standard wireless networks (VAPs - Virtual Access Points).

- **Guest** wireless network - Uses hotspot by default and is unprotected by default (no password required).
- **Standard** wireless network - A protected wireless network that requires a password and does not use a hotspot by default.

To delete the wireless network, go to **Device** > **Local Network**.

If multiple wireless networks (VAPs) are defined, they appear in a table below **2.4 GHz Radio band** and **5GHz Radio band**.

**1530 / 1550 appliances only**: The wireless client search options depend on the frequency that the appliance is set to. The Quantum Spark Appliance can be configured to only one frequency at a time and is set to 2.4 GHz by default. If you change the radio settings to 802.11 ac or 802.11 ac/n, the frequency automatically changes to 5 GHz. The **Home** > **System** page shows the wireless radio status.

**1570 / 1590 appliances only**: There are two radio transmitters: 2.4 GHz and 5 GHz. Each network is configured separately under a specified transmitter.

You can add a new guest or standard wireless network and edit, delete, or disable existing ones. You can also clone an existing VAP.

### To enable or disable the Wireless network:

- Move the slider to select the **ON** or **OFF** option. If you configured multiple VAPs, selecting **Off** turns them all off.

  **Note** - If you turn off the wireless radio and then turn it back on, the VAPs remain disabled. To enable the VAPs, you must select the relevant entries in the table and click **Enable**.

- To disable or enable the Wireless network, click **Disable/Enable**.

### To configure a new wireless network or edit an existing network:

1. Select the **Radio band** (**4GHz** or **5GHz**) and make sure the slider button is turned to **ON**.
2. For a new network, click **Configure**.

   The **New Wireless Network** window opens in the **Configuration** tab.
3. For an existing network, click **Edit Settings**.

The **Edit Wireless Network** window opens in the **Configuration** tab.

4. Enter the **Network name (SSID)**.

   Example: Guest1 or VAP 1. If you are editing an existing network, the name is already present in the field.

5. Select to **Enable network**, or **Use hotspot when connecting to network** to redirect users to the Hotspot portal before you allow access from this interface.

   Hotspot configuration is defined in the **Device** > **Network** section > **Hotspot** page.

6. Select the **Wireless radio transmitter** from the pull-down menu.

7. In the **Wireless Security** section, select one of these:

   - **Protected network (recommended)**.

     a. If you select this option, select these values from the pull-down menus:

        - **Security type**.
        - **Encryption type**.
        - **Authenticate using** - **Password** or **RADIUS server (Enterprise mode)**.

          **Note** - The **RADIUS servers (Enterprise mode)** option requires defining RADIUS servers in the **Users & Objects** view > **User Management** section > **Authentication Servers** page. Each user that tries to connect to the wireless network is authenticated through the RADIUS server. This option is also known as **WPA Enterprise**. The 802.1x standard is used when WiFi Authentication is set to RADIUS Server (Enterprise Mode).

        **Optional:** Click **Show** to show the password

     b. Enter the **Network password** or click **Generate**.

   - **Unprotected network (not recommended)**.

     If you select this option, every wireless client can connect to this network. Transferred data is not encrypted.

8. In the **Advanced Settings** section (click the arrow to expand), select the options you want:

   - **Hide the Network Name (SSID)** - When selected, this wireless network name is not automatically shown to users scanning for them. Connecting to the wireless network can be done manually by adding the specified network name.

- **Allow Station-to-Station traffic** - When selected, allows wireless stations on this network to communicate with each other. When cleared, traffic between wireless stations is blocked.
- **Enable MAC address filtering**. If you select his option, you must enter the MAC addresses that are allowed to access the wireless network.

9. Click **Apply**

# Dynamic Frequency Selection (DFS)

**Note** - This is only in specific appliances that support WiFi6.

DFS detects radar signals that must be protected against interference from 5.0 GHz (802.11ac/n) radios. When these signals are detected, the operating frequency of the 5.0 GHz (802.11ac/n) radio switches to one that does not interfere with the radar systems. DFS is enabled by default.

802.1x (a/n/ac/ax) is supported. The advantage of WiFi6 (802.11ax) is that it improves the throughput-per-area in high-density scenarios such as corporate offices, shopping malls, and dense residential areas.

For configuration, see below.

# Cloning a VAP

You cannot edit or change the main wireless network, or if you have only a single VAP. However, if you clone your VAP, you can edit the clone.

### To clone a VAP:

Select the relevant VAP and click **Clone**.

When you clone a VAP, it receives a new name which is displayed in the table. The IP address and range of the clone is different than the original.

### To edit a VAP:

1. Double click the relevant VAP or select the VAP name and click **Edit**.

   The **Edit** window opens.

   **Note** - The wireless radio transmitter is the main VAP.

2. In the **Configuration** tab, select the **Wireless Security**:

- **Protected network** (recommended) - Enter the relevant information in the fields.
- **Unprotected network** (not recommended)

3. In the **Advanced Settings** section (click the arrow to expand), select the options you want:
   - **Hide the Network Name (SSID)** - When selected, this wireless network name is not automatically shown to users scanning for them. Connecting to the wireless network can be done manually by adding the specified network name.
   - **Allow Station-to-Station traffic** - When selected, allows wireless stations on this network to communicate with each other. When cleared, traffic between wireless stations is blocked.
   - **Enable MAC address filtering**. If you select his option, you must enter the MAC addresses that are allowed to access the wireless network.
4. Click **Apply**

## Additional Configurations

**To change the Wireless Network password:**

1. Click **Password Protected**.

   The Change Wireless Network Password window opens.
2. Select the **Security** type from pull-down menu.
3. **Authenticate using**: Select **Password** or **RADIUS server** from the pull-down menu.
4. For **Password** - Enter a new password (if want to change).

   **Optional:** Click **Show** to show the characters.
5. Select if you want to **Allow access from this network to local networks (wireless network is trusted)**.
6. Click **Apply**

**To configure the wireless radio settings:**

1. For these fields, select options from the pull-down menu:
   - **Operation mode**
   - **Channel width**
   - **Channel**
   - **Transmitter power**
2. In the **Advanced** section, select the **Guard Interval** from the pull-down menu.

3. **For DFS**

   With DFS, an unlicensed device can use 5HGz frequency bands already allocated to radar systems without causing interference. The device detects the presence of a radar system on the channel and if the radar level is above a specific threshold, it vacates that channel and selects an alternate channel.

   a. For **Operation mode**, select 802.11a/n/ac/ax (5GHz).

   b. Select **Enable DFS** - When using an automatic channel, this allows the ACS (Automatic Channel Selection) to select channels that overlap with radar frequencies.

      **Note** - It may take a minute for the wireless radio to start transmitting due to regulation requirements when using channels that overlap with radar frequencies.

   c. Select **Enable Zero-Wait DFS** - This allows the wireless module to use a non-DFS channel while scanning channels that overlap with radar frequencies and build a list of "vacant" channels (channels where radar is not detected). When this list is ready, the wireless module may instantly switch to a non DFS channel without turning off the wireless transmission.

      **Note** - If you select the 160MHz channel width, make sure to disable the **Enable Zero-Wait DFS** feature. Otherwise, due to regulatory constraints, it may take at least 1 hour before the wireless module starts to transmit in 160MHz channel width.

4. Click **Apply**

Depending on your configuration, you may see other tabs and sections to configure:

**Wireless Network Tab**

- **Interface Connection**

  **Assigned to** - Select **Separate network** or one of the existing configured networks.

  When selecting a separate network configure this information:

  - **IP address** - IPv4 and IPv6 addresses
  - **Subnet mask** - for IPv4 addresses
  - **Prefix length** - for IPv6 addresses

- **DHCPv4 Server**

  Select one of the options:

    - **Enabled** - Enter the **IP address range** and if necessary the **IP address exclude range**.

      The appliance's own IP address is automatically excluded from this range

      You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects** view > **Network Resources** section > **Network Objects** page.

      Reserving specific IP addresses requires the MAC address of the device.

    - **Relay** - Enter the DHCP server IP address.

    - **Disabled**.

- **IPv6 Auto Assignment**

  Select one of the options:

    - **SLAAC (Stateless Address Autoconfiguration)**

    - **DHCPv6 Server** - Enter the IP address range and the IP addresses exclude range

    - **DHCPv6 Server Relay** - Enter the DHCPv6 server IP address and the Secondary DHCPv6 server IP address

### Access Policy tab

These options create automatic rules that are shown in the **Access Policy** > **Firewall** section > **Policy** page.

- **Allow access from this network to local networks (Wireless network is trusted)**

- **Log traffic from this network to local networks**

### Advanced tab

- Click the checkbox to exclude from DNS proxy.

- Advanced IPv6 settings

  Configure the Router advisement fields.

### DHCP/SLAAC Settings tab

**Note** - In IPv4-only mode, this tab is called **DHCPv4 Settings**.

The values for the DHCP options configured on this tab will be distributed by the DHCP server to the DHCP clients.

- **DNS Server Settings (For DHCPv6/SLAAC)**

  Select one of these options:

  - **Auto** - Use the DNS configuration of the device
  - **Use the following IP addresses** - Enter the first, second and third DNS servers

- **DNS Server Settings (For DHCPv4)**

  These settings are effective only if a DHCPv4 server is enabled.

  - **Auto** - Use the DNS configuration of the device
  - **Use the following IP addresses** - Enter the first, second and third DNS servers

- **Default Gateway**

  Select one of these options:

  - **Use this gateway's IP address as the default gateway.**
  - **Use the following IP address** - Enter an IP address to use as the default gateway.

- **WINS**

  Select one of these options:

  - **Use the WINS servers configured for the internet connection**
  - **Use the following WINS servers** - Enter the IP addresses of the **First** and **Second** WINS servers.

- **Lease**

  **Lease time** - Configure the timeout in hours for a single device to retain a dynamically acquired IP address.

- **Other Settings**

  You can optionally configure these additional parameters so they will be distributed to DHCP clients:

  - **Time servers**
  - **Call manager**
  - **TFTP server**
  - **TFTP boot file**
  - **X Window display manager**

- **Avaya IP phone**
- **Nortel IP phone**
- **Thomson IP phone**

- **Custom Options**

  Lets you add custom options that are not listed above.

  For each custom option, you must configure the name, tag, type, and data fields.

  When you finish editing the network, click **Apply**.

# Wireless Scheduler

You can set scheduled times for the WiFi to be on and off and differentiate between radio bands (2.4GHz and 5GHz).

**Use Case:** Configure the WiFi to work only during normal business hours and be off on weekends when the business is closed.

**To enable the wireless scheduler:**

1. In the **Wireless** page, click **Radio Settings**.

   The **Wireless Radio Edit** window opens.

2. Go to the **Scheduler** tab.
3. Move the slider to **ON** to enable the wireless scheduler.

**To add new schedule settings:**

1. In the **Wireless Radio Edit** window, click **New**.
2. Under **Choose Days**, select the specific days.
3. Click **Apply**

# Wi-Fi Quality Analyzer

## Background

The Wi-Fi Quality Analyzer detects the Wi-Fi networks near the appliance and shows the report with this information:

- Level of interference from other Wi-Fi networks on the current Wi-Fi channel.
- Signal level for the Wi-Fi clients connected to this appliance.

## Procedure

1. Connect to the command line on the Quantum Spark appliance.
2. Log in to the Expert mode.
3. Run the Wi-Fi Quality Analyzer:

   ```
   wifi_quality
   ```

## Example Output

```
WiFi Quality Report
===================
Appliance is using channel 11
The WiFi setup in terms of interference from neighbour APs is very
good (grade = 2.5). Even the strongest interferer of all APs -
ExampleWiFi, accounting for 74 percent of potential interference
has a relatively low rssi (= 24).
Wifi Setup Grades:
below 2.5 - excellent
2.5 - 3.0 - very good
3.0 - 3.5 - good
3.5 - 5.0 - not so good
5.0 - 6.5 - not good
above 6.5 - terrible
As for individual clients, they can experience quality issues if
their signal is too small, or they don't maintain a line of sight
with the appliance or they are just too remote. Please consult the
following table regarding the individual clients connected to the
appliance
ExampleClient1        :    mac=XX:XX:XX:XX:XX:XX: rssi = 55, very
good quality
ExampleClient2        :    mac=XX:XX:XX:XX:XX:XX: rssi = 21, good
quality
```

# Configuring the Local Network

The **Device** view > **Network** section > **Local Network** page lets you set and enable the local network connections, switches, bridge or wireless network (on wireless devices only).

A bridge connects two or more local area networks (LANs). A switch is similar to a bridge but can perform data transmission between multiple port pairs at the same time.

**Note** - You can only configure a bridge between two unassigned interfaces.

The **Network** table shows all available network connections.

The page also lets you:

- Configure multiple **switches** (port based VLANs) between the available local LAN interfaces and wireless networks. You can create tag-based VLANs under separate LAN ports and DMZ or under a LAN switch. Traffic is not monitored or inspected between the LAN ports of a switch.
- Configure multiple **bridges** between interfaces. Traffic in a bridge is always monitored and inspected by the appliance.
- Create and configure tag based **VLANs** (802.1q) on any of the LAN interfaces or DMZ.

  **Note** - DMZ is not supported in 1530 / 1550 appliances.

- Create an **alias IP**. With an alias IP, you can associate more than one IP address to a network interface. A single network device can have multiple connections to a network.
- Create and configure **VPN tunnels (VTI)** which can be used to create routing rules which determine which traffic is routed through the tunnel and therefore also encrypted (Route based VPN).
- Create a **BOND** (Link Aggregation) between two or more interfaces. This improves performance and redundancy by increasing the network throughput and bandwidth. The LAN Bond can be an unassigned network.
- On wireless devices - Add new **wireless networks** (**Virtual Access Points**). This can also be done through the **Device** > **Wireless** page.

  There are two radio transmitters: 2.4 GHz and 5 GHz. Each network is configured separately under a specified transmitter.

You can also use unassigned LAN ports to create an internet connection. In the table, these ports have the status **Assigned to Internet**.

**Notes:**

- LAN ports assigned to internet connections can only be disabled from the **Internet** page.
- You cannot edit a LAN port assigned to an internet connection. When you click **Edit**, the window opens, but when you click **Apply**, a warning shows that this deletes the connection.
- When you create a bridge or switch surface, these LAN ports do not appear in the selection box as optional ports.
- You cannot disable one of the switch ports. You can disable the switch or configure the requested port as unassigned.

### To create any of the above options:

Click **New** and select the option you want.

### To edit/delete/enable/disable any of the above options:

Select the relevant row and click **Edit/Delete/Enable/Disable**.

**Notes:**

- Physical interfaces cannot be deleted.
- Editing an interface that is part of a switch or a bridge lets you remove it from the switch or bridge.
- When a LAN or DMZ interface is part of an Internet connection, it is still visible on this page, but can be only be configured through the **Device** > **Internet** page.
- You must enable IPv6 in the **System Operations** tab.

For each network, the table on this page shows you:

- **Name** - Name of the network, interfaces that participate (if there are multiple interfaces), and a description (optional)
- **Local IPv4 Address**
- **Subnet Mask** - IPv4 addresses only
- **MAC Address**
- **Status** - Shows a status for physical interfaces and wireless networks:
  - **Physical interfaces** - Shows cable connection status of each physical interface that is enabled. Otherwise, it shows disabled.
  - **Wireless networks** - Shows if the wireless network is up or disabled.

# Reserved IP Address for Specific MAC

You can configure your network so that IP addresses are assigned only for known hosts. Known hosts are already defined as network objects and a specific MAC address is assigned to the IP. Other hosts' DHCP requests are ignored.

**To configure:**

1. Select the specific LAN name and click **Edit** or double-click the **LAN** name.

   The **Edit LAN** window opens.
2. In the **Configuration** tab, click **Enabled** under **DHCPv4 Server**.
3. In the **DHCPv4 Settings** tab, enter the DHCP domain name and click the checkbox for **Assign IP addresses for known host only**.
4. Click **Apply**

# Switch

A LAN Switch is a group of LAN ports (for example, LAN2, LAN3, LAN5) that are grouped together and represented by the "pivot" port (the port with lowest index, LAN2 in this example).

**Note** - Between the LAN ports of a switch, traffic is not monitored or inspected.

**To create/edit a switch configure the fields in the tabs:**

**The 'Configuration' tab**

1. In **Switch Configuration**, select or clear the interfaces you want to be part of the switch. The table shows you which interfaces are already part of the switch (shown with checkmarks in the table) and which interfaces are not assigned yet and can be added to the switch (empty checkboxes in the table). For example, if LAN8 is already part of another switch, it does not show in this table.
2. From **Assigned to**, select an option:
   - **Unassigned** - The switch is not part of any network and cannot be used
   - **Separate network** - When you select a separate network, configure the settings for the switch
   - **Monitor Mode** - See *"Monitor Mode on Quantum Spark Gateways" on page 129*
3. Choose the **IP address** and **Subnet mask** the switch uses.
4. **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface.

You define the Hotspot configuration in the **Device** > **Hotspot** page.

5. In **DHCPv4 Server**:

   Select one of the options:

   - **Enabled** - Enter the **IP address range** and if necessary the **IP address exclude range**. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specified IP addresses if you define network objects in the **Users & Objects** > **Network Objects** page. To reserve specified IP addresses, you must have the device MAC address.
   - **Relay** - Enter the DHCP server IP address. You can also enter a Secondary, Tertiary, and Quaternary DHCP server IP address.
   - **Disabled**

**IPv6 Auto Assignment for IPv6 configurations**

- **SLAAC (Stateless Address Autoconfiguration)** - The host selects its own full IPv6 address after it receives the IPv6 address prefix from the gateway. The appliance cannot reserve an IPv6 address for a specific host (Mac Address).

  **Note** - The common use case is a prefix length of 64. If you change it from 64, make sure the internal hosts support the new length.

- **DHCPv6 Server** - Same as the DHCPv4. You can reserve an IP address for a specified host.
- **DHCPv6 Server Relay** - Same as in IPv4.
- **Disabled (Static)**

# WAN as LAN

In the appliance, the two SFP ports are associated with DMZ and WAN. DMZ can already be used for an internal-network, but WAN is reserved for internet-connections.

With this feature, you can use the WAN port, usually reserved for internet (external) connections, for LAN (internal) connections. Some users prefer using SFP (fiber) for internal-networks (LAN), as it is more reliable in an environment with high electrical power.

When assigned to a LAN, the WAN port can be used for any type of internal network except for a BOND network. The WAN port (like the DMZ port), can only be used for a BOND network as part of an internet (external) network.

The WAN as LAN feature is disabled by default.

**To enable WAN as LAN:**

1. Go to **Device** > **Advanced Settings** and select **OS advanced settings - Enable LAN on WAN**.
2. Click **Edit** to change the value to `true`.

The **Device** > **Local Network** page now shows WAN ports included in the list of LAN and DMZ (local interfaces, switches, bridges, bonds and VLANs).

- When used for **WAN** networks, the interface name of the WAN port is **WAN**.
- When used for **LAN** networks, the interface name of the WAN port is **LANW**.

**Note** - The WAN as LAN feature is the only supported solution for users who want to connect to the Internet using LAN ports. Make sure the interface is configured correctly.

Configuration parameters for WAN as LAN are similar to DMZ.

# Monitor Mode on Quantum Spark Gateways

Security Gateways can monitor traffic from a Mirror Port or Span Port on a switch.

With Monitor Mode, the appliance uses Automatic Learning or user-defined networks to identify internal and external traffic, and to enforce policy.

**Automatic Learning** - The appliance automatically recognizes external networks by identifying the default gateway's network from requests to the Internet (specifically, requests to Google). The rest of the networks are considered internal.

**User-Defined Networks** - You can manually define internal networks. If a network is not defined as internal, it is considered external.

In both Automatic Learning and user-defined networks:

- Traffic to internal hosts is inspected by the Incoming/Internal/VPN Rule Base.
- Traffic to external hosts is inspected by the Outgoing Rule Base.
- Threat prevention's default configuration is optimized to inspect suspicious traffic from external hosts to internal hosts.

**To configure monitor mode in the WebUI:**

1. Go to **Device** > **Local Network**.
2. Select an interface and double-click.

   The **Edit** window opens in the **Configuration** tab.
3. In the **Assigned To** drop-down menu, select **Monitor Mode**.

The **Manually define internal networks** checkbox shows.

4. To use Automatic Learning, do not select **Manually define internal networks** and click **Apply**.
5. To use your own network definitions, select **Manually define internal networks**.

   The network definition features and table show.
6. Click **New**.
7. Enter the network **IP address**.
8. Enter the **subnet**. An internal network can be a 255.255.255.255 subnet, for one host.

   For example, to monitor the traffic after the router, enter the IP address of the Default Gateway and the 255.255.255.255 subnet.
9. Click **Apply**

   The Internal network you defined (with Monitor Mode in the name) shows in the list of interfaces.

**Note** - You can configure multiple local networks to be in monitor mode at the same time.

### After you configure monitor mode:

1. Go to **Device** > **Advanced Settings**.
2. Turn off **Anti-Spoofing**.

### To configure monitor mode in Gaia Clish:

1. To define a port for Monitor Mode:

   ```
   set interface <Port Name> monitor-mode
   ```
2. To configure Monitor Mode Automatic Learning, disable user-defined networks:

   ```
   set monitor-mode-configuration use-defined-networks false
   ```
3. To configure Monitor Mode with user-defined networks:

   ```
   add monitor-mode-network ipv4-address <IP Address> subnet-mask
   <Mask>
   ```

   ```
   set monitor-mode-configuration use-defined-networks true
   ```
4. To see user-defined Internal networks:

   ```
   show monitor-mode-network
   ```

5. To disable Anti-Spoofing:

   ```
   set antispoofing advanced-settings global-activation false
   ```

### If you do not see the Monitor Mode option:

1. Run this command in Gaia Clish:

   ```
   set monitor-mode-configuration allow-monitor-mode true
   ```

2. Select an interface in WebUI and click **Edit**.

   Monitor Mode is now added to the options list.

For more information on monitor mode, see sk112572.

# Mirror Port

All traffic that goes through one or more LAN ports of the appliance can be duplicated into one designated mirror port. For example, all traffic that passes through LAN1 and LAN2 is duplicated into LAN5, which is configured as the mirror port. You can only configure one mirror port at a time.

**Use Case** - If an external device is connected to the mirror port, it receives all traffic that goes through LAN1/LAN2 of the appliance. This enables you to monitor traffic that goes through the appliance from the external device.

The mirror port is the opposite of the existing monitor port feature, in which the traffic from an external source such as a network switch or router goes into the (WAN) port of the appliance, so the appliance can inspect the traffic going through the external source.

### To configure a mirror port:

To configure a mirror port:

1. In the **Device** > **Local Network** page, select the designated mirror port and unassign it:
   a. Click **Edit**.

      The **Edit LAN** window opens.

   b. In the **Configuration** tab, in the **Assigned to** field, select **Unassigned**.
   c. Click **Apply**
2. In the Local Network table, select the LAN port you want to duplicate and click **Edit**.

   The **Edit LAN** window opens.

3. In the **Port Mirroring** section of the **Advanced** tab, select the checkbox **Assign to mirror port**.
4. In the **Port** field, select the mirror port from the drop-down menu.

5. Click **Apply**.
6. In the Local Network table, right-click the mirror port and click **Enable**.
7. Repeat for each LAN port you want to duplicate in the mirror port.

# Physical Interfaces

### To edit a physical interface:

Configure the fields in the tabs. Note that for the DMZ there is an additional tab **Access Policy**:

**The 'Configuration' tab**

**Assigned to** - Select the required option:

- **Unassigned** - The physical interface is not part of any network and cannot be used.
- One of the existing configured **switches** or **bridges**
- **Separate network** - When selecting a separate network configure this information:
  - **IP address**
  - **Subnet mask**
  - DHCP Server settings

    Select one of the options:

    **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects** > **Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.

    **Relay** - Enter the DHCP server IP address.

    **Disabled**

**Note** - When you create a switch, you cannot remove the first interface inside unless you delete the switch.

### The 'Advanced' tab

The options that are shown vary based on interface type and status. Configure the options that are applicable:

- **Description** - Enter an optional description. The description is shown in the local network table next to the name.
- **MTU size** - Configure the Maximum Transmission Unit size for an interface. Note that in the Quantum Spark Appliance, the value is global for all physical LAN and DMZ ports.
- **Disable auto negotiation** - Select this option to configure manually the link speed of the interface.
- **Override default MAC address** – This option is for local networks except those on VLANs and wireless networks. Use this option to override the default MAC address of the network's interface:
    - When the device has two separate local networks connected to the same external switch.
    - If the ISP is searching for the gateway MAC address to accept the connection. If you upgrade your new gateway, the ISP may block it because the new gateway has a different MAC address. In this case, you can override the gateway MAC address with the old one.

  **Best Practice** - This is a rare configuration. Do not select this option unless you are sure you need it.
- **Exclude from DNS proxy** – Select this checkbox for any network that you do not want exposed to internal domains. In guest VAPs (wireless network for guests), this is selected by default.

### The 'Access Policy' tab (only for DMZ)

These options create automatic rules that are shown in the **Access Policy** > **Firewall Policy** page.

- **Allow access from this network to local networks**
- **Log traffic from this network to local networks**

# Bridge

**Note** - Bridge interface supports only two subordinate interfaces.
If you add three or more subordinate interface, then the appliance drops the traffic through this Bridge interface with the message "IP routing failed (bridge routing failure)".

To create a bridged internet connection in a cluster, see the **Configuring Internet Connectivity** page > *"Bridged Internet Connection in a Cluster" on page 98* section.

### To create/edit a bridge, configure the fields in the tabs:

**The 'Configuration' tab**

- In **Bridge Configuration**, select the networks you want to be part of the bridge.
- **Enable Spanning Tree Protocol** - When Spanning Tree Protocol (STP - IEEE 802.1d) is enabled, each bridge communicates with its neighboring bridges or switches to discover how they are interconnected. This information is then used to eliminate loops, while providing optimal routing of packets. STP also uses this information to provide fault tolerance, by re-computing the topology in the event that a bridge or a network link fails.
- Enter a **Name** for the bridge interface. Note that you can only enter "brN" where N is a number between 0 and 9. For example, br2.
- Select the **IP address** and **Subnet mask**.
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device** > **Hotspot** page.
- **DHCP Server**

  Select one of the options:

  - **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects** > **Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
  - **Relay** - Enter the DHCP server IP address.
  - **Disabled**

### The 'Advanced' tab

- **MTU size** - Configure the Maximum Transmission Unit size for an interface.
- **Disable auto negotiation** - Select this option to configure manually the link speed of the interface.
- **Override default MAC address** – This option is for local networks except those on VLANs and wireless networks. Use this option to override the default MAC address used by the network's interface, when the device has two separate local networks connected to the same external switch.

  **Best Practice** - This is a rare configuration. Do not select this option unless you are sure you need it.
- **Exclude from DNS proxy** – Select this checkbox for any network that you do not want exposed to internal domains. In guest VAPs (wireless network for guests), this is selected by default.

### To configure Advanced IPv6 settings:

1. Configure the **Router Advisement** fields.
2. Under **Prefix Delegation**, select the checkbox for **Enable prefix delegation** and enter the relevant information.

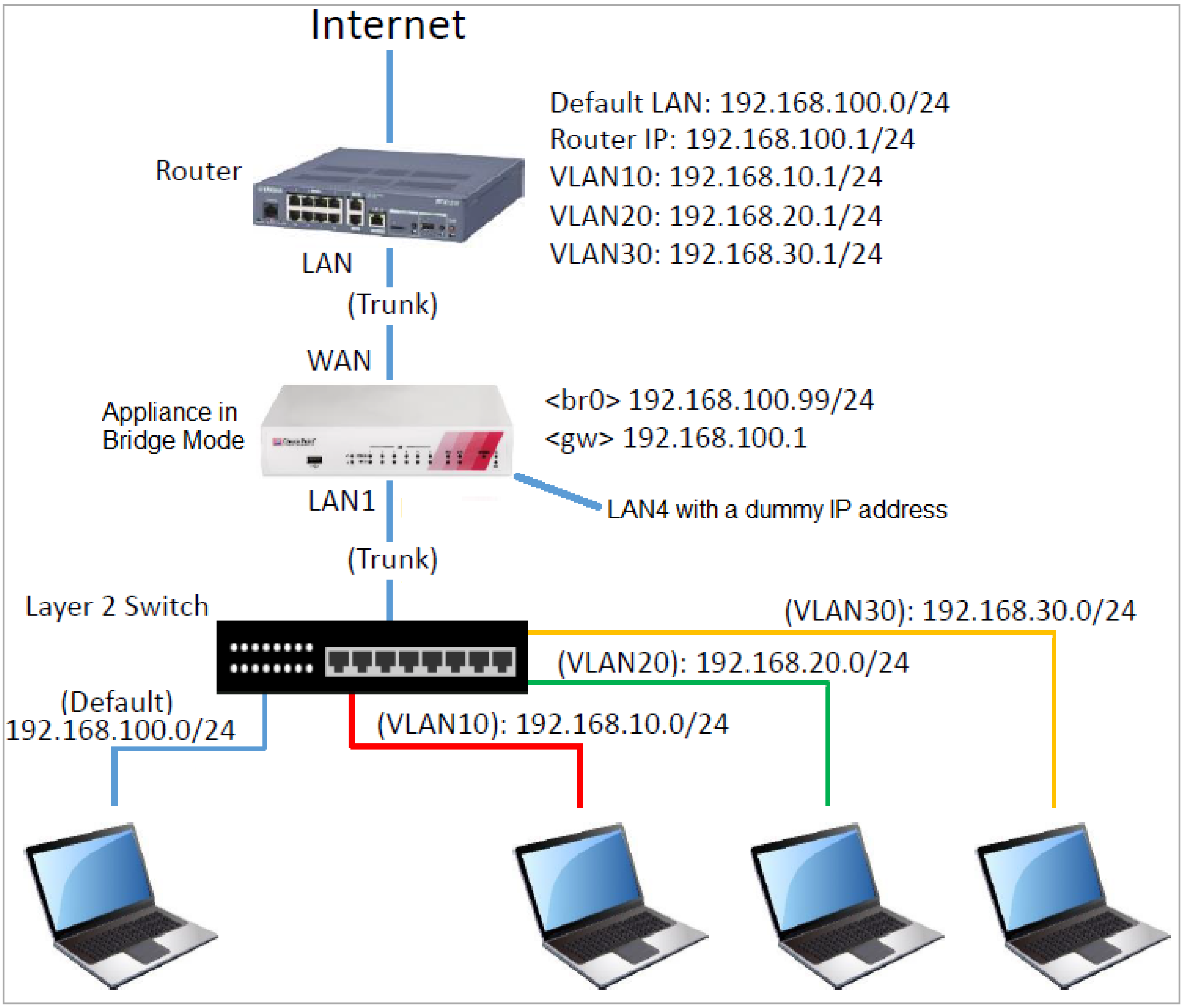
### To configure Application Control and URL Filtering on an appliance in the Bridge Mode that uses Tag-based VLANs

**Background:**

Logical topology before the change:

[SWITCH] --- VLAN Trunk --- (LAN) [Appliance in Bridge Mode] (WAN) --- VLAN Trunk --- [ROUTER]

Example physical topology after the change (configuring an interface with a dummy IP address):



**Configuration steps:**

1. Disconnect a cable from one of the available physical interfaces on the appliance (in our example, LAN4).
2. Assign a random IP address to this interface.

   This can by a dummy IP address that must not be used in your internal networks.
3. Go to the **Device** > **Advanced Settings** page. See *"Advanced Settings" on page 246*.
4. Search for **UserCheck Portal - Redirect Address**
5. Select this attribute.
6. Click **Edit**.
7. Enter the same IP address you assigned to the dedicated interface (in our example, LAN4).
8. Click **Apply**

# VLANs

### To create/edit a tag based VLAN:

You can create a new VLAN only if you have at least one physical interface that is not part of an existing network (switch or bridge). For more information on the maximum number of VLANs that you can configure for each appliance, refer to *sk113247*

**Note** - Quantum Spark Appliances (1500-2000 series) support management traffic over VLAN interfaces when centrally managed in R81.10.X. environments.

Configure the fields in the tabs:

### The 'Configuration' tab

- **VLAN ID** - Enter a number that is the virtual identifier.
- **Assigned to** - Select the physical interface where the new virtual network is created.
- **IP address**
- **Subnet mask**
- **Cluster status** - Starting from R81.10.15, you can configure the cluster status of the LAN connection, including the Cluster IP and Peer IP. If the interface is assigned to a separate network, you can select between **Monitored** or **non-HA**. Select **High Availability** to add the interface to a cluster.
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface.

  You define the Hotspot configuration in the **Device** > **Hotspot** page.
- **DHCP Server settings**

  Select one of the options:

  - **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects** > **Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
  - **Relay** - Enter the DHCP server IP address.
  - **Disabled**

# Alias IP

With an alias IP, you can associate more than one IP address to a network interface.

- A single network device can have multiple connections to a network.
- A specific port is used by more than one network.

All devices are on the same network, even though they show different IPs. For example, LAN4 and LAN4:1 have different IP addresses, but are on the same network. LAN4:1 is the alias.

You can also have an alias IP for VLAN and a switch.

### Use Case

A customer is migrating his device to a new subnet, but wants the host to still be able to "approach" a resource such as a printer on his old subnet during the transition period.

### To configure an alias IP for WAN:

1. Go to the **Internet Connection** page.
2. Configure another static IP type connection on the same Internet port.

   Example: WAN and WAN:1 (WAN:1 is the alias IP).

### To create an alias IP (LAN):

1. On the **Local Network** page, select **New** > **Alias**.

   The New Alias window opens.
2. Select the Local network port.
3. Add IP address
4. Add subnet mask
5. Click **Apply**

You can configure a total of 64 aliases for a LAN connection.

Alias IP is not supported on a bridge interface. You can only assign an alias IP to a separate network LAN or switch. If you remove or disable the LAN, any assigned alias IPs are also removed.

When you edit an alias IP, you cannot change the port or the ID.

To create an Alias IP on WAN, you must create an additional internet connection on the same WAN interface. See *"Configuring Internet Connectivity" on page 87*.

# VPN Tunnel (VTI)

### To create/edit a VPN Tunnel (VTI):

A Virtual Tunnel Interface (VTI) is a virtual interface on a Security Gateway that is related to an existing, Route Based VPN tunnel. The Route Based VPN tunnel works as a point-to-point connection between two peer Security Gateways in a VPN community. Each peer Security Gateway has one VTI that connects to the tunnel.

The VPN tunnel and its properties are defined by the VPN community that contains the two gateways. You must define the VPN community and its member Security Gateways before you can create a VTI.

### Configure the fields in the tabs:

### The 'Configuration' tab

- **VPN Tunnel ID** - A number identifying the VTI.
- **Peer** - The name of the remote VPN site. See *"Configuring VPN Sites" on page 407*.

  The VPN tunnel interface can be numbered or unnumbered. Select the applicable option:
- **Numbered VTI** - You configure a local and remote IP address for a numbered VTI:
  - **Local IPv4 address** - The IP address to be used for the local point-to-point virtual interface.
  - **Remote IP address** - The IP address to be used at the peer gateway's point-to-point virtual interface.
- **Unnumbered VTI** - When the VTI is unnumbered, it is not necessary to configure local and remote IP addresses. You define a local interface to use as the source IP address for outbound traffic.
  - **Internet connection** - Select from the list.
  - **Local bridge interface** - Select the local interface from the list.

# Virtual Access Point (VAP)

### To create/edit a Virtual Access Point (VAP):

See the **Device** > **Wireless Network** help page.

### The 'DHCP/SLAAC Settings' tab

**Note** - In IPv4-only mode, this tab is called **DHCPv4 Settings**.

The values for the DHCP options configured on this tab will be distributed by the DHCP server to the DHCP clients.

*DNS Server Settings (For DHCPv6/SLAAC)*

Select one of these options:

- **Auto** - Use the DNS configuration of the device.
- **Use the following IP addresses** - Enter the first, second and third DNS servers.

*DNS Server Settings (For DHCPv4)*

These settings are effective only if a DHCPv4 server is enabled.

Select one of these options:

- **Auto** - This uses the DNS configuration of the appliance as configured in the **Device** > **DNS** and **Device** > **Internet** pages.
- **Use the following IP addresses** - Enter the IP addresses for the **First DNS server**, **Second DNS server**, and **Third DNS server**.

*Default Gateway*

Select one of these options:

- **Use this gateway's IP address as the default gateway**
- **Use the following IP address** - Enter an IP address to use as the default gateway.

*WINS*

Select one of these options:

- **Use the WINS servers configured for the internet connection**
- **Use the following WINS servers** - Enter the IP addresses of the **First** and **Second** WINS servers.

*Lease section*

**Lease time** - Configure the timeout in hours for a single device to retain a dynamically acquired IP address.

*Other Settings*

You can optionally configure these additional parameters so they will be distributed to DHCP clients:

- **Time servers**
- **Call manager**
- **TFTP server**
- **TFTP boot file**
- **X Window display manager**
- **Avaya IP phone**
- **Nortel IP phone**
- **Thomson IP phone**

*Custom Options*

Lets you add custom options that are not listed above. For each custom option, you must configure the name, tag, type, and data fields.

# GRE

Starting from R81.10.07, you can create a GRE (Generic Routing Encapsulation) tunnel as a LAN interface connected with a remote peer and route all traffic between the two sites.

Each site has its own routable physical IP address. The GRE tunnel is created on top of a physical network interface, and each tunnel side is assigned a tunnel IP address which is different than the physical IP address.

**Notes**:

- Because the GRE tunnel connects two remote sites over the internet, Quantum Spark appliances must support such interfaces.
- Do not create the GRE tunnel over LAN.
- Starting from R81.10.15, GRE interfaces support OSPF.

**To create a GRE tunnel:**

1. In the WebUI, go to **Device** > **Local Network** and click **New**.
2. From the drop-down menu, select **GRE**.

   The **New GRE** window opens in the **Configuration** tab.
3. Enter the applicable information for the **GRE Settings** fields:

**GRE IPv4 Interface Address Settings section:**

- **IP address** - The IP address on a local interface (physical).
- **Peer address** - The IP address of the remote peer (physical).

**Interface Settings:**

- **GRE tunnel ID** - The ID is used as part of the GRE interface name. For example, if the ID is "4", the interface name is "gre4"
- **TTL** - Time to Live in seconds. The value is usually 255.

**Source Address and Remote Gateway Address:**

- **Local address** - The IP address assigned to the GRE interface (virtual).
- **Remote address** - The IP address of the peer on the GRE interface (virtual).

4. Click **Apply**.

# BOND

Bonding, also known as Link Aggregation, is a process that joins two or more interfaces together. It improves performance and redundancy by increasing the network throughput and bandwidth. Like other other LAN interfaces, the LANBOND can be an unassigned network or a cluster interface. Starting from R81.10.15, you can configure High Availability settings from this page.

### Use Case

Link Aggregation binds two or more physical ports together to form a LAG (Link Aggregation Group) bundle that results in higher bandwidth and link redundancy. If one link in the group fails, traffic is automatically routed through the remaining interfaces.

### To create a BOND (LAN):

1. In the **Local Network** page, click **New** and select **BOND (Link Aggregation)**.

   The **New BOND** window opens.

2. In the **Configuration** tab, under **BOND configuration**, select a minimum of 2 LANs that are unassigned and disabled.

   **Note** - You cannot select LAN interfaces that have a VLAN assigned to them.

3. Select the **Operation** mode:

- **802.3ad** - Dynamically uses Active interfaces to share the traffic load.

  Traffic is assigned to Active interfaces based on the transmit hash policy (**Layer2** or **Layer3+4**).
- **Round Robin** - Selects the Active interface sequentially.
- **XOR** - All interfaces are Active for Load Sharing.

  Traffic is assigned to Active interfaces based on the transmit hash policy (**Layer2** or **Layer3+4**).
- **High Availability (Active/Backup)** - Provides redundancy when there is an interface or link failure.

  If you select this mode, you must select a **Master** - the primary/default port for the traffic.

4. Under **Interface Configuration**:
   a. Select the **interface**.
   b. Enter the **Local IPv4 address** and **Subnet mask**.
   c. **Cluster status** - Starting from R81.10.15, you can configure the cluster status of the LAN connection, including the Cluster IP and Peer IP. If the interface is assigned to a separate network, you can select between **Monitored** or **non-HA**. Select **High Availability** to add the interface to a cluster.
   d. Select if you want to **Use hotspot when connecting to network**.
5. For **DHCPv4**, click **Enabled**.
6. In the **Advanced** tab, select the **Mii interval**.

   This interval is the frequency (in milliseconds) that the system polls the Media Independent Interface (MII), the standard interface for fast Ethernet) to get status.
7. If you selected **802.3ad** or **XOR** as your operation mode, select the **Hash policy** from the dropdown menu (**Layer2** or **Layer3+4**).
8. Click **Apply**

To create a WAN BOND, see *"Configuring Internet Connectivity" on page 87*.

# Configuring a Hotspot

A hotspot is an area that offers a wireless local area network with Internet access, through a router connected to a link to an Internet service provider.

Hotspot is automatically activated in the system.

**To define a network interface for a Hotspot:**

1. Click **Configure in Local Network**.

   The **Local Network** window opens.
2. Select interface and click **Edit**.

   The **Edit <interface>** window opens.
3. Select **Use Hotspot**.
4. Click **Apply**

   Any user that browses from configured interfaces is redirected to the Check Point Hotspot portal.

After you define a network interface for the hotspot, you can configure:

- **Guest access** - A session is created for an IP address when a user accepts terms or authenticates in the Hotspot portal. The session expires after the configured timeout (240 minutes by default).
- **Customize the Hotspot portal appearance.**
  1. Click **Customize Hotspot portal**.
  2. For **Portal title** - Keep the default or enter a different title.
  3. For **Portal message** - Keep the default or enter a different message.
  4. For **Terms of use** - Select this checkbox to add an "I agree with the following terms and conditions" checkbox on the Hotspot portal page. Enter the terms and conditions text in the text box. When users click the "terms and conditions" link, this text shows.
  5. To customize a logo for all portals shown by the appliance (Hotspot and captive portal used by User Awareness), click **Upload**, browse to the logo file and click **Apply**. If necessary, click **Use Default** to revert to the default logo.
  6. Click **Apply**
- **Hotspot exceptions**

  Define specified IP addresses, IP ranges or networks to exclude from the Hotspot.
  1. Click **Manage Exceptions**.

     The **Manage Hotspot Network Objects Exceptions** window opens.
  2. Select the objects to add as exceptions.

3. The **Selected Network Objects** window shows the selected objects. To remove an object from the list, click the x next to it.
4. To filter the object list, enter the filter value. The list shows the objects that match the filter.
5. If necessary, click **New** to add new objects to the list. For information on how to create a new object, see the **Users &Objects** > **Network Objects** page.
6. Click **Apply**

   The added objects are excluded from the Hotspot.

# User Authentication

In the Access section of the page, you can configure if authentication is required and allow access to all users or to a specified user group (Active Directory, RADIUS or local).

**To require user authentication:**

1. Select the **Require Authentication** checkbox.
2. You can allow access to **All users** or to a **Specific user group**.
3. If you selected **Specific user group**, enter the group's name in the text box.
4. Click **Apply**

   Any user/user group that browses from configured interfaces is redirected to the Check Point Hotspot portal and must enter authentication credentials.

**To configure the session timeout:**

1. In **Session timeout**, enter the number of minutes that defines how long a user stays logged in to the session before it is ends.
2. Click **Apply**

**To prevent simultaneous login to the Hotspot portal:**

1. Go to **Device** > **Advanced Settings.**
2. Select **Hotspot**.
3. Click **Edit**.

   The **Hotspot** window opens.
4. Click the checkbox for **Prevent simultaneous login**.
5. Click **Apply**

   The same user cannot log in to the Hotspot portal from more than one computer at a time.

# Disabling the Hotspot

1. Go to **Device** > **Advanced Settings**.
2. Search for Hotspot and double-click the entry.
3. Select **Disabled.**
4. Click **Apply**

On the **Active Devices** page (available from the **Home** and **Logs & Monitoring** tabs), you can revoke Hotspot access for connected users.

# Configuring MAC Filtering

MAC Filtering lets you manage an allowlist of MAC addresses that can access the LAN. All others are blocked. The list is global for all interfaces defined on physical LAN ports. Starting in R81.10.00, this feature is also supported in 1600 and 1800 appliances.

**Note** - There is separate MAC filtering on WiFi networks and on LAN ports, with DMZ and WAN excluded.

**To enable MAC filtering:**

1. Add a MAC address to the LAN MAC Filter allowlist.
2. Move the slider to **ON**.

After MAC filtering is enabled, you can disable the feature for specified networks.

**To edit the LAN MAC Filter allowlist:**

1. Go to **Device** > **MAC Filtering** > **LAN MAC Filter**.
2. To add a new MAC Address, click **Add** > **New**.
3. To select MAC addresses from the list of Active Devices, click **Add** > **Select**.
4. To edit a MAC address, select it from the list and click **Edit**.
5. To delete a MAC address, select it from the list and click **Delete**.

**To disable MAC filtering for a specific interface:**

1. Go to **Device** > **Local Network**.
2. Select a LAN interface and click **Edit**.

   The Edit LAN window opens.
3. Click **Advanced**.
4. Select **Disable MAC filtering**.

   To enable, clear this option.
5. Click **Apply**

**Note** - MAC filtering is not supported on external, DMZ, and port bonding interfaces.

# 802.1x Authentication Protocol

IEEE 802.1x is a port-based network access protocol that provides an authentication mechanism for devices that are physically attached to the network.

802.1x authentication can be enabled on LAN ports that are not part of port bonding, internet connections, or port mirroring.

**Workflow:**

1. Install and configure a RADIUS Server in your environment.
2. Configure the RADIUS Server object on the appliance. See *"Managing Authentication Servers" on page 448*.
3. Activate 802.1x authentication on a LAN switch, separate LAN interface or a tag-based VLAN interface defined on one of the LAN physical ports.
4. If 802.1x is turned on for a tag-based VLAN (because 802.1x is port-based), activate it on both the VLAN and the associated port (for example, LAN5 and LAN5.1).

### To enable 802.1x authentication on a LAN switch or interface:

1. Go to **Device** > **Local Network**.
2. Select the LAN interface and click **Edit**.

   The **Edit** window opens in the **Configuration** tab.
3. In the **Advanced** tab, select **Activate 802.1x authentication**.
4. Enter a time for **Re-authentication frequency (in seconds)**.
5. Click **Apply**

### To enable 802.1x authentication on a tag based VLAN interface:

1. Go to **Device** > **Local Network**.
2. Select the LAN and click **New** > **VLAN**.

   The **New VLAN** window opens in the **Configuration** tab.
3. For **Assigned to**: select the LAN ID.
4. In the **Advanced** tab, select **Activate 802.1x authentication**.
5. Enter a time for **Re-authentication frequency (in seconds)**.
6. Click **Apply**

**To disable 802.1x authentication on an interface:**

1. Go to **Device** > **Local Network**.

   Select the LAN interface and click **Edit**.

2. The **Edit** window opens in the **Configuration** tab.
3. Click the **Advanced** tab.
4. Clear **Activate 802.1x authentication**.
5. Click **Apply**

**To configure logging for MAC filtering and 802.1x authentication:**

1. Go to **Device** > **Advanced Settings**.
2. Set the value of the **MAC Filtering settings - Log blocked MAC addresses** attribute to
   - **Enabled** - To enable logging
   - **Disabled** - To disable logging.

   **Note** - This attribute is available only in Locally Managed mode. In Centrally Managed mode, configure logging with CLI.

3. **Optional** -
   - To reduce the number of logs, specify the value of the **MAC Filtering settings - Log suspension** attribute in seconds.
   - To show all logs, set the value to "0".

**Note** - Traffic dropped in the WiFi driver is not logged.

# Configuring the DNS Server

In the **Device** > **DNS** page you can configure the DNS server configuration and define the domain name.

## Configure DNS Servers

1. Select to define up to three DNS servers which is applied to all Internet connections or use the DNS configuration provided by the active Internet connection (Primary).

   If you select **Configure DNS servers**, make sure that you enter valid IP addresses.

   Use the first option if your DNS servers are located in the headquarters office. In this case, all DNS requests from this branch office are directed to these DNS servers.

   The second option allows a more dynamic definition of DNS servers. The gateway uses the DNS settings of the currently-active Internet connection (in case of static IP - the DNS manually provided under "Internet connection"-> Edit, in case of DHCP / Dialers - the DNS automatically provided by the ISP). If Internet Connection High Availability is enabled, the DNS servers switch automatically upon failover.

2. By default, the appliance functions as your DNS proxy and provides DNS resolving services to internal hosts behind it (network objects). This option is global and applies to all internal networks.

   To get IP addresses directly from the DNS servers defined above, clear the **Enable DNS Proxy** checkbox.

   When DNS proxy is enabled, **Resolve Network Objects** controls if the DNS proxy treats the local network objects as a **hosts list**. When selected, the local DNS servers resolves network object names to their IP addresses for internal network clients.

3. Enter a **Domain Name**. There are two separate uses of the domain name:

   - Local hosts (the Security Gateway and network objects) are optionally appended with the domain name when DNS resolving is performed.

   - DNS queries that do not contain a domain name are automatically appended with the domain name.

   **Note** - Syntax guidelines:
   - The domain name must start and end with an alphanumeric character.
   - The domain name can contain periods, hyphens, and alphanumeric characters.

4. Click **Apply**

## Forwarding the DNS requests from internal hosts to the configured DNS servers

### In versions R81.10.15 and higher

The default behavior is to forward the DNS requests only to the DNS servers configured in the Primary Internet connection.

Starting in this version, you can change the behavior to forward DNS requests to all configured DNS servers.

1. In WebUI, click the **Device** view.
2. In the **Advanced** section, click **Advanced Settings**.
3. Search for: **Enable primary DNS only**.
4. Double-click this setting.
5. Clear the checkbox **Enable primary DNS only**.
6. Click **Save**.

### In version R81.10.10 Builds 996002874 and higher

Starting in this build, you can change the behavior to forward the DNS requests only to the DNS servers configured in the Primary Internet connection.

1. In WebUI, click the **Device** view.
2. In the **Advanced** section, click **Advanced Settings**.
3. Search for: **Enable primary DNS only**.
4. Double-click this setting.
5. Select the checkbox **Enable primary DNS only**.
6. Click **Save**.

### In version R81.10.10 Builds lower than 996002874

The default behavior is to forward DNS requests to all configured DNS servers.

It is not possible to change this behavior.

### In version R81.10.08 Builds B996001735 and higher

The default behavior is to forward the DNS requests only to the DNS servers configured in the Primary Internet connection.

Starting in this build, you can change the behavior to forward DNS requests to all configured DNS servers.

1. In WebUI, click the **Device** view.
2. In the **Advanced** section, click **Advanced Settings**.
3. Search for: **Enable primary DNS only**.
4. Double-click this setting
5. Clear the checkbox **Enable primary DNS only**/
6. Click **Save**.

#### In version R81.10.08 (Builds lower than B996001735) and lower versions

The default behavior is to forward DNS requests to all configured DNS servers.

It is not possible to change this behavior.

# Configuring the Proxy Server

In the **Device** > **Proxy** page, you can configure a proxy server to use to connect to the Check Point update and license servers.

1. Select **Use a proxy server**.
2. Enter a **Host name or IP address**.
3. Enter a **Port**.
4. Click **Apply**

# Backup, Restore, Upgrade, and Other System Operations

In the **Device** > **System Operations** page you can:

- Reboot
- Restore factory default settings.
- Revert to the factory default image and settings.
- Automatically or manually upgrade the appliance firmware to the latest Check Point version.
- Revert to earlier firmware image.
- Backup appliance settings to a file stored on your desktop computer.
- Restore a backed up configuration.
- Enable IPv6 networking and enforce IPv6 security.

**Note** - After a reboot or failover in a high-availability setup, the appliance resumes operation automatically after power is restored, with no user intervention required.

**To reboot the appliance:**

1. Click **Reboot**.
2. Click **OK** in the confirmation message.

**To restore factory default settings:**

1. Click **Default Settings**.
2. Click **OK** in the confirmation message.

   The factory default settings are restored. The appliance reboots to complete the operation.

   **Note** - This does not change the software image. Only the settings are restored to their default values (IP address `192.168.1.1`, WebUI address `https://192.168.1.1:4434`, the username `admin` and the password `admin`).

**To revert to the factory default image:**

1. Click **Factory Defaults**.
2. Click **OK** in the confirmation message.

   The factory default settings are restored. The appliance reboots to complete the operation.

   **Note** - This restores the default software image which the appliance came with and also the default settings (IP address `https://192.168.1.1:4434`, the username is `admin`, and the password is `admin`).

**To make sure you have the latest firmware version:**

Click **Check now**.

**To automatically upgrade your appliance firmware when Cloud Services is not configured:**

1. Click **Configure automatic upgrades**.

   The Automatic Firmware Upgrades window opens.
2. Click **Perform firmware upgrades automatically**.
3. Select the upgrade option to use when new firmware is detected:
   - Upgrade immediately

     Or
   - Upgrade according to this frequency.
4. If you selected **Upgrade according to this frequency**, select one of the **Occurs** options:
   - **Daily** - Select the Time of day.
   - **Weekly** - Select the Day of week and Time of day.
   - **Monthly** - Select the Day of month and Time of day.
5. Click **Apply**

**Notes:**

- When a new firmware upgrade is available, a note shows the version number. Click **Upgrade Now** to upgrade it immediately, or click **More Information** to see what is new in the firmware version.
- If the gateway is configured by Cloud Services, automatic firmware upgrades are locked. They can only be set by Cloud Services.

### To upgrade your appliance firmware manually:

1. Click **Manual Upgrade**.

   The Upgrade Software Wizard opens.

2. Follow the Wizard instructions.

   **Note** - The firewall remains active while the upgrade is in process. Traffic disruption can only be caused by:
   - Saving a local image before the upgrade (this causes the Firewall daemon to shut down). This may lead to disruption in VPN connections.
   - The upgrade process automatically reboots the appliance.

### To revert to an earlier firmware image:

1. Click **Revert to Previous Image**.
2. Click **OK** in the confirmation message.

   The appliance reboots to complete the operation.

### To backup appliance settings:

1. Click **Backup**.

   The **Backup Settings** page opens.

2. To encrypt the backup file, select the **Use File Encryption** checkbox. Set and confirm a password.
3. To back up the security policy installed on the appliance, select the **Backup Security Policy** checkbox. You can add **Comments** about the specific backup file created.
4. Click **Save Backup**. The File Download dialog box appears.

   The file name format is:

   ```
   <current software version>-<YY-Month-day>-<HH_MM_Seconds>.zip
   ```

5. Click **Save** and select a location.

### To restore a backed up configuration:

1. Click **Restore**.

   The Restore Settings page appears.

2. Browse to the location of the backed up file.
3. Click **Upload File**.

**Important:**

- To *replace* an existing appliance with another one (for example, upon hardware failure) you can restore the settings saved on your previous appliance and reactivate your license (through **Device** > **License**).
- To *duplicate* an existing appliance you can restore the settings of the original appliance on the new one.
- Restoring settings of a different version is supported, but not automatically between every two versions. If the restore action is not supported between two versions, the gateway does not allow you to restore the settings.

**Note** - The upgrade path from 700 to 1500 appliances is currently supported only for locally managed devices.

# Using the Software Upgrade Wizard

Follow the instructions in each page of the Software Upgrade Wizard.

Click **Cancel** to quit the wizard.

## Welcome

Click the **Check Point Download Center** link to download an upgrade package as directed. If you already downloaded the file, you can skip this step.

## Upload Software

Click **Browse** to select the upgrade package file.

Click **Upload**. This may take a few minutes. When the upload is complete, the wizard automatically validates the image. A progress indicator at the bottom of the page tells you the percentage completed. When there is successful image validation, an "Upload Finished" status shows.

## Upgrade Settings

The system always performs an upgrade on a separate flash partition and your current-running partition is not affected. You can always switch back to the current image if there is an immediate failure in the upgrade process. If the appliance does not come up properly from the boot, disconnect the power cable and reconnect it. The appliance automatically reverts to the previous image.

Click the **Revert to Previous Image** button on the **System Operations** page to return to an earlier image. The backup contains the entire image, including the firmware, all system settings and the current security policy.

When you click **Next**, the upgrade process starts.

### Upgrading

The **Upgrading** page shows an upgrade progress indicator and checks off each step as it is completed.

- Initializing upgrade process
- Installing new image

## Backing up the System

The backup file includes all your system settings such as network settings and DNS configuration. The backup file also contains the Secure Internal Communication certificate and your license.

If you want to *replace* an existing appliance with another one, you can restore the settings of your previous appliance and re-activate your license (on the **License Page** > **Activate License** page).

If you want to *duplicate* an existing appliance, you can restore the settings of the original appliance on the new one. Make sure to change the IP address of the duplicated appliance (on the **Device** > **Internet** page) and generate a new license.

**To create a backup file:**

1. Click **Create Backup File**.

   The **Backup Settings** window opens.

2. To encrypt the file, click **Use file encryption**.

   If you select this option, you must enter and confirm a password.

3. **Optional** - Add a comment about the backup file.
4. Click **Create Backup**.

   System settings are backed up.

**To configure a periodic backup:**

1. In **Device** > **System Operations** > **Backup and Restore System Settings**, click **Settings**.

   The **Periodic Backup Settings** window opens.

2. Click **Enable scheduled backups**.
3. Configure the file storage destination:

a. Select the **Protocol** from the dropdown menu:

   - **SFTP**
   - **FTP**
   - **SCP**
   - **FLASH**

b. Enter a **Backup server path**.

c. Enter a username and password.

d. Click **Save**.

4. **Optional** - Select **Use file encryption**.

   If you select this option, you must enter and confirm a password.

5. In **Schedule Periodic Backup**, select frequency:

   - **Daily** - Select time of day (hour range).
   - **Weekly** - Select day of week and time of day.
   - **Monthly** - Select day of month and time of day.

     **Note** - If a month does not include the selected day, the backup is executed on the last day of the month.

6. Click **Save**.

# IPv6 Settings

**To enable IPv6:**

Click **Enable IPv6**.

Now you can configure an IPv6 address in network and policy settings on the *"Configuring Internet Connectivity" on page 87* page.

**Note** - You must reboot the appliance first.

# Configuring Local and Remote System Administrators

The **Device** > **Administrators** page lists the appliance administrators. Here you can:

- Create new local administrators.
- Configure the session timeout.
- Limit login failure attempts.
- Generate a QR code to connect the mobile application with the appliance for the first time.
- Regenerate keys.

Administrators can also be defined in a remote RADIUS server and you can configure the appliance to allow them access. Authentication of those remotely defined administrators is done by the same RADIUS server.

**Note** - This page is available from the **Device** and **Users & Objects** tabs.

# Administrator Roles:

- **Super Administrator** - All permissions. Super Administrators can create new locally defined administrators and change permissions for others.
- **Read Only Administrator** - Limited permissions. Read Only Administrators cannot update appliance configuration but can change their own passwords or run a traffic monitoring report from the **Tools** page.
- **Networking Administrator** - Limited permissions. Networking Administrators can update or modify operating system settings. They can select a service or network object but cannot create or modify it.
- **Mobile Administrator** - Mobile administrators are allowed all networking operations on all interfaces. They can change their own passwords, generate reports, reboot, change events and mobile policy, active hosts operations and pairing. They cannot login from or access the WebUI.
- **Remote Access Administrator** - Limited permissions. Remote access administrators can manage the VPN remote access configuration. They can add, edit and delete VPN remote access users and servers.
- **Access Policy Administrator** - Limited permissions. Access policy administrators can manage the Firewall settings; Applications and URL filtering settings; and the Firewall access policy. They can also create, edit, and delete network objects, services and custom applications.
- **Self-serve Administer** - Create this role in the Spark Management application in the Infinity Portal. Log in to your local gateway as a Self-serve Administrator to access the Self-serve portal.

Two administrators with write permissions cannot log in at the same time. If an administrator is already logged in, a message shows. You can choose to log in with Read-Only permission or to continue. If you continue the login process, the first administrator session ends automatically.

The correct Administrator Role must be configured to perform the operations listed below. If not, a **Permission Error** message shows.

# Local Administrators

**To create a local administrator:**

1. Click **New**.

   The **Add Administrator** page opens.

2. Enter the administrator details:

   **Note** - To enable Two-Factor Authentication (available starting from the R81.10.10 release), all administrators must have both an email address and a phone number configured. Click **Test** to verify that you can receive messages at both the email address and phone number.

   - **Name**. The hyphen (-) character is allowed in the administrator name.
   - **Password** and then **Confirm password**.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)

   - **Email address**.

     **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

   - **Phone number**. - Include the country code and do not include “+” at the beginning of the phone number. For example, "44123456789" where "44" is the country code.

     **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

   - **Administrator role** Select from the pull-down menu.
   - **Enforce password change upon the next login**. . The next time the administrator logs in, this message appears: "Your password has expired and must be changed."

     After the password is changed, the checkbox is clear. You can reselect to enforce password change at any time.

3. Click **Save**.

   The name and Administrator Role is added to the table. When logged in to the WebUI, the administrator name and role is shown at the top of the page.

**Note** - If Two-Factor Authentication is not enabled, defining an email address and phone number is **optional**. However, you must have either an email address **or** a phone number defined to:

- Receive Security alert notifications by email or SMS. See *"Notifications" on page 60*
- To reset your password on the Login page of the WebUI (see below).

**To edit the details of locally defined administrators:**

1. Select the administrator from the table and click **Edit**.
2. Make the relevant changes.
3. Click **Apply**

**To delete a locally defined administrator:**

1. Select an administrator from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

**Note** - You cannot delete an administrator who is currently logged in.

**To reset password:**

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.08 version.

You can securely reset your password when you log in to your Security Gateway.

**Note** - You must have an email address or phone number configured as part of the administrator details.

1. In the **Login** page, enter the **User Name** and click **Forgot my password.**
2. The **Find Your Account** screen appears. Enter your **Username** and your **Email** or **Phone number**, and click **Next**.

   You receive a message with a security code (One Time Password).
3. Enter the security code and click **Next**.
4. Create and enter your new password in the applicable field.

   **Note** - The password must contain a minimum of 6 characters.
5. In the **Confirm password** field, Enter the password again.

6. Click **Next**
7. A message on the screen confirms your password was successfully changed.
8. Click **Next** to proceed to the **Login** page.

# Remote Administrators

**Note** - In R81.10.10, Two-Factor Authentication is not supported when RADIUS or TACACS is configured for administrator access.

**To allow access for administrators defined in a remote RADIUS server:**

1. Make sure administrators are defined in the remote RADIUS server.
2. Make sure a RADIUS server is defined on the appliance. If there is no server, click the **RADIUS configuration** link at the top of this page. You must configure the IP address and shared secret used by the RADIUS server.
3. When you have a configured RADIUS server, click **Edit permissions**.

   The **RADIUS Authentication** window opens.
4. Select **Enable RADIUS authentication for administrators**.

   **Use roles defined on RADIUS server** is selected by default.
5. Configure the role for each user on the RADIUS server. See additional details below.

   **Note** - A user without role definition will get a login error.
6. If you select **Use default role for RADIUS users**, select the **Administrators Role**:
   - Super Admin
   - Read only
   - Networking Admin
   - Mobile Admin
7. To define groups, click **Use specific RADIUS groups only** and enter the RADIUS groups separated by a comma.
8. Click **Apply**

**To set the Session Timeout value for both local and remotely defined administrators:**

1. Click **Security Settings**.

   The **Administrators Security Settings** window opens.

2. Configure the session timeout (maximum time period of inactivity in minutes). The maximum value is 999 minutes.

3. To limit login failure attempts, click the **Limit administrators login failure attempts** checkbox.

4. Enter the number of **Maximum consecutive login attempts** allowed before an administrator is locked out.

5. In **Lock period**, enter the time (in seconds) that must pass before a locked out administrator can attempt to log in again.

6. To enforce password complexity on administrators, click the checkbox and enter the number of days for the password to expire.

   **Note** - We strongly recommend the use of complex passwords. Password must contain at least 12 characters - uppercase, lowercase, numeric, and non-alphanumeric characters. Allowed alphanumeric characters: `! @ # % ^ & * ( ) - _ + : ;`

7. Click **Apply**

# Pairing a Mobile Device

To connect the mobile application with the appliance for the first time:

1. Click **Mobile Pairing Code**.

   The **Connect Mobile Device** window opens.

2. Select an administrator from the pull down menu.

3. Click **Generate**.

   This generates a QR code to connect the Check Point WatchTower mobile application with the appliance for the first time.

For more information about the mobile application, see the *WatchTower App User Guide*.

# Configuring a RADIUS Server for non-local Quantum Spark Appliance users

Non-local users can be defined on a RADIUS server and not in the Quantum Spark Appliance. When a non-local user logs in to the appliance, the RADIUS server authenticates the user and assigns the applicable permissions. You must configure the RADIUS server to correctly authenticate and authorize non-local users.

**Notes:**

- The configuration of the RADIUS Servers may change according to the type of operating system on which the RADIUS Server is installed.
- If you define a RADIUS user with a null password (on the RADIUS server), the appliance cannot authenticate that user.

**Configuring a Steel-Belted RADIUS server for non-local appliance users**

1. Create the dictionary file `checkpoint.dct` on the RADIUS server, in the default dictionary directory (that contains `radius.dct`). Add these lines in the `checkpoint.dct` file:

```
@radius.dct
MACRO CheckPoint-VSA(t,s) 26 [vid=2620 type1=%t% len1=+2
data=%s%]
ATTRIBUTE CP-Gaia-User-Role CheckPoint-VSA(229, string)  r
ATTRIBUTE CP-Gaia-SuperUser-Access CheckPoint-VSA(230,
integer)  r
```

2. Add these lines in the `vendor.ini` file on the RADIUS server (keep in alphabetical order with the other vendor products in this file):

```
vendor-product = Quantum Spark Appliance
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```

3. Add this line in the `dictiona.dcm` file:

   `"@checkpoint.dct"`

4. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   `CP-Gaia-User-Role = <role>`

   Where *<role>* allowed values are:

| Administrator Role | Value |
|---|---|
| Super Admin | `adminRole` |
| Read only | `monitorrole` |
| Networking Admin | `networkingrole` |
| Mobile Admin | `mobilerole` |

### Configuring a FreeRADIUS server for non-local appliance users

1. Create the dictionary file `dictionary.checkpoint` in the `/etc/freeradius/` on the RADIUS server.

   Add these lines in the `dictionary.checkpoint` file:

   ```
   # Check Point dictionary file for FreeRADIUS AAA server
   VENDOR CheckPoint 2620
   ATTRIBUTE   CP-Gaia-User-Role          229   string
   CheckPoint
   ATTRIBUTE   CP-Gaia-SuperUser-Access   230   integer
   CheckPoint
   ```

2. Add this line in the `/etc/freeradius/dictionary` file

   `"$INCLUDE dictionary.checkpoint"`

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   `CP-Gaia-User-Role = <role>`

   Where *<role>* is the name of the administrator role that is defined in the WebUI.

| Administrator Role | Value |
|---|---|
| Super Admin | `adminRole` |
| Read only | `monitorrole` |
| Networking Admin | `networkingrole` |
| Mobile Admin | `mobilerole` |

### Configuring an OpenRADIUS server for non-local appliance users

1. Create the dictionary file `dict.checkpoint` in the `/etc/openradius/subdicts/` directory on the RADIUS server:

```
# Check Point Gaia vendor specific attributes
# (Formatted for the OpenRADIUS RADIUS server.)
# Add this file to etc/openradius/subdicts/ and add the line
# "$include subdicts/dict.checkpoint" to
/etc/openradius/dictionaries
# right after dict.ascend.
$add vendor 2620 CheckPoint
$set default vendor=CheckPoint
     space=RAD-VSA-STD
     len_ofs=1 len_size=1 len_adj=0
     val_ofs=2 val_size=-2 val_type=String
     nodec=0 noenc=0
$add attribute 229 CP-Gaia-User-Role
$add attribute 230 CP-Gaia-SuperUser-Access val_type=Integer
val_size=4
```

2. Add this line in the `/etc/openradius/dictionaries` file immediately after `dict.ascend`:

   `$include subdicts/dict.checkpoint`

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   `CP-Gaia-User-Role = <role>`

   Where *<role>* is the name of the administrator role that is defined in the WebUI.

| Administrator Role | Value |
|---|---|
| Super Admin | `adminRole` |
| Read only | `monitorrole` |
| Networking Admin | `networkingrole` |
| Mobile Admin | `mobilerole` |

### To log in as a Super User:

A user with super user permissions can use the Quantum Spark Appliance shell to do system-level operations, including working with the file system.

1. Connect to the Quantum Spark Appliance platform over SSH or serial console.
2. Log in to the Gaia Clish shell with your user name and password.
3. Run: `expert`
4. Enter the Expert mode password.

**Important**:

- To configure the Expert mode (Bash) as the default shell, run this command (**not recommended**):
  ```
  bashUser on
  ```
- To configure the Gaia Clish as the default shell, run this command (**recommended**):
  ```
  bashUser off
  ```

# Configuring Administrator Access

On the **Device** > **System** > **Administrator Access** page you can:

- Configure the IP addresses and interface sources that administrators can use to access the Quantum Spark Appliance.
- Enable Two-Factor Authentication (2FA) to add an extra layer of security on the gateway.
- Configure the Web and SSH ports.

**To set the interface sources from which administrator access is allowed**

Select one or more of these options:

- **LAN** - All internal physical ports
- **Trusted wireless** - Wireless networks that are allowed access to the LAN by default (only in Wireless Network models.)
- **VPN** - Uses encrypted traffic through VPN tunnels from a remote site or uses a remote access client
- **Internet** - Clear traffic from the Internet (not recommended to allow access from all IP addresses)

**To allow administrator access from any IP address**

1. Select the **Any IP address** option. This option is less secure and not recommended. We recommend you allow access from the Internet to specific IP addresses only.
2. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
3. Click **Save**.

   An administrator can access the Quantum Spark Appliance using any IP address through the allowed interface sources.

**To allow administrator access from specified IP addresses**

1. Select the **Specified IP addresses only** option.
2. Click **New**.

   The **IP Address Configuration** page appears.
3. Select **Type**:

- IPv4 address
- IPv4 network
- IPv6 address
- IPv6 network

4. Enter the IP address or click **Get IP from My Computer**.
5. Click **Save**.

   The IP address is added to the table.
6. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
7. Click **Save**.

   An administrator can use the configured IP addresses to access the appliance through the allowed interface sources.

#### To allow administrator access from both specified and any IP addresses

Select this option when it is necessary to allow administrator access from the Internet (you must define the specified IP addresses). Access from other sources is allowed from any IP address.

1. Select the Internet source checkbox.
2. Select the **Specified IP addresses from the internet and any IP address from other sources** option.
3. Click **New**.

   The **IP Address Configuration** page shows.
4. Select **Type**:
   - IPv4 address
   - IPv4 network
   - IPv6 address
   - IPv6 network
5. Enter the IP address or click **Get IP from My Computer**.
6. Click **Save**.

   The IP address is added to the table.
7. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.

8. Click **Save**.

   An administrator can use the configured IP addresses to access the appliance through the allowed interface sources.

**To delete administrator access from a specific IP address**

1. Select the IP Address you want to delete from the IP Address table.
2. Click **Delete**.

**Important**:

- Configuring different access permissions for LAN and Internet is not supported when your Internet Connection is configured in bridge mode (the option **Allow administration access from** does not show Internet or LAN).
- An automatic implied rule is defined to allow the access specified here. There is no need to add an explicit rule in the Access Policy page to allow this access.
- When you block the IP address or the interface group through which you are currently connected, you are not disconnected immediately. The access policy is applied immediately, but your current session remains active until you log out.

# Two-Factor Authentication (2FA)

Two-Factor Authentication is an extra layer of security on the gateway. When Two-Factor Authentication is enabled on the **Administrator Access** page, its use is mandatory for all administrators configured on the appliance and is required for login. All administrators must have both an email address and phone number configured.

When Two-Factor Authentication is enabled, if any administrators are missing information, a warning message appears on the **Device** > **System** > **Administrator Access** page that all administrators must first configure an email address and phone number. A list of administrators who are missing information also appears.

Another message that may appear on this page is a recommendation to use a Network Time Protocol (NTP) server to set the date and time on your appliance to avoid sync issues with the Authenticator app.

**Note** - This feature is available starting from R81.10.10.

**Note** - In R81.10.10, Two-Factor Authentication is not supported when RADIUS or TACACS is configured for administrator access.

**Important** - When Two-Factor Authentication is enabled, it is always required for login.

### Prerequisites for Two-Factor Authentication

1. In each administrator object, configure an email address **and** a phone number. See *"Configuring Local and Remote System Administrators" on page 438*.
2. To avoid sync issues with the Authenticator app, use a Network Time Protocol (NTP) sever to set the date and time on your appliance. See *"Managing Date and Time" on page 179*.

#### To enable Two-Factor Authentication enforcement for administrators

1. Go to the **Device** > **System** > **Administrator Access** page.
2. In the **Two-Factor Authentication (2FA)** section, select **Enable Two-Factor Authentication enforcement**.
3. Click **Save**.
4. The gateway sends an email (from `do-not-reply@portal.checkpoint.com`) to all configured administrators that explains how to use the Authenticator app.

   The email also contains a QR code and emergency keys.

   **Important** - Save the emails with the emergency keys. Use these keys to log in if you lose your smartphone, lose your mobile number pairing configuration, or if the gateway is not connected to the Internet. Note that each emergency key can be used only one time.
5. In the WebUI popup window, select **I received email** if you received the email or click **Resend email**.
6. Install the Authenticator app.

   You can use either the Microsoft Authenticator or the Google Authenticator.

   Both are available from the Apple App store or Google Play.
7. In the Authenticator app, add a new account in one of these ways:
   - Scan the QR code you received in the email.
   - Enter the one-time verification code you received in the email.

### To log in to the WebUI with Two-Factor Authentication

1. On the appliance **Login** page, enter your administrator name and password.

   The Two-Factor Authentication screen appears.

2. Use one of these options to receive your verification code:

   - Select the two checkboxes **SMS** and **Email**

     **Note** - To log in with this authentication option, the gateway must be connected to the Internet.

   - Select only the **SMS** checkbox

     **Note** - To log in with this authentication option, the gateway must be connected to the Internet.

   - Select only the **Email** checkbox

     **Note** - To log in with this authentication option, the gateway must be connected to the Internet.

   - Click **Authenticator app**

     **Note** - After the initial authentication, you can use the time-based code generated in the Authenticator app to log in even when the gateway is not connected to the Internet.

   **Description**

   Enter the verification code that you receive based on the selected login option:

   - From the SMS.
   - From the email.
   - From the Authenticator app.

3. Click **Next**.

4. Enter the verification code you received and click **Next**.

5. If you did not receive a code, click **Resend code** or **Try another way** to receive the code by another method.

### To log in to the command line with Two-Factor Authentication

1. Connect to the command line on the appliance.
2. Enter your username and password.
3. Enter the number of your choice of how to receive the verification code.
4. Enter the verification code.

### To receive new Two-Factor Authentication keys for a specific administrator

1. Go to the **Device** > **System** > **Administrators** page.
2. Select the administrator.
3. Click the **Regenerate Keys** button.

**Note** - This invalidates the current secret key and emergency keys.

The new keys are sent to the email address of the selected administrator. Verify that you received the email and set the Authenticator app with the new secret key to allow login via the Authenticator app.

# Managing Device Details

On the **Device** > **Device Details** page, you can:

- Enter an **Appliance Name** to identify the appliance.

  **Note** - The appliance name can only contain alphanumeric characters and the hyphen character. Do not use the hyphen as the first or last character.

- **For wireless devices only** - Configure the **Country**. The allowed wireless radio settings vary based on the standards in each country.
- Assign a Web portal certificate.

**To assign a Web portal certificate:**

1. Click the downward arrow next to the **Web portal certificate** field.

   The list of uploaded certificates shows.

2. Select the desired certificate.

   **Note** - You cannot select the default VPN certificate.

3. Click **Apply**
4. Reload the page.

# Managing Date and Time

The **Device** > **Date and Time** page shows the current system date and time. You can configure the device date and time manually or with Network Time Protocol (NTP). NTP allows a connected device to synchronize its clocks with the NTP server clock.

### To configure date and time manually:

1. Select the **Set Date and Time Manually** option.
2. Enter the current **Date** and **Time**. Click the calendar icon to enter the date. Specify whether the time is AM or PM.
3. Click **Apply**

### To set the date and time using a Network Time Protocol (NTP) server:

1. Select the **Set Date and Time Using a Network Time Protocol (NTP) Server** option.
2. Enter the Host name or IP addresses of the **NTP Server**. If the Primary NTP Server fails to respond, the Secondary NTP Server is queried.
3. Set the **Update Interval (minutes)** field.
4. Select the **NTP Authentication** checkbox if you want to supply a **Shared Secret** and a **Shared Secret Identifier** (this is optional).

   **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)

5. Click **Apply**

### To enable a local NTP server:

This allows a connected device to synchronize clocks with the NTP server clock. When enabled, you can run an NTP server from your appliance.

Select the checkbox **Run NTP server on this appliance**.

### To configure a Time Zone:

1. From the **Local Time Zone** list, select the correct time zone option.
2. Select the **Automatically adjust clock for daylight saving changes** checkbox to enable automatic daylight saving changes.
3. Click **Apply**

# Configuring DDNS and Access Service

In the **Device** > **DDNS & Device Access** page, you can:

- Configure DDNS account details in one of the supported providers.
- Configure a service that lets you remotely connect to the appliance in instances where it is behind NAT, a firewall, or has a dynamically assigned IP address.

## DDNS

When you configure DDNS, the appliance updates the provider with its IP addresses. Users can then connect to the device with a host name from the provider instead of IP addresses.

This is especially important for remote access users who connect to the device to the internal network through VPN.

**Note** - If you configured a SAML Identity Provider to use a DDNS address for the Quantum Spark appliance, changing this DDNS address breaks the configuration. To continue using the SAML Identity Provider, you must add a new Unique identifier URL and Reply URL to the SAML application in the Identity Provider's portal. For more information, see *"Configuring Authentication Servers for Remote Access" on page 384*. For more information, see *"Configuring SAML Authentication for Remote Access VPN" on page 390*.

**To configure DDNS:**

1. Select **Connect to the appliance by name from the Internet (DDNS)**.
2. Enter the details of your account on the page:
   - **Provider** - Select the DDNS provider that you set up an account with.
   - **User name** - Enter the user name of the account.
   - **Password** - Enter the password of the account.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ‘ " \ (maximum number of characters: 255)
   - **Host name** - Enter your routable host name as defined in your DDNS account.

   For more information about these details, refer to your provider's website.
3. Make sure **Reinitialize internal certificates** is selected. When you enable this feature or change settings, you must reinitialize the internal certificates for them to be valid for the new DNS.

# Reach My Device

Reach My Device lets you remotely connect to the appliance from the Internet so that you can use the WebUI or CLI when necessary. This is done by tunneling the administrative UI or CLI connections through a Check Point Cloud Service. Such configuration is very useful in instances where the appliance is behind a NAT device or firewall, and cannot be reached directly. In addition, the feature makes it easier to access an appliance with a dynamically assigned IP address.

**To register to the Reach My Device service:**

1. Click **Register**.

   The Reach My Device window opens.

2. For **Host Name**, use the default host name or enter a name for this appliance to enable remote access.
3. If the host name was already defined, select **Register with an existing homename** and enter the **Validation token** of the gateway. This token verifies that an existing name belongs to this appliance owner.
4. Click **Apply**

   The validation token, web link, and shell link are shown on the page.

5. Go to **Device** > **Administrator Access**. Configure **Internet** as a source for administrator access and **Set specified IP addresses**.

When the gateway participates in VPN, you can exclude the WAN interface (or any other interface used for the Internet connection) from the encryption domain and use Reach My Device traffic without a VPN tunnel.

In the **VPN Site to Site global settings Advanced Setting**, enable **Do not encrypt connections originating from the local gateway**.

**How to access the gateway with the Reach My Device service:**

When registration is complete, an outgoing tunnel to the Check Point Cloud Service is established with the appliance's IP address.

# Remote Access to the WebUI

Web Link - Use this URL in a browser to remotely access the appliance.

For example: `https://mygateway-web.smbrelay.checkpoint.com`

Enter the applicable user name and password.

## Remote Access to the CLI

Shell Link - Use this URL in a browser to open an SSH connection to the appliance to use CLI commands.

For example: `https://mygateway-shell.smbrelay.checkpoint.com`

Enter the administrator credentials.

# Using System Tools

On the **Tools** page you can perform various actions to diagnose problems with the appliance.

The same **Tools** page is available in:

- The **Home** view > **Troubleshooting** section.
- The **Device** view > **System** section.
- The **Logs & Monitoring** view > **Diagnostics** section.

| Action | Available From | Description |
|---|---|---|
| **Monitor System Resources** | R81.10.00 | Opens a popup windows that shows:<br>■ **CPU Usage History**<br>The information is refreshed automatically.<br>■ **Memory Usage History**<br>Memory usage is calculated without memory that was allocated in advance to handle traffic and without cache memory.<br>This gives a more accurate picture of the actual memory usage in the appliance but it may differ from figures you receive from Linux tools.<br>The information is refreshed automatically.<br>■ **Disk Usage**<br>Click the **Refresh** button for the most updated disk usage information.<br>Click the names of column to sort the output. |
| **Show Routing Table** | R81.10.00 | Opens a popup window that shows this information for each route:<br>■ **Source**<br>■ **Destination**<br>■ **Service**<br>■ **Gateway**<br>■ **Metric**<br>■ **Interface**<br>■ **Origin** |

| Action | Available From | Description |
|---|---|---|
| **Show Router Configuration** | R81.10.05 | Opens a popup window where you select one of the categories, and the window shows the corresponding Gaia Clish commands:<br>- **BGP**<br>- **OSPF**<br>- **Inbound route filters**<br>- **Route redistribution** |
| **Run Command** | R81.10.10 | Opens a popup window in which you can select a predefined CLI command and see its output:<br>- **Policy status** (shows the status of different security policies)<br>- **Scan network** (shows the connected IoT devices)<br>- **Show diagnostics** (runs the Gaia Clish command "`show diag`").) |
| **Test Cloud Services Ports** | R81.10.00 | Opens a popup window that shows the result of the Cloud Services Connectivity Test<br>(the output of the Gaia Clish command "`test cloud-connectivity`"). |

| Action | Available From | Description |
|---|---|---|
| **Tcpdump Tool** | R81.10.00 | Opens a popup window, in which you can capture traffic that passes through appliance interfaces.<br>❗ **Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window. |

| Action | Available From | Description |
|---|---|---|
| | | |

| Action | Available From | Description |
|---|---|---|
| **Firewall Monitor Tool** | R81.10.10 | Opens a popup window, in which you can capture traffic that passes through appliance interfaces.<br>**Warnings:**<br>■ When you use this tool, the CPU load increases. Schedule a maintenance window.<br>■ When you select the option "`-p all`", the CPU load increases significantly because this tool shows the information for each inspection chain module.<br>**Notes:**<br>■ The appliance runs the "`fw monitor`" command with the specified parameters. See the:<br>• *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances* > Chapter "Miscellaneous Commands" > Section "fw commands".<br>• *R81.10 CLI Reference Guide* > Chapter "Security Gateway Commands" > Section "fw" > Section "fw monitor".<br>■ Compared to the **Tcpdump Tool**:<br>• This tool shows how each packet passes through the Security Gateway inspection chain modules.<br>• This tool saves the captured traffic only in the plain-text format (filename is "`fw_monitor.log`").<br>■ You can view the captured traffic in real time or save it into a plain-text file.<br>■ When you start a new traffic capture and save it into a file, and a file with such name already exists, the appliance adds a running number to the default filename (this way, it does not overwrite an existing file).<br>■ The appliance captures traffic only on interfaces with a configured IP address.<br>■ The packet capture stops automatically if the WebUI session ends.<br>**Procedure:** |

| Action | Available From | Description |
|---|---|---|
| | | 1. Click the **Firewall Monitor Tool** button.<br>2. **Optional:** Configure the applicable filters:<br>a. In the **Monitor outgoing packets** field, enter how many outgoing packets to capture before the tool must stop the traffic capture.<br>b. In the **Monitor incoming packets** field, enter how many incoming packets to capture before the tool must stop the traffic capture.<br>c. Select "**-p all**" to see the information for each inspection chain module.<br>**Warning** - The CPU load increases significantly.<br>d. Select "**grep**" to enter a free text filter.<br>- This field is case-sensitive.<br>- If the text must contains spaces, then you must enclose it in single quotes or double quotes.<br>- The tool captures the specified number of packets, and then filters the output to show only the relevant lines.<br>3. To save the captured traffic into a plain-text file:<br>Note - If you selected "**grep**", then the saved file contains only the relevant lines you see on the screen.<br>a. Click **Save** to download the file.<br>b. Your web browser saves this file (`fw_monitor.log`) in the default download folder. |

| Action | Available From | Description |
|---|---|---|
| **Firewall Ctl Tool** | R81.10.10 | Opens a popup window, in which you can see the kernel debug that shows which packets the Security Gateway drops.<br>**Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window.<br>**Notes:**<br>- The appliance runs the "`fw ctl zdebug -m fw + drop`" command. See the *R81.10 Quantum Security Gateway Guide* > Chapter "Kernel Debug".<br>- You can view the kernel debug output in real time or save it into a plain-text file.<br>- When you start a new kernel debug and save it into a file, and a file with such name already exists, the appliance adds a running number to the default filename (this way, it does not overwrite an existing file).<br>- The kernel debug stops automatically if the WebUI session ends.<br>**Procedure:**<br>1. Click the **Firewall Ctl Tool** button.<br>2. **Optional:** In the **Command timeout** field, enter the duration (in seconds) of the kernel debug.<br>3. **Optional:** In the "**grep**" field, enter the applicable filter:<br>- This field is case-sensitive.<br>- If the text must contains spaces, then you must enclose it in single quotes or double quotes.<br>- The tool captures the specified number of packets, and then filters the output to show only the relevant lines.<br>4. To save the kernel debug output into a plain-text file:<br>Note - If you entered a "**grep**" filter, then the saved file contains only the relevant lines you see on the screen.<br>a. Click **Save** to download the file. |

| Action | Available From | Description |
|---|---|---|
| | | b. Your web browser saves this file (`fw_ctl_zdebug_drop.log`) in the default download folder. |

| Action | Available From | Description |
|---|---|---|
| **VPN Debug Tool** | R81.10.10 | Opens a popup window, in which you can start a VPN debug.<br>**Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window.<br>**Notes:**<br>■ The appliance runs the "`fw ctl zdebug -m fw + drop`" command.<br>See the *R81.10 Quantum Security Gateway Guide* > Chapter "".<br>• *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances* > Chapter "Miscellaneous Commands" > Section "fw commands".<br>• *R81.10 CLI Reference Guide* > Chapter "Security Gateway Commands" > Section "fw" > Section "fw monitor".<br>■ You can view the kernel debug output in real time or save it into a plain-text file.<br>■ When you start a new kernel debug and save it into a file, the appliance adds a running number to the default filename (this way, it does not overwrite and existing debug file).<br>■ The kernel debug stops automatically if the WebUI session ends.<br>**Procedure:**<br>1. Click the **VPN Debug Tool** button.<br>2. Click the **Start Debugging** button.<br>3. Wait until you see the line "`VPN debugging in progress`".<br>4. Do **not** close this popup window (it will stop the VPN debug).<br>5. Replicate the VPN issue:<br>■ Remote Access VPN connection to this appliance.<br>■ Site to Site VPN connection to / from this appliance.<br>6. Click the **Stop Debugging** button.<br>7. Click **Download File** to download the archive with the required log files. |

| Action | Available From | Description |
|---|---|---|
| | | 8. Your web browser saves the archive file (`vpn_<YYYYMMDDHHMM>.tgz`) in the default download folder.<br>9. To have more information, also collect the CPinfo file - see the **Generate CPInfo File** below.<br>For the complete debug procedure, refer to sk62482. |
| **Display DSL Statistics** | R81.10.00 | Opens popup window that shows the DSL statistics.<br>Available only on DSL models. |
| **Generate CPInfo File** | R81.10.00 | Collects outputs of many commands and contents of various log files into an archive package.<br>This data helps Check Point Support understand the configuration and troubleshoot issues.<br>**Procedure:**<br>1. Click **Generate CPInfo File**.<br>A message next to the button shows the progress.<br>2. When the task completes, the button changes to **Download CPInfo File**.<br>3. Click **Download CPInfo File** to download the file.<br>4. Your web browser saves this file (`R81.10<Build>_<MMDDHHMM>.cpinfo.gz`) in the default download folder.<br>5. When the download completes, the button changes to **Generate CPInfo File**. |
| **Ping** | R81.10.00 | Opens a popup window that shows the result of the ping command to the specified IP address / hostname.<br>The appliance sends ICMP Requests to the specified destination. |
| **Trace** | R81.10.00 | Opens a popup window that shows the result of the traceroute command to the specified IP address / hostname.<br>The appliance sends ICMP Requests to the specified destination. |
| **Lookup** | R81.10.00 | Opens a popup window that shows the result of the DNS lookup for the specified IP address / hostname (the output of the Gaia Clish command "`nslookup`"). |

| Action | Available From | Description |
|---|---|---|
| **Download** | R81.10.00 | Opens sk159712 to download the Windows driver for a USB-C console socket.<br>**Explanation:**<br>When the mini-USB is used as a console connector, Windows OS does not automatically detect and download the driver needed for serial communication.<br>You must manually install the driver.<br>For more information, see sk182035. |

# Advanced Routing

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

In the **Device** > **Advanced Routing** tab, you can configure these dynamic routing settings:

- **BGP** - Border Gateway Patrol (BGP). Can be deployed within and between autonomous systems (AS).
- **OSPF** - Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) used to exchange routing information between routers within a single AS.
- **Inbound Route Filters** - Control which external routes a routing protocol accepts.
- **Route Redistribution** - Redistribute routes from one routing protocol into another protocol. Similar to route maps for an export policy.
- **Routing Options** - Configure protocol ranks.
- **Routing Monitor** - View the routing table and configure manual routing rules.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances* .

# BGP

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

In the **Device** > **Advanced Routing** tab > **BGP** page, you can configure Border Gateway Patrol (BGP) dynamic routing settings.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- Configuring BGP in the WebUI
- Configuring BGP in Clish

# PIM

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.10 version.

In the **Device** > **Advanced Routing** tab > **PIM** page, you can configure Protocol-Independent Multicast (PIM) dynamic routing settings.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- Configuring PIM in the WebUI
- Configuring PIM in Clish

# OSPF

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

In the **Device** > **Advanced Routing** tab > **OSPF** page, you can configure Open Shortest Path First (OSPF) dynamic routing settings.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- OSPFv2 in WebUI
- OSPFv2 in Clish

# Inbound Route Filters

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

In the **Device** > **Advanced Routing** tab, you can configure Inbound Route Filters for dynamic routing.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- Inbound Route Filters

# Route Redistribution

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

In the **Device** > **Advanced Routing** tab > **Route Redistribution** page, you can configure Route Redistribution for dynamic routing.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- Route Redistribution

# Routing Options

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

In the **Device** > **Advanced Routing** tab > **Routing Options** page, you can configure Routing Options (protocol ranks) for dynamic routing settings.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- IPsec Routing Options
- IPsec Routing in Gaia Clish

# Routing Monitor

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

In the **Device** > **Advanced Routing** tab > **Routing Table** page, you can view the routing table and configure manual routing rules.

For WebUI and Gaia Clish configuration instructions, see the *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- Monitoring IPsec Routing in Gaia Clish
- Monitoring BGP
- Monitoring OSPF

# Configuring the Routing Table

## Background

This page shows the routing table with the routes added on your appliance:

| Version | Description |
|---|---|
| R81.10.05 and higher | The **Device** view > **Advanced Routing** section > **Routing Table** page. |
| R81.10.00 | The **Device** view > **Network** section > **Routing** page. |

**Notes:**

- You can add or edit routes and configure manual routing rules.
  You cannot edit system defined routes.
- You can specify routes for and associate IP addresses with selected VPN tunnels.
  To add, delete, and modify the IP addresses, use dynamic routing protocols.
- When no default route is active, this page shows this message:
  `Note - No default route is configured. Internet connections might be down or not configured.`
- For Internet Connection High Availability, the default route changes automatically on failover (based on the active Internet connection).
- When a network interface is disabled, the routing table shows all routes for that interface as **inactive**. A route automatically becomes active when the interface is enabled. Traffic for an inactive route is routed based on active routing rules (usually, to the default route).
- You cannot edit, delete, enable, and disable routes created by the operating system for directly attached networks or by dynamic routing protocols.

## Routing Table Columns

If you configured IPv6 connections, the new IPv6 Routing Table appears below the IPv4 Routing Table.

**Explanation**

| Column | Description |
|---|---|
| **Destination** | The route rule applies only to traffic whose destination matches the destination IP address/network. |
| **Source** | **IPv4 address only.**<br>The route rule applies only to traffic whose source matches the source IP address/network. |
| **Service** | **IPv4 address only.**<br>The route rule applies only to traffic whose service matches the service IP protocol and ports or service group. |
| **Next Hop** | The next hop gateway for this route, with these options:<br>■ Specified IP address of the next hop gateway.<br>■ Specified Internet connection from the connections configured in the appliance.<br>■ Specified VPN Tunnel Interface (VTI). |
| **Metric** | The priority of the route.<br>If multiple routes to the same destination exist, the route with the lowest metric is selected.<br>For IPv6 addresses, the range is:<br>■ 0-100 for non-default routes<br>■ 101-200 for default routes. |
| **Protocol** | **IPv4 address only**.<br>Type of route:<br>■ Static<br>■ Directly connected<br>■ BGP<br>■ OSPF<br>■ RIP<br>■ Aggregate<br>■ Kernel<br>■ N/A |

| Column | Description |
|---|---|
| **Rank** | **IPv4 address only**.<br>A numeric value used to determine which protocol has a higher priority - the lower the value, the higher the priority).<br>**Notes:**<br>- You can configure this parameter only in Gaia Clish.<br>- Static routes have a constant rank of 60 (cannot be changed). |

# Limitations

- When there is a default route on an internal port, WebUI and SSH access to the appliance is allowed only through the LAN ports or the active Internet connection (and not through an inactive Internet interface).
- In R81.10.00, static routes are not supported with a VPN Tunnel (VTI) as the Next Hop.

# Adding a Specific IPv4 Static Route

This procedure adds a specific static route to send traffic from any source, to any destination, for any protocol to a specific IPv4 address.

**Procedure**

1. From the left navigation panel, click **Device**.
2. In the **Advanced Routing** section, click the **Routing Table** page.
3. Above the routing table, click **New**.

   The **New Static Routing Rule** window opens.
4. In the **Destination** column:
   - To route traffic to any destination, leave the default value **Any**.
   - To route traffic to a specific destination IPv4 address:
     a. Click the value **Any**.
     b. Select **Specified IP Address**.
     c. Configure the required **IP Address**.
     d. Configure the required **Subnet Mask**.
     e. Click **OK**.
5. In the **Source** column:

- To route traffic from any source, leave the default value **Any**
- To route traffic from a specific IPv4 address:
    1. Click the value **Any**.
    2. Select **Specified IP Address**.
    3. Configure the required **IP Address**.
    4. Configure the required **Subnet Mask**.
    5. Click **OK**.

6. In the **Service** column:
    - To route traffic for all services (protocols), leave the default value **Any**
    - To route traffic for a specific service:
        a. Click the value ***Any**.

        b. Select the required service object or a service group object.

        **Notes:**
        - You can select only one service object or one service group object.
        - In the bottom right corner, you can click **New** > **Service**, or **Service group** to create a custom service or a group of services.

        c. Click **OK**.
7. In the **Next Hop** column:

a. Click the cell.

b. Select the required option:

- **IP Address** - Enter the IPv4 address of the required next hop.

  **Note** - This option supports the nexthop probing only if in the **Destination** column, you selected **Specified IP Address** (destination-based route).
  - For the probing to work, the nexthop IP address must be on the same subnet as one of the **internal** appliance interfaces (LAN, DMZ).
  - If it is necessary to probe a nexthop of an Internet connection, then enable SD-WAN and use the SD-WAN probing settings (see *"SD-WAN" on page 275*).

- **Internet connection** - Select the required Internet connection.

  **Note** - This option does not support the nexthop probing.

- **VPN Tunnel (VTI)** - Select the required VPN Tunnel Interface or the GRE interface (you must configure it in advance).

  **Note** - This option supports the nexthop probing only if in the **Destination** column, you selected **Specified IP Address** (destination-based route).

- **Interface** - Select the required Local Network interface (LAN, DMZ).

  **Notes:**
  - In the R81.10.X releases, this option is available starting from the R81.10.05 version.
  - This option does not support the nexthop probing.

c. Click **OK**.

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

9. **Optional:** In the **Metric** field, enter a value:

   **Notes:**
   - Enter a value between 0 and 100.
   - The lower the value, the higher the priority.
   - The default metric is 0.

10. **Optional**: In the **Rank** field, enter a value between 1 and 255 to define priority between routes with the same destination but for different routing protocols.

**Notes:**

- In the R81.10.X releases, this field is available starting from the R81.10.10 version.
- Rank is allowed only if in the **Destination** column, you selected **Specified IP Address**.
- Rank is per destination.
  All routes with the same destination have the same rank, even though their next hop and metric are different.
- The default rank is 60.
- To change the default route rank, go to **Device** view > *"Advanced Settings" on page 246* .

11. **Optional:** Configure the nexthop probing.

    **In R81.10.08 and lower versions:**

    You must disable the probing because in these versions, the probing feature supports only default static routes.

    - In R81.10.08 and R81.10.07 versions:

      In the **Monitoring** field, select **Off**.

    - In R81.10.05 and lower versions:

      In the **Probing method** field, select **Off**.

    **In R81.10.10 and higher versions:**

    In the **Monitoring** field, select the applicable option:

    - **Off** - To disable the route probing (this is the default).
    - **On** - To enable the route probing.

    Configure the applicable probing servers. For example:

    - `dns.google.com`
    - `dns.cloudflare.com`
    - `dns.opendns.com`

**Notes:**

- Starting from R81.10.10, the probing feature supports only default static routes and destination-based routes.
  Policy-based routes are supported starting from R81.10.15
- If the Next Hop type is an IP address,
  For destination-based routes, the nexthop IP address must be on the same subnet as the destination IP address.
  For example, for a route with a destination to 7.7.7.0/24 and nexthop 192.168.2.3, a probing server must have an IP address from the 7.7.7.0/24 subnet (for example, 7.7.7.10).
- If the nexthop type is a VTI (or a GRE), the nexthop can either be on the subnet of the destination IP address or the IP address of the remote-peer of the tunnel if you want to probe the tunnel.

12. **Optional:** In the **Advanced Probing Settings** section, configure the probing settings:

    - **Probing frequency** - Interval between pings.
    - **Percentage of failed attempts** - Threshold to consider the nexthop as unreachable.
    - **Max latency** - Maximum latency for pings.
    - **Reconnection delay** - Delay before the appliance starts using this route again after the nexthop becomes reachable again.
    - **History timeline size** - Size of the probing history timeline in the **Route Monitoring** window (see *"Route Monitoring" on page 213*).

    **Note** - You can hover over the field name to see the ? icon and hover over it to see the tooltip.

13. Save the changes:

    - In R81.10.10 and higher versions:

      Click **Save**.

    - In R81.10.08 and lower versions:

      Click **Apply**.

## Adding a Default IPv4 Static Route

This procedure adds a default static route to send traffic from any source, to any destination, for any protocol.

**Procedure**

1. From the left navigation panel, click **Device**.
2. In the **Advanced Routing** section, click the **Routing Table** page.
3. Above the routing table, click **New**.

   The **New Static Routing Rule** window opens.
4. In the **Destination** column:

   Leave the default value **Any**.
5. In the **Source** column:

   Leave the default value **Any**.
6. In the **Service** column:

   Leave the default value **Any**.
7. In the **Next Hop** column:

a. Click the cell.

b. Select the required option:

- **IP Address** - Enter the IPv4 address of the required next hop.

  **Note** - This option supports the nexthop probing.
  - For the probing to work, the nexthop IP address must be on the same subnet as one of the **internal** appliance interfaces (LAN, DMZ).
  - If it is necessary to probe a nexthop of an Internet connection, then enable SD-WAN and use the SD-WAN probing settings (see *"SD-WAN" on page 275*).

- **Internet connection** - Select the required Internet connection.

  **Note** - This option does not support the nexthop probing.

- **VPN Tunnel (VTI)** - Select the required VPN Tunnel Interface or the GRE interface (you must configure it in advance).

  **Note** - This option supports the nexthop probing.

- **Interface** - Select the required Local Network interface (LAN, DMZ).

  **Notes:**
  - In the R81.10.X releases, this option is available starting from the R81.10.05 version.
  - This option does not support the nexthop probing.

c. Click **OK**.

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

9. In the **Metric** field, enter a value:

   **Notes:**
   - Enter a value between 101 and 200.
   - The lower the value, the higher the priority.

10. **Optional:** In the **Probing method** field, select the applicable option:

    - **Off** - route probing is disabled.
    - **On** - route probing is enabled.

    Configure the applicable nexthop servers to probe. For example:

- `dns.google.com`
- `dns.cloudflare.com`
- `dns.opendns.com`

**Notes:**

- Starting from R81.10.10, the probing feature supports only default static routes and destination-based routes.
  Policy-based routes are supported starting from R81.10.15.
- If the Next Hop type is an IP address,
  For destination-based routes, the nexthop IP address must be on the same subnet as the destination IP address.
  For example, for a route with a destination to 7.7.7.0/24 and nexthop 192.168.2.3, a probing server must have an IP address from the 7.7.7.0/24 subnet (for example, 7.7.7.10).
- If the nexthop type is a VTI (or a GRE), the probing server can either be on the subnet of the destination IP address or the IP address of the remote-peer of the tunnel if you want to probe the tunnel.

11. **Optional:** In the **Advanced Probing Settings** section, configure the probing settings:

    - **Probing frequency** - Interval between pings.
    - **Percentage of failed attempts** - Threshold to consider the nexthop as unreachable.
    - **Max latency** - Maximum latency for pings.
    - **Reconnection delay** - Delay before the appliance starts using this route again after the nexthop becomes reachable again.
    - **History timeline size** - Size of the probing history timeline in the **Route Monitoring** window (see *"Route Monitoring" on page 213*).

    **Note** - You can hover over the field name to see the ? icon and hover over it to see the tooltip.

12. Save the changes:

    - In R81.10.10 and higher versions:

      Click **Save**.

    - In R81.10.08 and lower versions:

      Click **Apply**.

## Editing an Existing Static Route

**Procedure**

1. From the left navigation panel, click **Device**.
2. In the **Advanced Routing** section, click the **Routing Table** page.
3. In the routing table, click the route.
4. Above the routing table, click **Edit**.
5. Change the configuration.
6. Click **Apply**.

## Deleting an Existing Static Route

**Procedure**

1. From the left navigation panel, click **Device**.
2. In the **Advanced Routing** section, click the **Routing Table** page.
3. In the routing table, click the route.
4. Above the routing table, click **Delete**.

## Enabling or Disabling an Existing Static Route

**Procedure**

1. From the left navigation panel, click **Device**.
2. In the **Advanced Routing** section, click the **Routing Table** page.
3. In the routing table, click the route.
4. Above the routing table, click **Enable** or **Disable**.

## Route Monitoring

Above the IPv4 Routing table, click **Monitor**.

**Explanation**

The **Route Monitoring** window opens.

Every row represents a server that the route probes to and its statistics.

Example:

| Next Hop | Route Status | Server | Packet Loss | Failures | Min Latency | Avg. Latency |
|---|---|---|---|---|---|---|
| 1.1.1.1 | Active | dns.google.com | 0 | 0 | 4 | 5.7 |

Each monitored route can have a maximum of 3 rows (one for each server).

**Route Status:**

- Active (green)
- Inactive (red)
- Reconnecting (orange)

# Static Routes and SD-WAN

### Explanation

When SD-WAN is enabled on the appliance (this is the default), SD-WAN routing decision takes priority over all static routes (configured in the **Device** view > the **Advanced Routing** section > the **Routing Table** page) that send traffic through **Internet Connections**.

This is the default SD-WAN configuration:

1. The **SD-WAN** blade is enabled.
2. Each **Internet** connection is enabled for SD-WAN.

If you do **not** want to use SD-WAN, then to send traffic through Internet Connections based on the configured static routes, follow one of these options:

- Disable the **SD-WAN** blade:

  ⓘ **Note** - This completely disables SD-WAN on the appliance.

  1. Click the **Access Policy** view > in the **Firewall** section, click the **SD-WAN** page.
  2. At the top of the page, move the slider to the left position (near the text "**SD-WANblade is enabled**").

- In each specific **Internet** connection, clear the option **This Internet connection will be a part of SD-WAN**:

  ⓘ **Note** - Use this option to disable SD-WAN only in a specific interface and keep using SD-WAN with other interfaces.

  1. Click the **Device** view > in the **Network** section, click the **Internet** page.
  2. Select the Internet connection and click **Edit**.
  3. Go to the right tab **Advanced**.
  4. Expand the last section **SD-WAN Settings**.
  5. Clear the option **This Internet connection will be a part of SD-WAN**.

# Managing Installed Certificates

On the **Installed Certificates** page, you can create and manage appliance certificates or upload a P12 certificate. Uploaded certificates and the default certificates are displayed in a table. To see certificate details, click the certificate name.

You can upload a certificate signed by an intermediate CA or root CA. All intermediate and root CAs found in the P12 file are automatically uploaded to the trusted CAs list.

**Note** - This page is available from the **Device** and **VPN** tabs.

On the **VPN Remote Access Blade Control** page, after you enable the SSL VPN feature, you can select and assign a certificate from the list of the installed certificates (with the exception of the Default Web Portal certificate). You can also do this on the **Remote Access Advanced** tab.

On the **Device** > **Device Details** page, you can select and assign a Web portal certificate from the list of installed certificates (with the exception of the Default certificate).

Installed certificates are used in site-to-site VPN, SSL VPN, and the Web portal.

When Cloud Services is turned on and the appliance is configured by Cloud Services, the Cloud Services Provider certificate is downloaded automatically to the appliance. The Cloud Services Provider certificate is used by community members configured by Cloud Services. - If you turn Cloud Services off, the Cloud Services Provider certificate is removed.

**These are the steps to create a signed certificate:**

1. Create a signing request.
2. Export the signed request (download the signing request from the appliance).
3. Send the signing request to the CA.
4. When you receive the signed certificate from the CA, upload it to the appliance.

**To create a new certificate to be signed by a CA:**

1. Click **New Signing Request**.
2. Enter a **Certificate** name.
3. In the **Subject DN** enter a distinguished name (e.g. `CN=myGateway`).
4. **Optional:** Click **New** to add alternate names for the certificate.

   Select the **Type**, enter the **Alternate name**, and click **Apply**.
5. Click **Generate**.

The new signing request is added to the table and the status shows "Waiting for signed certificate".

**Note** - You cannot edit the request after it is created.

If the new signing request is signed by the Internal CA and the Organization Name is not defined in the DN, the Internal CA automatically generates the Organization Name.

**To export the signing request:**

Click **Export**.

**To upload the signed certificate when you receive the signed certificate from the CA:**

1. Select the signing request entry from the table.
2. Click **Upload Signed Certificate**.
3. Browse to the signed certificate file (*.crt).
4. Click **Complete**.

   The status of the installed certificate record changes from "Waiting for signed certificate" to "Verified".

**To upload a P12 file:**

1. Click **Upload P12 Certificate**.
2. Browse to the file.
3. Edit the **Certificate name** if necessary.
4. Enter the certificate **password**.
5. Click **Apply**

# Managing Internal Certificates

In the **Certificates Internal Certificate** page you can view details of an internal VPN certificate. You can also view and reinitialize the certificate used by the internal CA that signed the certificate and can be used to sign external certificates.

**Note** - This page is available from the **Device** and **VPN** tabs.

When you create an internal VPN certificate, when a certificate that is signed by the internal CA is used, the CA's certificate must be reinitialized when the Internet connection's IP addresses change.

To avoid constant reinitialization, we recommend you use the DDNS feature. See **Device** > **DDNS**. When DDNS is configured, you only need to reinitialize the certificate once. Changes in the DDNS feature configuration by default automatically reinitialize certificates.

**To reinitialize certificates:**

1. Click **Reinitialize Certificates**.
2. Enter the **Host/IP address**.

   Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.
3. Select the number of years for which the Internal VPN Certificate is valid. The default is 3. The maximum value allowed is 20.
4. Click **Apply**

   **Note** - The internal VPN certificate expiration date cannot be later than the CA expiration date.

### To replace an internal CA certificate:

1. Click **Replace Internal CA Certificate**.
2. Click **Browse** to select the CA certificate file that includes the private key.
3. Enter the **Certificate name** and private key's password to allow the device to sign certificates with the uploaded CA.
4. Enter the **Host/IP address**.

   Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.
5. Click **Apply**

### To export an internal CA certificate:

Click **Export Internal CA Certificate** to download the internal CA certificate.

### To sign a remote site's certificate request by the internal CA:

1. Click **Sign a Request**.
2. Click **Browse** to upload the signing request file as created in the remote site.

   In third party appliances, make sure to look in its Administration Guide to see where signing requests are created.

   The file must be in a path accessible to the appliance. After you click **OK** in the file browsing window, the file is uploaded. If it is correctly formatted, it is signed by the Internal CA and the **Download** button is available.
3. Click **Download**.

   The signed certificate is downloaded through your browser and is available to be imported to the remote site's certificates list.

# Configuring High Availability

## Background

Cluster maintains connections in the organization's network when there is a failure in one of the Cluster Members. The cluster provides redundancy.

In the **Device** view > **Advanced** section > **High Availability** page you can create a cluster of two appliances for high availability.

After you configure a cluster, you can select to **Enable** or **Disable** the cluster.

**Notes:**

- This release supports only the High Availability Cluster mode:
  One Cluster Member is Active. The other Cluster Member is Standby.
  - In versions R81.10.15 and higher:
    The cluster supports these recovery modes (which Cluster Member to select as Active during a cluster fail-back, when the cluster returns to normal operation after a cluster failover):
    - **Active up**
      This is the default.
      The Cluster Member that is currently in the Active state, remains in this state.
      The other Cluster Member that returns to normal operation, remains in the Standby state.
    - **Primary up**
      The Cluster Member with higher priority is the first one to be configured. The primary Cluster Member that has the highest priority becomes the new Active.
      The state of the previously Active Cluster Member changes to Standby.
  - In versions R81.10.00 - R81.10.10:
    The cluster supports only the "**Active up**" recovery mode.
    The Cluster Member that is currently in the Active state, remains in this state.
    The other Cluster Member that returns to normal operation, remains in the Standby state.
- After you configure the cluster, when you connect to the Cluster Virtual IP address, the cluster automatically redirects you to the current Active Cluster Member.
  To log in to specific Cluster Member, you must connect to the physical IP address of that Cluster Member.

# Limitations

- You cannot create a cluster when you have a switch defined in the network settings on the appliance. If necessary, change network settings in the **Device** > **Local Network** page.

  Starting from R81.10.15, cluster in Bridge Mode is supported.
- In versions R81.10.10 and lower, it is not supported to configure a cluster of Quantum Spark Appliances when the Internet connection is a Bond interface.
- Cluster requires Static IP addresses on the physical cluster interfaces.
- Cluster does not support pure IPv6 addresses on cluster interfaces (you must also configure IPv4 addresses).
- All cluster configuration is done through the Active Cluster Member. The WebUI of the Standby Cluster Member only has some options available for fine tuning - basic network settings, and logs (a cluster managed by Quantum Spark Portal cluster also has Cloud Services).
- A Spark cluster may display CoreXL inconsistency between the cluster members. The models are: 1530, 1535, 1570, 1575, and 1900.

  Such inconsistency may be because the associated Spark license was not installed on both cluster members or the license installation was not followed by reboot. If this is the case, one cluster member is Active and the other is Down.

  1. When you run this command on the Down member:

     ```
     cphaprob -a if
     ```

     CoreXL pnote is displayed.
  2. When you run this command on both members:

     ```
     fw ctl multik stat
     ```

     The number of CoreXL instances for each member will be different.

     To recover:

     a. Verify that the Spark license is installed on both members.

     b. Make sure that license installation was followed by reboot of both cluster members.

     c. If the issue is not resolved after following these steps, refer to sk174423 and manually set the number of CoreXL instances according to the default number of CoreXL instances for this model.

# Prerequisites

- In **WebUI** > **Device** > **Local Network**, delete switch configurations before you start to configure a cluster.
- The appliances in a cluster must have the same hardware, firmware (version and build), and licenses.

  **Note** - Connect the sync cables only after you complete the First Time Configuration Wizard and remove the switch on both appliances. No additional configuration is required on the members.

**Best Practice** - Designate the same LAN port for the Sync interface. The default Sync interface is **LAN2/SYNC**. For appliance models 1600, 1800, 1900 and 2000, we recommend that you configure a bond of two interfaces for synchronization.

# Configuration Workflow

1. Complete the First Time Configuration Wizard on both appliances.

   In the **Local Network** page of the wizard, clear the checkbox **Enable switch on LAN ports**.

2. Configure network settings on the appliance that is the primary Cluster Member.

3. Connect cables between the Sync interfaces on the appliances.

   **Note** - Sync ports can also be connected through a switch.

4. Configure the primary Cluster Member.

   **Procedure**

   a. Connect to the WebUI on the appliance.

   b. From the left navigation panel, click **Device**.

   c. In the **Advanced** section, click the **High Availability** page.

   d. Click **Configure Cluster**.

      The **New Cluster Wizard** opens.

   e. On the page **Step 1: Gateway Priority**:

      i. Select this option:

         - In versions R81.10.15 and higher:

           **Configure first member**.

         - In versions R81.10.00 - R81.10.10

           **Configure as primary member**.

      ii. Click **Next**.

f. On the page **Step 2: SIC Settings**:

**Steps for versions R81.10.15 and higher**

**Important** - The configuration on the second Cluster Member must match the configuration on the primary Cluster Member.

i. In the **Sync Interface** section, configure the required settings for the synchronization interfaces:

- In the field **Sync interface (master)**, select the first (main) synchronization interface. Default: **LAN2**
- In the field **Second sync interface**, select the second synchronization interface.

  **Best Practice** - For large appliances such as the 1600, 1800, 1900, and 2000, we highly recommend that you select a second sync interface.

  This creates a bond interface called **SYNCBOND** that includes both the first and second synchronization interfaces.

ii. In the **Advanced** sub-section, you can override the default settings:

   i. In the field **Operation mode**, you can select the working mode between the synchronization interfaces of the Cluster Members:

      - Select **Health check** if the synchronization interfaces on the Cluster Members are connected through a switch.

      - Select **Link state** (this is the default) if the synchronization interfaces on the Cluster Members are connected directly to each other.

   ii. In the field **Sync IP address**, you can configure a different IPv4 address of the synchronization interface on the primary Cluster Member. Default: **10.231.149.1**

   iii. In the **Sync IP subnet** field, you can configure a different IPv4 address of the synchronization subnet. Default: **255.255.255.0**

   iv. In the field **Other member sync IP address**, you can configure a different IPv4 address of the synchronization interface on the second Cluster Member. Default: **10.231.149.2**

   v. In the field **Synchronization mode**, you can select the working mode for the cluster synchronization:

      - **Optimized sync**

        This is the default.

        This mode synchronizes most of kernel tables to ensure smooth cluster failover.

        This mode does not synchronize large kernel tables (such as "Connections").

      - **Sync is enabled**

        This mode synchronizes all the kernel tables.

        **Important** - Depending on the number of concurrent connections and the enabled Software Blades, this mode can increase the load on the CPU.

      - **Sync is disabled**

        This mode disables the synchronization.

vi. In the field **High Availability mode**, you can configure the Cluster Member recovery method - which Cluster Member to select as Active during a cluster fail-back (when the cluster returns to normal operation after a cluster failover):

**Important:**
- This mode must be the same on both Cluster Members.
- Changing this mode may cause a cluster failover.

- **Active up**

  This is the default.

  The Cluster Member that is currently in the Active state, remains in this state.

  The other Cluster Member that returns to normal operation, remains in the Standby state.

- **Primary up**

  The Cluster Member with higher priority is the first one to be configured. The primary Cluster Member that has the highest priority becomes the new Active.

  The state of the previously Active Cluster Member changes to Standby.

iii. In the **Secure Internal Communication** section, in the fields **Password** and **Confirm**, enter a one-time password for connecting the two Cluster Members to each other.

**Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)

iv. Click **Next**.

**Steps for versions R81.10.00 - R81.10.10**

**Important** - The configuration on the second Cluster Member must match the configuration on the primary Cluster Member.

i. In the **Secure Internal Communication** section, in the fields **Password** and **Confirm**, enter a one-time password for connecting the two Cluster Members to each other.

   **Notes:**
   - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)
   - You must enter the same one-time password when you configure the second Cluster Member.

ii. In the **Advanced** section, you can override the default settings:

    i. In the field **Sync interface**, you can select a synchronization interface. Default: **LAN2**

    ii. In the field **Sync IP address**, you can configure the IPv4 address of the synchronization interface on the primary Cluster Member. Default: **10.231.149.1**

    iii. In the field **Sync IP subnet**, you can configure the IPv4 address of the synchronization subnet. Default: **255.255.255.0**

    iv. In the field **Other member sync IP address**, you can configure the IPv4 address of the synchronization interface on the second Cluster Member. Default: **10.231.149.2**

iii. Click **Next**.

g. On the page **Step 3: Gateway Interfaces (<X> out of <Y>)**:

On these pages, you configure the "internal" and "external" cluster interfaces.

> **Note** - The physical IP addresses of cluster interfaces and the cluster Virtual IP address must be in the same subnet unless you are configuring a *"Single Routable IP Cluster" on page 239*.

**Steps for versions R81.10.15 and higher**

i. Select **Enable High Availability on interface** (this is the default).

If you enable the high availability on an interface, the primary Cluster Member monitors it and if there is a failure, it automatically fails over to the second Cluster Member.

If you clear this option, then you can also clear the option **Monitor interface state (fail over when interface is down)** to stop the cluster monitoring completely.

ii. In the field **Cluster IP address**, configure the applicable cluster Virtual IPv4 address. All hosts and network devices on the corresponding connected network must send their traffic to this Virtual IP address as their default gateway.

iii. In the field **Subnet mask**, configure the applicable IPv4 subnet mask for the cluster Virtual IP address.

iv. In the field **This physical IP address**, the wizard shows the IPv4 address configured on the interface.

v. In the field **Peer physical IP address**, configure the applicable IPv4 address.

vi. Click **Next**.

**Steps for versions R81.10.00 - R81.10.10**

i. Select **Enable High Availability on interface** (this is the default).

If you enable the high availability on an interface, the primary Cluster Member monitors it and if there is a failure, it automatically fails over to the second Cluster Member.

If you clear this option, then you can also clear the option **Monitor interface state (fail over when interface is down)** to stop the cluster monitoring completely.

ii. In the field **Cluster IP address**, configure the applicable cluster Virtual IPv4 address. All hosts and network devices on the corresponding connected network must send their traffic to this Virtual IP address as their default gateway.

iii. In the field **Subnet mask**, configure the applicable IPv4 subnet mask for the cluster Virtual IP address.

iv. In the field **Primary physical IP address**, the wizard shows the IPv4 address configured on the interface.

v. In the field **second physical IP address**, configure the applicable IPv4 address.

vi. Click **Next**.

h. Click **Finish**.

**Note** - At the top of the page, the **Peer gateway** field shows "**is not defined**". This status changes after you finish configuring the second Cluster Member.

5. Configure the second Cluster Member.

**Procedure**

a. Connect to the WebUI on the appliance.

b. From the left navigation panel, click **Device**.

c. In the **Advanced** section, click the **High Availability** page.

d. Click **Configure Cluster**.

The **New Cluster Wizard** opens.

e. On the page **Step 1: Gateway Priority**:

i. Select this option:

- R81.10.15 and higher:

  **Configure as peer member**.

- R81.10.00 - R81.10.10

  **Configure as second member**.

ii. Click **Next**.

f. On the page **Step 2: SIC Settings**:

**Steps for versions R81.10.15 and higher**

> **Important** - The configuration on the second Cluster Member must match the configuration on the primary Cluster Member.

i. In the **Sync Interface** section, configure the required settings for the synchronization interfaces:

- In the field **Sync interface (master)**, select the first (main) synchronization interface. Default: **LAN2**
- In the field **Second sync interface**, select the second synchronization interface.

> **Best Practice** - For large appliances such as the 1600, 1800, 1900, and 2000, we highly recommend that you select a second sync interface.

This creates a bond interface called **SYNCBOND** that includes both the first and second synchronization interfaces.

ii. In the **Advanced** sub-section, you can override the default settings:

   i. In the field **Operation mode**, you can select the working mode between the synchronization interfaces of the Cluster Members:

      - Select **Health check** if the synchronization interfaces on the Cluster Members are connected through a switch.

      - Select **Link state** (this is the default) if the synchronization interfaces on the Cluster Members are connected directly to each other.

   ii. In the field **Sync IP address**, you can configure a different IPv4 address of the synchronization interface on the primary Cluster Member. Default: **10.231.149.1**

   iii. In the **Sync IP subnet** field, you can configure a different IPv4 address of the synchronization subnet. Default: **255.255.255.0**

   iv. In the field **Other member sync IP address**, you can configure a different IPv4 address of the synchronization interface on the second Cluster Member. Default: **10.231.149.2**

v. In the field **High Availability mode**, you can configure the Cluster Member recovery method - which Cluster Member to select as Active during a cluster fail-back (when the cluster returns to normal operation after a cluster failover):

> **Important:**
> - This mode must be the same on both Cluster Members.
> - Changing this mode may cause a cluster failover.

- **Active up**

  This is the default.

  The Cluster Member that is currently in the Active state, remains in this state.

  The other Cluster Member that returns to normal operation, remains in the Standby state.

- **Primary up**

  The Cluster Member with higher priority is the first one to be configured. The primary Cluster Member that has the highest priority becomes the new Active.

  The state of the previously Active Cluster Member changes to Standby.

iii. In the **Secure Internal Communication** section, in the field **Password** enter the same one-time password you configured for the primary Cluster Member.

**Steps for versions R81.10.00 - R81.10.10**

> **Important** - The configuration on the second Cluster Member must match the configuration on the primary Cluster Member.

i. In the **Secure Internal Communication** section, in the field **Password** enter the same one-time password you configured for the primary Cluster Member.

ii. In the **Advanced** section, you can override the default settings:

  i. In the field **Sync interface**, you can select a synchronization interface. Default: **LAN2**

  ii. In the field **Sync IP address**, you can configure the IPv4 address of the synchronization interface on the primary Cluster Member. Default: **10.231.149.1**

  iii. In the field **Sync IP subnet**, you can configure the IPv4 address of the synchronization subnet. Default: **255.255.255.0**

  iv. In the field **Other member sync IP address**, you can configure the IPv4 address of the synchronization interface on the second Cluster Member. Default: **10.231.149.2**

iii. Click **Next**.

g. Click **Establish Trust**.

The second Cluster Member fetches the settings from the primary Cluster Member and applies them.

h. Click **Finish**.

# Viewing Cluster Interfaces

### Procedure

1. Connect to the WebUI on a Cluster Member:

   ```
   https://<IP Address of the Cluster Member>:4434
   ```

   **Best Practice** - After the cluster is successfully configured, connect to `https://<Virtual IP Address of the Cluster>:4434`. This redirects you to the WebUI **Home** > **System** page for the active Cluster Member.

2. From the left navigation panel, click **Device**.

3. In the **Advanced** section, click the **High Availability** page.

4. The table **List of Configured Interfaces** shows information about the cluster interfaces:

| Column | Description |
|---|---|
| **Name** | Name of the interface. |

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td><b>Status</b></td><td>Cluster status of the interface:
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td><b>High Availability</b></td><td>Two physical interfaces in 2 Cluster Members act as a single interface toward the network, using a single virtual IP address.<br><b>Note</b> - In this cluster solution, each interface has a local IP address in addition to the shared single virtual IP address.</td></tr>
<tr><td><b>Sync</b></td><td>Two physical interfaces must be defined as Sync interfaces and connected between the members to allow proper failover as needed. The default is to use LAN2/Sync physical port.</td></tr>
<tr><td><b>Non HA</b></td><td>This status is also called <b>private</b>.<br>The physical interface in this member does not participate in High Availability functions.</td></tr>
<tr><td><b>Monitored</b></td><td>This status is also called <b>private monitored</b>.<br>The physical interface on this Cluster Member is not coupled with another interface on the other Cluster Member as in High Availability interface mode.<br>The interface's status is still monitored, and if a problem occurs, the Cluster Member fails over to the other Cluster Member.</td></tr>
</table>
</td></tr>
<tr><td><b>IP Address</b></td><td>Cluster Virtual IP address configured on the interface.</td></tr>
<tr><td><b>Member IP Address</b></td><td>Physical IP address configured on the interface.</td></tr>
</table>

# Viewing the Cluster Status

### Procedure

1. Connect to the WebUI on a Cluster Member:

   ```
   https://<IP Address of the Cluster Member>:4434
   ```

   **Best Practice** - After the cluster is successfully configured, connect to `https://<Virtual IP Address of the Cluster>:4434`. This redirects you to the WebUI **Home** > **System** page for the active Cluster Member.

2. From the left navigation panel, click **Device**.
3. In the **Advanced** section, click the **High Availability** page.
4. Click **View diagnostics**.

### Cluster Notifications

Starting from R81.10.17, cluster notifications are generated by default in all failover instances:

- Automatic failovers.
- Manual failovers.
- Primary (Active) member is down.
- Primary (Active) member is back up.
- Standby (Secondary) member is down.
- Standby (Secondary) member is back up.

**Note** - Notifications are generated only from the current Active member and include:

- The reason for the failover.
- The Active member's previous and current state.
- The Standby member's current and previous state.

# Failing Over Manually

### Failing over from the Primary Cluster Member to the second Cluster Member

1. Connect to the WebUI on the primary Cluster Member:

   ```
   https://<IP Address of the Primary Cluster Member>:4434
   ```

2. From the left navigation panel, click **Device**.
3. In the **Advanced** section, click the **High Availability** page.
4. Click **Force Member Down**.

   A confirmation message appears.

5. Click **Yes**.
6. Cluster State:
   - The primary Cluster Member is now Down.
   - The second Cluster Member is now Active.
7. The primary Cluster Member logs you out from WebUI because it has to reload it (to show only the supported pages).

**Notes:**

- Only one Cluster Member can be down at a time.
  For the Cluster Member in the Down state, the **Force Member Down** button becomes **Disable Manual Failover**.
- If you want the primary Cluster Member to handle the traffic, you must fall back from the second Cluster Member to the primary Cluster Member.

### Falling back from the second Cluster Member to the Primary Cluster Member

1. Connect to the WebUI on the primary Cluster Member:

   ```
   https://<IP Address of the Primary Cluster Member>:4434
   ```

2. From the left navigation panel, click **Device**.
3. In the **Advanced** section, click the **High Availability** page.
4. Click **Disable Manual Failover**.

   A confirmation message shows.

5. Click **Yes**.

In **Primary Up** mode, the original primary Cluster Member is now the Active Cluster Member.

In **Active Up** mode, run **Disable Manual Failover** to make the member Standby.

# Resetting Cluster Configuration

### Procedure

1. Connect to the WebUI on one of the Cluster Members:

   ```
   https://<IP Address of the Cluster Member>:4434
   ```

2. From the left navigation panel, click **Device**.
3. In the **Advanced** section, click the **High Availability** page.
4. Click **Reset Cluster Configuration**.

ℹ **Important** - This deletes all cluster configuration settings from both Cluster Members. You must run the **New Cluster Wizard** again to configure the cluster.

# Upgrading a Cluster Manually

### Procedure

**Notes:**

- Only manual local upgrade is supported.
- Upgrade each Cluster Member individually.
- Start the upgrade on the Standby Cluster Member.
- After the upgrade, the appliance remains the Standby. You must failover and then upgrade the new Standby member.
- Start the upgrade on the new Standby Cluster Member (former Active).

1. Upgrade the current Standby Cluster Member:

   a. Connect to the WebUI on a Cluster Member:

   ```
   https://<IP Address of the Cluster Member>:4434
   ```

   b. From the left navigation panel, click **Device**.

   c. In the **Advanced** section, click the **High Availability** page.

   d. At the top of this page, examine the cluster state.

   If the current cluster state shows "**This gateway (<...>) is standby**", then continue to the next step.

   Otherwise, connect to the other Cluster Member

   e. In the **System** section, click the **System Operations** page.

   f. Click **Manual Upgrade**.

   The **Upgrade Software Wizard** opens.

   g. Follow the wizard instructions.

   h. After the upgrade, this appliance remains the Standby.

2. Upgrade the new Standby Cluster Member (former Active Cluster Member):

   a. Connect to the WebUI on the Cluster Member:

   ```
   https://<IP Address of the High Availability>:4434
   ```

   b. From the left navigation panel, click **Device**.

   c. In the **Advanced** section, click the **High Availability** page.

d. At the top of this page, examine the cluster state.

   Wait for the current cluster state to show "**This gateway (<...>) is standby**", and then continue to the next step.

e. In the **System** section, click the **System Operations** page.

f. Click **Manual Upgrade**.

   The **Upgrade Software Wizard** opens.

g. Follow the wizard instructions.

h. After the upgrade, this appliance remains as the Standby.

# Single Routable IP Cluster

, You can configure a Single Routable IP cluster where the virtual IP address is in a different subnet than the physical IP addresses of the Cluster Members. Only the virtual IP address is routable. Traffic sent from Cluster Members to internal or external networks is hidden behind the cluster Virtual IP address.

Advantages of using different subnets:

- Use only one public IP address for the cluster.
- Hide physical Cluster Members' IP addresses behind the cluster Virtual IP address.
- Create a cluster in an existing subnet that has a limited number of available IP addresses.

#### Prerequisites for both Cluster Members

- The Internet connection must be of type **Static**.
- The IP address of the Internet connection must be a fake, non-routable on the same subnet as the Internet Connection of the other member. For example, the IP address of the Internet connection of the first member is 4.4.4.4 with subnet of 255.255.255.0, and the IP address of the second member is subnet 255.255.255.0.
- When first configuring the Internet connection, you must configure a default gateway. This gateway IP address must be fake as well and in the same subnet as the Cluster Members' IP addresses. In our example, 4.4.4.1.
- You must turn off probe monitoring:
  1. Click **Edit** to open the **Edit Internet Connection** window > **Connection Monitoring** tab.
  2. Clear all probing checkboxes.

- You must turn off SD-WAN (supported starting from R81.10.10).

**Procedure**

1. Configure the primary and second Cluster Members as for a regular cluster (see *"Configuration Workflow" on page 222*) but with these differences:
   1. After you configure the second member:
      1. Go back to the primary (Active) member and click **Edit**.
      2. Set the **Default gateway** as the default gateway of the Virtual IP address subnet.
   2. For each Cluster Member, in the **Connection Monitoring** tab, click the checkboxes to restore the probing options.
   3. If SD-WAN is supported, turn it on.
2. Click **Save** to save your changes.

The related route to the Virtual IP address subnet shows in the Routing Table.

# Cluster Managed by Quantum Spark Management

You can configure a cluster in which both gateways are managed by the Quantum Spark Management service in Infinity Portal.

Connect to Quantum Spark Management after you configure the cluster.

A cluster supported by Quantum Spark Management is very similar to a Locally Managed cluster. One cluster member is Active, and the other cluster member is Standby. To change the status of the Active member, click **Force Member Down**.

## Connecting a Cluster Gateway to Spark Management

**Prerequisites:**

- An account in the Infinity Portal with the Spark Management application. See the *Quantum Spark Management Administration Guide*.
- Both gateways must have the same hardware, firmware (version and build), and licenses.
- The firmware version must be R81.10.15 and higher.
- The cluster is configured on the gateway level (see *"Configuration Workflow" on page 222*).

For more information on Cloud Services, see the *"Configuring Cloud Services" on page 51* page.

**Connecting a cluster to Spark Management for the first time**

The cluster is configured locally and not yet connected to Spark Management.

1. In Spark Management:
   a. Navigate to the **Gateways** page
   b. Create a new gateway object.
   c. In the **Gateway type** field, select **Spark Cluster**.
   d. Enter a name and select a plan.
   e. Create the cluster members objects in Spark Management. Each member represents a physical gateway member of the cluster.

      **Notes:**
      - You can create each member from the **New Gateway Wizard** page or later on the Cluster object in the **General** tab.
      - If you add the members later, click **Save** after you add both members.

f. Click **Finish**. You are redirected to the cluster's **General** tab

g. Copy the **HA activation key**.

2. On the active member of the cluster local WebUI:

   a. Navigate to **Home** > **Cloud Services.**

   b. Select the option **Manage with Spark Management.**

   c. Paste the HA activation key you copied from the Spark Management in the applicable field.

   d. Both members begin the Cloud Services activation process. In a few minutes the process completes and both members appear as connected.

### Converting a single gateway (connected to Spark Management to a cluster

The gateway was added and cluster configuration was completed on the local WebUI.

1. In Spark Management:

   a. Navigate to the **Gateways** page

   b. Create a new gateway object.

   c. In the **Gateway type** field, select **Spark Cluster**.

   d. Enter a name and select a plan. This is usually the same plan that is used by the single gateway.

   e. Create the cluster members objects in Spark Management

      - For the first member, click **Search** and select the relevant gateway.
      - For the second member, create a new gateway object to represent the second member of the cluster.

      **Notes:**
      - You can create each member from the **New Gateway Wizard** page or later on the Cluster object in the **General** tab.
      - If you add the members later, click **Save** after you add both members.

   f. Click **Finish**. You are redirected to the cluster's **General** tab

   g. Copy the **HA activation key**.

2. On the active member of the cluster local WebUI:

a. Navigate to **Home** > **Cloud Services**.

b. Change the **Cloud Management** mode to **Off** and click **Save**.

c. Select the **Manage with Spark Management** option.

d. Paste the HA activation key you copied from the Spark Management into the applicable field.

e. Both members begin the Cloud Activation process. In a few minutes the process completes and both members and appear as connected.

### Using cloud capabilities on a locally managed cluster

Enable the new Cloud capabilities for Extended Monitoring on a cluster that is managed locally.

1. On the active member local WebUI:

   a. Navigate to **Home** > **Cloud Services**.

   b. Select the **Use cloud capabilities** option and follow these steps:

      i. **Step 1** - Create an Infinity Portal account to connect the cluster. If you already have an account, skip this step.

      ii. **Step 2** - Get the token:

         i. Click the **Get token** link.

         ii. Log in to Infinity Portal with your credentials. If your user is affiliated with more than a single account, select the relevant account.

         iii. Copy the token.

      iii. **Step 3** – Paste the activation token into the applicable field.

   c. Both members begin the Cloud Activation process. In a few minutes the process completes and both members and appear as connected.

### Using cloud capabilities on a single gateway to convert the gateway into a cluster

A single gateway, with enabled Cloud capabilities for Extended Monitoring, is converted into a cluster. The gateway was added and cluster configuration was completed on the local WebUI.

- Option 1 - Reconnect to the Cloud as a cluster (Simple):
  1. Navigate to **Home** > **Cloud Services**.
  2. Change the **Cloud Management** mode to **Off** and click **Save**.
  3. Select the **Use cloud capabilities** option and follow these steps:
     a. **Step 1** - Create an Infinity Portal account to connect the cluster. If you already have an account, skip this step.
     b. **Step 2** - Get the token:
        i. Click the **Get token** link.
        ii. Log in to Infinity Portal with your credentials. If your user is affiliated with more than a single account, select the relevant account.
        iii. Copy the token.
     c. **Step 3** - Paste the activation token into the applicable field.
  4. Both members begin the Cloud Activation process. In a few minutes the process completes and both members and appear as connected.

     **Notes:**
     - In this method the logs history available locally on the appliance is not retained. The reason is that the gateway initiates a new unique connection with Cloud Services. To retain the logs, use Option 2.
     - To view the history, the data still exists when logging into to Spark Management application in the Infinity Portal

- Option 2 - Extend the single gateway to a cluster in Spark Management.

  **Note** - Even when you use the Cloud Capabilities option, Spark Management configuration for the gateway still exists.

  Follow the steps to convert a single gateway to a cluster:

  1. In Spark Management:
     a. Navigate to the **Gateways** page
     b. Create a new gateway object.
     c. In the **Gateway type** field, select **Spark Cluster**.
     d. Enter a name and select a plan. This is usually the same plan that is used by the single gateway.
     e. Create the cluster members objects in Spark Management
        - For the first member, click **Search** and select the relevant gateway.
        - For the second member, create a new gateway object to represent the second member of the cluster.

          **Notes:**
          - You can create each member from the **New Gateway Wizard** page or later on the Cluster object in the **General** tab.
          - If you add the members later, click **Save** after you add both members.
     f. Click **Finish**. You are redirected to the cluster's **General** tab
     g. Copy the **HA activation key**.
  2. On the active member of the cluster local WebUI:
     a. Navigate to **Home** > **Cloud Services**.
     b. Change the **Cloud Management** mode to **Off** and click **Save**.
     c. Select the **Manage with Spark Management** option.
     d. Paste the HA activation key you copied from the Spark Management into the applicable field.
     e. Both members begin the Cloud Activation process. In a few minutes the process completes and both members and appear as connected.

# Advanced Settings

The **Device** view > **Advanced** section > **Advanced Settings** page is for advanced administrators or *Check Point Support*.

You can configure values for multiple advanced settings for the various blades.

**Important** - Changing these advanced settings without fully understanding them can be harmful to the stability, security, and performance of this appliance. Continue only if you are certain that you understand the required changes. For further details regarding the attributes, consult with *Check Point Support* when necessary.

**Note** - Some attributes appear only in the Locally Managed mode.

## Filtering the List of Attributes

1. In the search field that shows **Type to filter**, enter the text.

   The table updates in real time.

2. To cancel the filter, click **X** next to the search string.

## Configuring the Attribute Values

1. Left-click an attribute to select.
2. Click **Edit**.

   The attribute window opens.

3. Configure the settings, or click **Restore Defaults** to reset the attribute to the default settings.
4. Click **Apply**

## Restoring Default Values

1. Above the table with attributes, click **Restore Defaults**.

   The **Confirm** window opens.

2. Click **Yes**.
3. All appliance attributes are reset to the default settings.

# Clarifications

This section contains clarifications for specific attributes.

| Attribute Name | Note |
|---|---|
| **Cluster Synchronization** | Starting from R81.10.15, you can select the **Synchronization** mode:<br>■ **Sync Enabled** - All kernel tables are synced, enabling seamless failover between members.<br>■ **Sync Disabled** - Kernel tables are not synced between the cluster members. This may lead to disrupted connections.<br>■ **Optimized Sync** - Syncs most kernel tables but not heavy kernel tables. In this mode, failover results in closed connections.<br>**Note** - VPN tunnels persist following failover.<br>The benefit of not synchronizing tables is improved performance. The downside is that upon failover you may need to re-initiate connections.<br>Switching to **Sync Enabled** or **Optimized Sync** mode requires a reboot of both cluster members. |
| **Two-Factor Authentication - Enable selection of target where to send the passcode (SMS/email)** | 1. Select or clear the checkbox:<br>■ **Cleared** - The appliance sends the OTP by SMS and by Email (this is the default).<br>■ **Selected** - After an end-user clicks "Connect" in their Remote Access VPN client, in the next window the end-user must enter a mobile phone number to get the OTP by SMS, or enter an email to get the OTP by Email.<br>2. Click **Apply**<br>**Note** - This setting does not affect the selection screen in the WebUI on the **VPN Remote Access Control** page. The user must still configure to receive the passcode through email, SMS, or both options. |
| All attributes, whose name starts with "**DSL globals**" | When all the ADSL standards are turned off in the **Advanced Settings**, and you can only connect using the VDSL2 standard, the VPI, the VCI, and the encapsulation options still appear, even though they are not used to open an Internet connection. |

# Changes Between Versions

This section describes changes in attributes in different R81.10.X versions.

| Attribute Name | Supported Versions |
|---|---|
| Managed Services - Disable logging to SD | R81.10.17 GA Replacement and higher |
| Remote Access VPN - Encryption algorithm used for Phase 2 | R81.10.17 GA Replacement and higher |
| WebUI settings and customizations - Enable where in use | R81.10.17 and higher |
| Cluster - Disable all non-synced interfaces | R81.10.15 and higher |
| System Settings - Allow access from any IP address | R81.10.15 and higher |
| OS advanced settings - Enable SIM switch on lower tech | R81.10.15 and higher |
| OS advanced settings - SIM switch on lower tech delay | R81.10.15 and higher |
| OS advance settings - SIM switch on lower tech lowest allowed tech | R81.10.15 and higher |
| OS advanced settings - Default routes rank | R81.10.10 and higher |
| Dr. Spark job | R81.10.08 and higher |
| Fonic settings - Mode | R81.10.08 and higher |
| OS advanced settings - Enable automatic WiFi channel change | R81.10.08 and higher |
| OS advanced settings - Enable GPS | R81.10.07 and higher |
| OS advanced settings - Enable Jumbo Frames | R81.10.07 and higher |
| USB Modem Watchdog - Enabled by Default | R81.10.05 and higher |
| Smart Accel Settings - Accel Trusted Https Domains Only | R81.10.05 and higher |
| Cluster - Synchronization | R81.10.05 and higher |
| Smart Accel Services - Security logs enabled | R81.10.05 and higher |
| Two-Factor Authentication - Enable selection of target where to send the passcode (SMS/email) | R81.10.05 and higher |

| Attribute Name | Supported Versions |
|---|---|
| **OS advanced settings - IPv6 prefix selection Mode** | R81.10.05 and higher |
| **VPN Site to Site global settings - IKEV2 Key Type** | R81.10.05 and higher<br>For more information on how to set up this connection, see the:<br>- *Harmony Connect Administration Guide*<br>- *Harmony Connect for SMB Gateways Integration Guide* |

# Managing the Access Policy

This section describes how to set up and manage your Quantum Spark appliance Access Policy.

## Configuring the Firewall Access Policy and Blade

These sections explain how to configure the Firewall Access Policy and Blades in a streamlined workflow. You can set the default Access Policy control level, set the default applications and URLs to block and allow secure browsing, and configure User Awareness.

Follow these steps to set up and manage your organization's security policy effectively.

### Getting Started with Firewall Access Policy Configuration

The **Access Policy** defines the security requirements for your firewall. It manages incoming, internal, and outgoing traffic and includes these components:

- **Firewall Policy** - Manages packet inspection rules.
- **Application & URL Filtering** - Controls Internet browsing and application usage.

**Follow these steps to configure and manage your organization's security policy:**

1. Go to the **Access Policy** view > **Firewall** section > **Blade Control** page to configure the Firewall Access Policy.

   This is the interface to define the default policy for incoming, internal, and outgoing traffic to and from your organization. Configurations in the **Firewall Blade Control** page are shown as automatically generated system rules at the bottom of the Rule Base.

2. To define manual rules that are exceptions to the default policy defined in this page, go to the **Firewall Policy** page. You can also define and view the rule based policy.

3. On the **Firewall Servers** page, define the default access policy for specific servers within your organization and manage the automatically generated system rules.

# Configuring the Firewall Access Policy

### Step 1: Set the Default Policy Level

1. Navigate to the **Access Policy** view > **Firewall** section > **Blade Control** page.
2. Select one of these options to set the default Access Policy:
   - **Strict** - Blocks all traffic unless explicitly allowed. Use this option for maximum security.

     In this mode, your policy can only be defined through the **Servers** page and by manually defining access policy rules in the **Access Policy** > **Firewall Policy page**.
   - **Standard** - Default option. Allows outgoing traffic and internal communication, and blocks incoming unencrypted traffic from untrusted sources.
   - **Off** - Disables the firewall and allows unrestricted traffic. Manually defined rules are not applied. Do not use this option in secured environments.

**Note** - When Cloud Services manages the blade, a lock icon shows. You cannot toggle between the on and off states. If you change other policy settings, the change is only temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

### Step 2: Customize outgoing services (Standard Policy only)

1. Click **all services**.
2. Select one of these:
   - **Block all outgoing services except the following** - Select which services to allow.
   - **Allow all outgoing services** - To allow all services.
3. Click **Save**.

### Step 3: Define Access Policy rules

1. Go to the **Access Policy** > **Blade Control** page.
2. Add manual rules for exceptions or specific requirements:
   - If no manual rules are configured, click the **Firewall Policy** link to add manual rules to the Firewall policy.
   - To view and modify existing rules, click **manual rules**.
3. Click **Servers** to see how many servers are defined in the appliance and to define server specific policies. A server object is an IP address that can have a specific access policy assigned to it.
   a. If no servers are configured, click **Add a server**.
   b. Define NAT rules if applicable (for example, port forwarding).
4. Automatically generated access rules to servers are created above the default policy rules and can be seen in the **Access Policy** > **Firewall Policy** page. You can also create exception rules for servers.

# Application & URL Filtering

In the Application & URL Filtering section you can define how to handle applications and URL categories on traffic from your organization to the Internet.

Application & URL Filtering are service based features and require Internet connectivity to download the latest signature package for new applications and to contact the Check Point cloud for URL categorization.

**Best Practice** - We recommend that you block browsing to security risk categories and applications by default.

You can configure additional applications and categories to block by default according to your company's policy. In addition, you can also select to limit bandwidth consumption by specific applications to improve bandwidth control.

**Step 1: Define Filtering Policies**

1. In the **Access Policy** > **Firewall** > **Blade Control** page, go to the **Application and URL Filtering** section.
2. Select the applicable options:
   - **Block security risk categories** - Block applications and URLs that can be a security risk and are categorized as spyware, phishing, botnet, spam, anonymizer, or hacking. This option is selected by default.
   - **Block inappropriate content** - Block Internet access to websites with inappropriate content such as sex, violence, weapons, gambling, and alcohol.
   - **Block file sharing applications** - Block file-sharing from typically illegal sources such as torrents and peer-to-peer applications.
   - **Block other undesired applications** - Click this option to manage your basic Application & URL Filtering policy. Manually add and block applications or categories of URLs to a group of undesired applications. You can also create a new URL or application if it is not in the database.

- **Limit bandwidth consuming applications** - Applications that use a lot of bandwidth can decrease performance necessary for important business applications. This option gives accelerated QoS (bandwidth control) for applications. When you select this option, P2P file sharing, media sharing, and media streams are selected by default but you can edit the group to add applications or categories that you want to limit with regards to the amount of bandwidth they consume.

  **Note** - You must indicate the maximum bandwidth limit according to your Internet connection upload and download bandwidth. Consult your ISP for this information. For the limit to be effective, it must be lower than the actual bandwidth supplied by your ISP. Upload and download bandwidths are usually not the same.

**Step 2: Enable URL Filtering Only (Optional)**

Use this mode to enforce rules based only on URL categories:

- Predefined applications are not blocked.
- Custom applications and URLs are enforced.

The default policy defined here is viewed as automatically generated rules in the bottom of the Outgoing traffic Rule Base in the **Access Policy** > **Policy** page.

# Tracking and Logs

**To configure traffic logging:**

1. On the **Access Policy Control** page, go to **Tracking**.
2. Specify the log options:
   - **Blocked traffic** - Options: **All**, **Outgoing**, **Incoming and Internal**
   - **Allowed traffic** - Options: **All**, **Outgoing**, **Incoming and Internal**

**Notes**:

- These settings apply to all the incoming and outgoing traffic blocked or accepted by the default Firewall and Application & URL Filtering automatically generated rules.
- These settings do not apply to automatically generated rules for VPN, DMZ, and wireless networks.

# User Awareness

Configure the appliance to enforce access control for individual users and groups and show user-based logs instead of IP address based logs.

**Procedure:**

1. Click **Configure** to set up how User Awareness recognizes users. When this is configured, you can see users in logs and also configure user based Access Policy rules.
   - If User Awareness is configured, the **Enable User Awareness** checkbox appears.
   - To disable User Awareness, clear the checkbox.
   - To make changes to the configuration, click **Edit settings**.
2. Use AD-based authentication for seamless user recognition.The user database and authentication are all done through the AD server. When a user logs in to the AD server, the appliance is notified. Users from the AD server can be used as the **Source** in Access Policy rules.

   To define an AD server, click **Active Directory servers**. You can also create an AD server is also available in the Edit settings wizard.
3. Enable Browser-Based Authentication for manually added local users.

   Users can be defined locally in the **Users & Objects** > **Users** page with a password. For the appliance to recognize the traffic of those users, you must configure Browser-Based Authentication and the specific destinations to which they must first be identified before accessing.

   Browser-Based Authentication is not usually used for all traffic but only for specific destinations because it requires the end user to log in manually through a dedicated portal.

# Updates

To ensure accurate URL categorization and application recognition, make sure your database is updated regularly.

**Procedure**

1. Verify the update status under **Application and URL Filtering > Update Status**.
   - **Up to date**
   - **Updated service unreachable** - This usually is due to a loss in Internet connectivity. Check your Internet connection in the **Device** > **Internet** page and contact your ISP if the problem persists.
   - **Not up to date** - A new update package is ready to be downloaded but the scheduled hour for updates did not yet occur. Updates are usually scheduled for off-peak hours (weekends or nights).
2. Schedule updates:
   a. Hover over the icon next to the update status and click **Schedule Updates**.

   b. Select the blades for which to schedule updates. You must manually update the rest of the blades when new updates packages are available and a **Not up to date** message is shown in the status bar at the bottom of the WebUI application.

   c. Select a **Recurrence** time frame:
      - **Hourly** - Enter the time interval for **Every x hours.**
      - **Daily** - Select the **Time of day**.
      - **Weekly** - Select the **Day of week** and **Time of day**.
      - **Monthly** - Select the **Day of month** and **Time of day**.

   d. Click **Save**.

## Additional Information

The Check Point Application Database contains more than 4,500 applications and 96 million categorized URLs.

Each application has a description, a category, additional categories, and a risk level. You can include applications and categories in your Application Control and URL Filtering rules. If your appliance is licensed for the Application Control & URL Filtering blades, the database is updated regularly with new applications, categories and social networking widgets. This lets you easily create and maintain an up to date policy.

You can see the Application Database from these links in the WebUI:

- **Block other undesired applications**
- **Applications & URLs** - This opens the **Users & Objects** > **Applications & URLs** page.
- **Check Point AppWiki** - Use this tool to search and filter the Application & URL Filtering Database.

# Working with the Firewall Access Policy

## Firewall Policy

In the **Access Policy** tab > **Firewall** section > **Policy** page you can manage the Firewall Rule Base. You can create, edit, delete, enable or disable rules.

In the **Access Policy** tab > **Blade Control** page you determine the basic firewall policy mode:

- In **Standard** mode, this page shows you both automatically generated rules based on the configuration of your default policy and manually defined rules as exceptions to this default policy.
- In **Strict** mode, all access is blocked by default and this page is the only way to configure access rules for your organization.

The Rule Base is divided into two sections. Each of the two sections represent a different security policy - how your organization browses to the Internet (the world outside your organization) and the security policy to access your organization's resources (both from within and from outside your organization). At the top of the page there are three links that let you see both or only one of the sections.

- **Outgoing access to the Internet** - For all outgoing traffic rules. In this Rule Base you determine the policy to access the Internet outside your organization. Commonly the policy here is to allow the basic traffic, but you can block applications and URLs based on your company's discretion. In the **Access Policy** > **Firewall Blade Control** page you can configure the default policy to block applications and URLs. This page lets you add manual rules as exceptions to the default policy. You can also **customize messages** that are shown to users for specified websites when they are blocked or accepted by the Rule Base (see below). You can also use an **Ask** action for applications or URLs that lets the end user determine whether browsing is for work related purposes or not. For example, we recommend you add a rule that asks the users before browsing to uncategorized URLs. Such a rule can disrupt possible bot attacks.
- **Incoming, internal and VPN traffic** - For all incoming, internal and VPN traffic rules. In this Rule Base, you determine the policy to access your organization's resources. All internal networks, wireless networks, **and** external VPN sites are considered part of your organization and traffic to them is inspected in this Rule Base. Commonly the policy here is to block traffic from outside your organization into it and allow traffic within your organization.

  In Standard mode, you can configure in various pages a more granular default policy:

  - **Traffic from specific sources into your organization** can be blocked or accepted by default. This configuration can be found in each specific sources' edit mode:

  - External VPN sites - Configure default access from/to **VPN** > **Site to Site Blade Control** page.
  - Remote Access VPN users - Configure default access from **VPN** > **Remote Access Blade** Control page.
  - Wireless networks - Configure default access for each wireless network from the Access tab in each wireless network's edit window in the **Device** > **Wireless Network** page.
  - DMZ network - Configure default access from the DMZ object's edit window in the **Device** > **Local Network** page.

    **Note** - DMZ is not supported in 1530 / 1550 appliances.

- **Traffic to defined server objects** as configured in each server's edit window in the **Access Policy** > **Firewall Servers** page.

  This page lets you add manual rules as exceptions to the default policy. In Strict mode, the default policy blocks everything and you configure access only through manual rules.

Within each section there are these sections:

- **Manual Rules** - Rules that you manually create.
- **Auto Generated Rules** - Rules that the system determines based on the initial Firewall Policy mode (Strict or Standard) as explained above. These rules are also influenced by other elements in the system. For example, when you add a server, a corresponding rule is added to the Incoming, internal and VPN traffic section.

These are the fields that manage the rules for the Firewall Access Policy:

| Rule Base Field | Description |
|---|---|
| No. | Rule number in the Firewall Rule Base. |
| Name | Rule name. |
| Hits | Displays the Hit Count, the number of connections that each security rule in the Access Rule Base matches during a specified time frame:<br>■ Number of hits for each rule<br>■ Percentage of hits for each rule<br>■ Relative hit count level - Zero (0 hits), Low (less than 10 percent of the hit count range), Medium (between 10-70 percent), High (between 70-90 percent) and Very High (above 90 percent). To see the relative level, hover your mouse to the left of the number in the Hit column<br>■ Time of the first hit for each rule<br>■ Time of the last hit for each rule<br>**To select the timeframe (1, 7 or 30 days):**<br>In the top toolbar of the **Outgoing Internet Access Rules** and the **Incoming, Internal and VPN Traffic,** click **More > Hit Count settings** > **Hit Count report time frame**.<br>**Note** - Days are calendar days, starting from 0:00 local time. |
| Source | IP address, network object, user group, or domain object that initiates the connection.<br>Starting in R81.10.15, you can have a maximum of 100 sources in the same rule. |
| Destination | IP address or network object that is the target of the connection.<br>Starting in R81.10.15, you can have a maximum of 100 destinations in the same rule. |
| Applications and Services | Applications, web sites and network services that are accepted or blocked. You can filter the list by common applications, categories, custom defined applications, URLs or groups. For more information, see *"Managing Applications & URLs" on page 457*.<br>This field is only shown in the Outgoing access to the Internet section.<br>Starting in R81.10.15, you can have a maximum of 100 applications and services in the same rule. |

| Rule Base Field | Description |
|---|---|
| Action | Firewall action that is done when traffic matches the rule: **Accept** or **Block**.<br>For outgoing traffic rules, you can use the **Customize messages** option to configure "Ask" or "Inform" actions in addition to the regular Block or Accept actions.<br>The messages shown can be set for these action types:<br>■ Accept and Inform<br>■ Block and Inform<br>■ Ask - The end user decides if this traffic is for work purposes or personal. See the **Customize messages** section below. Users are redirected to a portal that shows a message or question.<br>**Note** - Starting from R81.10.05, a policy rule with an application and action that redirects to the user portal (ask, block and inform, accept and inform) fails to redirect when SSL Inspection is on and the default bypass rule in the SSL Inspection Exception page is enabled.<br>If a time range is set for the rule, a clock icon is displayed. |
| Log | The tracking and logging action that is done when traffic matches the rule. |
| Comment / Auto generated rule | Details shown immediately below the above fields for:<br>■ Comments you enter when you create a rule.<br>■ Rules that the system automatically generates. You can click the object name link in the comment to open its configuration tab. |

### The "Ask" action

The outgoing Rule Base gives the option to set an **Ask** action instead of just allow or block for browser based applications. There are several commonly used cases where this is helpful:

- This action can be used for traffic that is normally not allowed in your organization, but you do want it to be available for work-related purposes. End users are asked if they need to browse for work-related purposes and can continue without requiring the administrator to make changes to the access policy for this single event. For example, traffic to Facebook is generally blocked but you want your HR department to be able to access it for work-related purposes.
- This action for traffic to uncategorized URLs can also give security against malware that managed to be installed inside your organization. Such malware is blocked by the Ask action.

## Configuring Access Rules

**To create a new manually defined access rule:**

1. Click the arrow next to **New**. When the page shows both Rule Bases, click **New** in the appropriate table.

2. Click one of the available positioning options for the rule:

   **Top Rule**, **Bottom Rule**, **Above Selected**, or **Under Selected**.

   The **Add Rule** window opens. It shows the rule fields in two ways:

   - A rule summary sentence with default values.
   - A table with the rule base fields in a table.

3. Click the links in the rule summary or the table cells to select network objects or options that fill out the rule base fields. See the descriptions above.

   **Note** - The **Application** field applies only to outgoing rules.

   In the **Source** field, you can optionally select between entering a manual IP address (network), a network object, a domain object, or a user group (to configure a user based policy, make sure the User Awareness blade is activated). Users can be defined locally on the appliance or externally in an Active Directory.

   For more details, see the **Access Policy** > **User Awareness Blade Control** page.

4. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule in the Access Policy.

5. To limit the rule to a certain time range, select **Apply only during this time** and select the start and end times.

6. In outgoing rules, to limit the download traffic rate, select **Limit download traffic of applications to** and enter the **Kpbs** rate.

7. In outgoing rules, to limit the upload traffic rate, select **Limit upload traffic of applications to** and enter the **Kpbs** rate.

8. In incoming rules, to match only for encrypted VPN traffic, select **Match only for encrypted traffic**.

9. Click **Apply**

   The rule is added to the outgoing or incoming section of the Access Policy.

### To clone a rule:

Clone a rule to add a rule that is almost the same as the one that already exists.

1. Select a rule and click **Clone**.
2. Edit the fields as necessary.
3. Click **Apply**

### To edit a rule:

**Note** - For Access Policy rules, you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**

### To delete a rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

### To enable or disable a rule:

- To disable a manually defined rule that you have added to the rule base, select the rule and click **Disable**.
- To enable a manually defined rule that you previously disabled, select the rule and click **Enable**.

### To change the rule order:

1. Select the rule to move.
2. Drag and drop it to the necessary position.

   **Note** - You can only change the order of manually defined rules.

# Updatable Objects

An updatable object is a network object which represents an external service, such as Office 365, AWS, Geo locations, and more. You can select from the list of updatable objects. The categories depend on the online service update.

External services providers publish lists of IP addresses or Domains or both to allow access to their services. These lists are dynamically updated. Updatable objects derive their contents from these published lists of the providers, which Check Point uploads to the Check Point cloud. The updatable objects are updated automatically on the Security Gateway each time the provider changes a list. There is no need to install policy for the updates to take effect.

For a list of currently supported objects, see sk173416.

You can import updatable objects to use in the firewall policy rules.

**To import an updatable object:**

1. In the **Firewall Access Policy** page, in the Rule Base, click **New**. If necessary, specify the rule order.
2. Click **Updatable objects** and select the objects you want.
3. Click **Import**.
4. Edit the rule so the source and destination use the specified countries.
5. Select the **Action** and **Log**.
6. **Optional** - Enter a comment.
7. **Optional** - Apply limitations such as time or traffic limits.
8. Click **Apply**.

## Customizing Messages

You can customize messages to let the Security Gateway communicate with users. This helps users understand that some websites are against the company's security policy. It also tells users about the changing Internet policy for websites and applications. When you configure such messages, the user's Internet browser shows the messages in a new window when traffic is matched on a rule using one of the message related actions.

These are the Action options and their related notifications:

| Rule Base action | Notifications |
|---|---|
| **Accept and Inform** | Shows an informative message to users. Users can continue to the application or cancel the request. |
| **Block and Inform** | Shows a message to users and blocks the application request. |
| **Ask** | Shows a message to users and asks them if they want to continue with the request or not. See above for more details. |

**To customize messages:**

1. Click **Customize messages** in the **Outgoing access to the Internet** section.
2. Configure the options in each of these tabs:
   - **Accept and Inform**
   - **Block and Inform**
   - **Ask**
3. Configure the applicable fields for each of the notifications:
   - **Title** - Keep the default or enter a different title.
   - **Subject** - Keep the default or enter a different subject.
   - **Body** - Keep the default or enter different body text. You can click **Optional keywords** for a list of keywords that you can add in the body text to give the user more information.
   - **Ignore text** (only for Ask) - This is the confirmation message for the Ask user message. Keep the default text or enter different text

- **User must enter a reason** (only for Ask) - Select this checkbox if users must enter an explanation for their activity. The user message contains a text box for entering the reason.
- **Fallback action** - Select an alternative action (Block or Accept) for when the notification cannot be shown in the browser or application that caused the notification, most notably in non-web applications. If it is determined that the notification cannot be shown in the browser or application, the behavior is:
  - If the Fallback action is **Accept** - The user can access the website or application.
  - If the Fallback action is **Block** - The Security Gateway tries to show the notification in the application that caused the notification. If it cannot, the website or application is blocked, and the user does not see a notification.
- **Frequency** - You can set the number of times that users get notifications for accessing applications that are not permitted by the policy. The options are:
  - **Once a day**
  - **Once a week**
  - **Once a month**

    For example, in a rule that contains in the Application - Social Networking category, if you select **Once a day** as the frequency, a user who accesses Facebook multiple times get one notification.
- **Redirect the user to URL** - You can redirect the user to an external portal, not on the gateway. In the **URL** field, enter the URL for the external portal. The specified URL can be an external system. It gets authentications credentials from the user, such as a user name or password. It sends this information to the gateway. Only applicable for the Block and Inform notification.

4. Click the **Customize** tab to customize a logo for all portals shown by the appliance (Hotspot and captive portal used by User Awareness). Click **Upload**, browse to the logo file and click **Apply**. If necessary, you can revert to the default logo by clicking **Use Default**.
5. Click **Apply**

# Defining Firewall Servers

In the **Servers** page you can see a list of servers defined in your system. You can create, edit, delete or search for server objects. Server objects are network objects that are defined with their access and NAT (if applicable) policies.

New server objects are created using a wizard:

- Step 1 - Select the server type.
- Step 2 - Define the server's details.
- Step 3 - Set up the server's access policy properties.
- Step 4 - NAT configuration (if relevant)

After you create a server, one or more corresponding rules are automatically generated and added to the Access Policy automatically and shown in the **Access Policy** > **Firewall Policy** page. The comment in the rule shows the object name. You can click the object name link in the comment to open the Access tab in the Server Properties.

An easier way to define server objects is by detecting them in the **Home** > **Active Devices** page and saving them as servers. For example, this option automatically detects the MAC address of the server making configuration easier.

During the wizard:

- Click **Cancel** to quit the wizard.
- Click **Next** to move to the next page of the wizard.
- Click **Back** to go to an earlier page of the wizard.
- Click **Finish** to complete the wizard.

### To create a new object:

Click **New**. The New Server Wizard opens and shows **Step1: Server Type**.

### Step 1: Server Type

1. Select the server type. There are built-in types for common servers.

   You can manually define a server that listens to any configured ports and you can also change a common server type's ports.

2. When selecting built-in types, you can optionally click Edit to edit the protocol ports.

3. When you select Other Server:

   - Select the Protocol (TCP, UDP, or both).
   - Enter the TCP/UDP Ports (enter port numbers and/or port ranges separated by commas, for example, 1,3,5-8,15).

### Step 2: Server Definitions

1. Enter a Name, IP address, and Comments (optional).

2. Select the options that apply to the server. For more information see **Users & Objects** > **Network Objects**.

   - Allow DNS server to resolve this object name - When the gateway is the DNS server for your internal networks the name of the server/network object will be translated to its IP address if this option is selected.
   - Exclude from DHCP service - The internal DHCP service will not distribute the configured IP address of this server/network object to anyone.
     - Reserve IP address in DHCP service for MAC - The internal DHCP service will distribute the configured IP address only to this server/network object according to its MAC address.
     - Enter the MAC address - This is required for IP reservation. When you create the object from the Active Devices page, the MAC address is detected automatically.

### Step 3: Access

1. Select the zones from which the server is accessible:
   - All zones (including the Internet) - Select this option to create a server that anyone from outside the organization can access. This option requires configuring how the server is accessible through NAT (in the next step).
   - Only trusted zones (my organization) - Select the applicable checkboxes. You can override these settings by adding manual access rules.
     - LAN - Physical internal networks.
     - Remote Access VPN users - Users that connect from their homes/mobile devices to the office.
     - Secure wireless networks - Password protected networks, not including guest networks.
     - DMZ - The network physically connected to the DMZ port when it is not used for a secondary Internet connection.

       **Note** - DMZ is not supported in 1530 / 1550 appliances.
     - Remote VPN sites - Networks defined behind gateways to remote VPN sites.
2. If you do not want the server to be accessible to pings, clear the Allow access to server in the ICMP (ping) checkbox.
3. Select the logging policy of traffic to the server:
   - Log blocked connections
   - Log accepted connections

### Step 4: NAT (when server is accessible from the Internet)

**The server's configured IP address (x.x.x.x) is public** - This option is only relevant if the **Hide internal networks behind the Gateway's external IP address** checkbox in the **Access Policy** > **NAT Control** page is cleared (see above for details). It means there are no NAT rules on the server.

When you complete the wizard, the server is added to the list of servers on the page and the automatically generated access rules are added to the **Access Policy** > **Firewall Policy** Rule Base.

**Note** - This page is available from the **Firewall** and **NAT** sections on the **Access Policy** tab.

# Defining NAT Control

In the **Access Policy** > **Firewall NAT** page you can configure NAT for outgoing traffic and see how many servers are defined in the system. Servers are defined in the **Access Policy** > **Servers** page and are network objects configured with their access and NAT settings. This lets you configure servers that are accessible from the Internet even if they do not have a routable IP address. You can also configure servers with NAT settings from this page.

**Note** - Locally Managed Quantum Spark Appliances support only one static NAT IP address of one real IP address. For more information, see sk179550.

**To disable NAT for outgoing traffic (Hide NAT):**

By default, NAT is configured for outgoing traffic. If it is necessary to disable NAT, make sure **Hide internal networks behind the Gateway's external IP address** is set to **OFF**.

**Important** - In most cases, if you turn off the hide NAT feature, you cause Internet connectivity issues. If your appliance is the gateway of your office to the Internet DO NOT set to off without consulting with networking experts.

**To configure a server that is routable from the Internet (server with NAT):**

1. Click **New Server (forwarding rule)**.
2. See the **Access Policy** > **Servers** page for instructions on how to use the server wizard.
3. In the Access step of the server wizard, select one of the options when asked from where this server is accessible.
4. In the NAT step of the server wizard, select the relevant option:
   - The gateway's external (public) IP address - This configures access through Port Forwarding. The appliance has an external routable IP address which is configured in its Internet connections (on the Device > Internet page). Traffic to the appliance to the ports configured for the server object in step 1 of the wizard is forwarded to the server. This allows traffic from the Internet into the organization (public servers) while still using one external routable IP address.
   - A different (public) IP address - This configures access through Static NAT. If a routable IP address was purchased for the server, enter it in the address field. While the rest of the internal network is hidden behind the gateway's external IP address, this specified server will use its own accessible IP address. Traffic to the specified IP address on relevant ports as configured in step 1 of the wizard will be forwarded to this server.
   - The server's configured IP address (x.x.x.x) is public - This option is only relevant if the Hide internal networks behind the Gateway's external IP address checkbox in the **Access Policy** > **NAT Control** page is cleared (see above for details). It means there are no NAT rules on the server.
5. When you have multiple internal servers that use the same port, select **Redirect from port** and enter a different port number that is used when you access this server from the Internet. Traffic to the server on the port you entered is forwarded to the server's port.
6. By default, the **Force translated traffic to return to the gateway** checkbox is selected. This allows access from internal networks to external IP addresses of servers through the local switch. The source is translated to "This Gateway". When the checkbox is cleared, the source is "Any" and there is no access from the internal network to external IP addresses through the switch.
7. Click **Finish**.

After you create a server with NAT settings, one or more corresponding rules are automatically generated and added to the NAT rules under the Auto Generated Forwarding Rules section. Click **View NAT rules** to see them. The comment in the rule shows the server object name. You can click the object name link to open the Access tab of the server's properties or click the Servers page link to go to the Firewall Servers page.

### Advanced - Manual NAT Rules

**Note** - For the majority of cases, manual NAT rules are not necessary. There is no need to use this option unless you are an experienced network administrator.

A more advanced way to configure address translation is by defining manual NAT rules. If servers with NAT are configured, the manual NAT rules do not apply to them. However, they apply even when Hide NAT is activated.

These are the fields that manage the NAT rules.

| Rule Base Field | Description |
|---|---|
| **Original Source** | The network object (a specified IP address) or network group object (a specified IP address range) that is the original source of the connections to translate.<br>**Note** - Updatable objects and FQDN can be used only as an original source. For more information on how to import, see *"Updatable Objects" on page 264*. |
| **Original Destination** | The network object (a specified IP address) or network group object (a specified IP address range) that is the original destination of the connections to translate.<br>**Note** - Updatable objects and FQDN can be used only as an original destination. For more information on how to import, see *"Updatable Objects" on page 264*. |
| **Original Service** | The original service used for the connections to translate. |
| **Translated Source** | The network object or network group object that is the new source to which the original source is translated. |
| **Translated Destination** | The network object or network group object that is the new destination to which the original destination is translated. |
| **Translated Service** | The new service to which the original service is translated. |

### To create a new NAT rule:

1. If the NAT rules table is not shown on the page, click the **View NAT rules** link.
2. Click the arrow next to **New**.
3. Click one of the available positioning options for the rule: **Top Rule**, **Bottom Rule**, **Above Selected**, or **Under Selected**.

   The Add Manual NAT Rule window opens. It shows the rule fields in two manners:

   - A rule summary sentence with default values.
   - A table with the Rule Base fields in a table.
4. Click the links in the rule summary or the table cells to select network objects or options that fill out the Rule Base fields. See the descriptions above.
5. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule in NAT Manual Rules.
6. Select the **Hide multiple sources behind the translated source addresses** if you want the original source to contain multiple IP addresses, IP ranges, networks, etc. and the translated source to be a single IP address.

   When this option is not selected, you can still use an IP range in the Original Source and a different IP range **of the same size** in the Translated Source. This rule does the IP address translation from one range to another, respectively (the first IP in the first range is translated to the first IP in the second range, and so on).
7. Select **Serve as an ARP Proxy for the original destination's IP address** for the gateway to reply to ARP requests sent to the original destination's IP address. Note that this does not apply to IP ranges or networks.
8. Click **Apply**

After you create manual rule, it is added to the NAT rules table under the Manual NAT Rules section.

### To edit a rule:

**Note** - For Access Policy rules, you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**

### To delete a rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

### To enable or disable a rule:

1. To disable a manually defined rule that you have added to the rule base, select the rule and click **Disable**.
2. To enable a manually defined rule that you have previously disabled, select the rule and click **Enable**.

### To change the rule order:

ℹ **Note** - You can only change the order of manually defined rules.

1. Select the rule to move.
2. Drag and drop it to the necessary position.

# SD-WAN

Starting in R81.10.10, SD-WAN feature is available in Locally Managed Quantum Spark appliances.

SD-WAN directs traffic for a specific application over a specific interface. It uses pre-configured recommended general settings, without the need for manual configuration. Traffic for specific applications uses different links to optimize the performance and utilization of all available links. Without SD-WAN, traffic is routed automatically based on the destination IP address.

SD-WAN is configured to use a primary ISP for most traffic, and a secondary ISP (for example, LTE) as a backup if the primary link fails.

On the **Access Policy** > **Firewall** section > **SD-WAN** page, you can configure the SD-WAN rules and monitor the traffic.

**Note** - SD-WAN for Centrally Managed appliances is available starting from R81.10.05. For more information, see the *Quantum SD-WAN Administration Guide*.

## Gateway Prerequisites

- More than one internet connection is configured.
- Connection to the internet.

## SD-WAN Known Limitations

- Smart SD-WAN does not support VTI.

  There are 4 possible workarounds:

  - Disable the SD-WAN blade.
  - Disable Smart SD-WAN and configure manual SD-WAN policy rules with the **Internet** object.
  - Configure manual SD-WAN policy rules for the VTI routes.
  - Add a new specific rule to the Routing Table that does not have "**Any**" as the source or destination.

    **Note** - In the route configuration, instead of selecting the `vpnt` interface, configure the VTI peer's IP address.

- SD-WAN Policy does not support Custom Applications.
- SD-WAN does not support Bond, Bridge, and Alias interfaces.
- SD-WAN does not support Internet Connections with IPv6 address configured.

# Getting Started with SD-WAN

1. **Configure at least two Internet connections**

   a. Connect to the appliance WebUI.

   b. From the left tree, click **Device**.

   c. In the middle pane, expand the section **Network** and click **Internet**.

d. Configure at least two internet connections - one for each ISP:

   i. Click **New**.

      The **New Internet Connection** window opens.

   ii. On the **Configuration** tab:

      i. In the **Connection name** field, enter the applicable name for this connection.

      ii. In the **Interface** field, select the applicable interface.

      iii. In the **Connection type** field, select the applicable type.

   iii. On the **Connection Monitoring** tab:

      Select **Automatically detect loss of connectivity to the default gateway**.

   iv. On the **Advanced** tab:

      i. Click **SD-WAN Settings** to expand the section.

      ii. In the **Upload speed (Mbps)** field, configure the values provided by the ISPs for the upload speed of the Internet connection. For example, Bezeq gives an upload speed of 100 MB.

      iii. In the **Download speed (Mbps)** field, configure the values provided by the ISP for the download speed of the Internet connection. For example, Bezeq gives a download speed of 1000 MB.

         SD-WAN uses all the links that meet the thresholds and fives weights proportionally to the configured upload/download speed.

      iv. Select the checkbox **This internet connection will be a part of SD-WAN**.

      v. For the checkbox **This internet connection will be set as backup in SD-WAN**, select this only for links that are expensive or of poor quality. For example, Cellular networks have a plan, and if you exceed your limit it can be costly. In the MPLS network, you pay per use.

   v. Click **Save**.

For more information see *"Configuring Internet Connectivity" on page 87*.

**Notes**:

- You can also configure a new SD-WAN connection on the **Access Policy** > **SD-WAN** page.
- To navigate directly from the **SD-WAN** page to the **Device** > **Internet** page, click **Manage and monitor links**.

2. **Configure the global SD-WAN Probing Settings**

   **Note** - The SD-WAN interfaces send ICMP Echo Requests to the specified destination. Based on the received ICMP Echo Responses, the appliance decides which ISP link (SD-WAN interface) to use.

   a. In the SD-WAN mode line (**SD-WAN blade is enabled**), click **Configure**.

   b. In the **First host** field, enter the IPv4 Address or Hostname for the first probing destination.

      The default is `dns.google.com`

   c. In the **Second host** field, enter the IPv4 Address or Hostname for the first probing destination.

      The default is `dns.cloudflare.com`

   d. In the **Third host** field, enter the IPv4 Address or Hostname for the first probing destination.

      The default is `dns.opendns.com`

   e. In the **Probing interval** field, enter the time between the probing packets (in milli-seconds).

      The default is 1000 msec (1 sec).

f. In the **Probing mode** field, select the applicable value.

The default is `Best`.

**Explanation**

This field controls which Internet connection the appliance selects in each steering object based on the probing mode:

- **Best** - Selects the Internet connection that has the best probing mode (the lowest values for the probing characteristics of packet loss, latency, and jitter). This is the default.
- **Average** - Selects the Internet connection that has the average probing mode.
- **Worst** - Selects the Internet connection that has the worst probing mode (the highest values for the probing characteristics of packet loss, latency, and jitter).

**Example:**

These two Internet connections are configured for SD-WAN - "WAN" and "DMZ".

There are three probing hosts (destinations) - "Host 1", "Host 2", and "Host 3".

The probing mode over the configuration probing interval are:

| | WAN | | | DMZ | | |
|---|---|---|---|---|---|---|
| **Probing Characteristic** | **Host 1** | **Host 2** | **Host 3** | **Host 1** | **Host 2** | **Host 3** |
| Packet Loss (%) | 1 | 1 | 4 | 2 | 3 | 7 |
| Latency (msec) | 1 | 1 | 4 | 2 | 3 | 7 |
| Jitter (msec) | 1 | 1 | 4 | 2 | 3 | 7 |

Where:

- The best probing mode was:
  - For "WAN": Packet Loss = 1, Latency = 1, Jitter = 1
  - For "DMZ": Packet Loss = 2, Latency = 2, Jitter = 2

- The average probing mode was:
  - For "WAN": Packet Loss = (1+1+4)/3 = 2, Latency = (1+1+4)/3 = 2, Jitter = (1+1+4)/3 = 2
  - For "DMZ": Packet Loss = (2+3+7)/3 = 4, Latency = (2+3+7)/3 = 4, Jitter = (2+3+7)/3 = 4
- The worst probing mode was:
  - For "WAN": Packet Loss = 4, Latency = 4, Jitter = 4
  - For "DMZ": Packet Loss = 7, Latency = 7, Jitter = 7

Therefore:

- If you select "**Best**", the appliance selects the Internet connection "WAN".
- If you select "**Average**", the appliance selects the corresponding Internet connection.
- If you select "**Worst**", the appliance selects the Internet connection "DMZ".

**Note** - If there is a tie between the Internet connections, the appliance selects an Internet connection based the configured **Link Utilization** (see below):

- If you selected the option **Link Aggregation**, the appliance uses all good interfaces.
- If you selected the option **Prioritize**, the appliance fails over and falls back between the Internet connections.

g. In the **Packet loss up to** field, enter the maximum acceptable packet loss in probing packets (in %).

   The default is 30%.

h. In the **Latency up to** field, enter the maximum acceptable latency in probing packets (in milli-seconds).

   The default is 200 msec.

i. In the **Jitter up to** field, enter the maximum acceptable jitter in probing packets (in milli-seconds).

   The default is 80 msec.

j. Click **Save**.

3. **Configure the Smart SD-WAN Prioritization of ISP Links**

ⓘ **Note** - After you configure multiple connections, you can only work in the High Availability mode.

a. From the left tree, click **Access Policy**.

b. In the middle pane, expand the section **Firewall** and click **SD-WAN**.

c. Scroll down until you see the tabs **Performance** and **Policy**.

d. Below the section **Custom Rules**, move the slider **Smart SD-WAN uses prioritize** to the right to enable this option.

e. On the right side of this slider, click **Configure**.

   The **Smart SD-WAN Settings** window opens.

f. In the **Link Utilization** section, select the Link Utilization method for Smart SD-WAN:

   - **Link Aggregation** - Selected by default. The appliance uses all SD-WAN interfaces that meet the threshold criteria.
   - **Prioritize** - The appliance uses the Internet connections based on the configured priority order.

     To change the priority order of connections:

     i. Click and hold the applicable table row.

     ii. Drag the table row up or down to the required position.

     iii. Release the mouse button.

     iv. Click **Save**.

4. **If necessary, configure custom SD-WAN rules**

   These rules configure a steering behavior for specific application traffic. The steering behavior determines how the appliance sends traffic to the Internet. The default behavior is Local Breakout. See *"Predefined Steering Behavior Objects" on page 285* and *"Configuring User-Defined Steering Behavior Objects" on page 285*.

   The appliance applies the rules in the order you put them in the policy.

a. Click **New**.

**Notes:**

- If you just click the **New** button, the appliance creates a rule at the bottom of this section. You can move it to the required position. You can click the downward arrow on the right side of the **New** button and select the applicable rule position in advance (**Top Rule**, **Bottom Rule**, **Above Selected**, **Below Selected**).
- You can edit, disable, and enable the rule after you create it.

b. In the New SD-WAN Rule window, select the applicable objects in these columns:

> **Important** - To select user-defined objects, you must create them before you create a new rule.
> This applies to:
>
> - Network Objects for hosts and networks (**Users & Objects** view > **Network Resources** > **Network Objects**)
> - Network Object Groups (**Users & Objects** view > **Network Resources** > **Network Object Groups**)
> - Applications (**Users & Objects** view > **Network Resources** > **Applications & URLs**)
> - Services (**Users & Objects** view > **Network Resources** > **Services**)
> - Service Groups (**Users & Objects** view > **Network Resources** > **Service Groups**)
> - Servers (**Users & Objects** view > **Network Resources** > **Servers**)
> - Steering Behaviors (**Access Policy** view > **Firewall** > **SD-WAN**) See *"Configuring User-Defined Steering Behavior Objects" on page 285*

- **Source**

    i. Click the **+** icon.

    ii. Click the applicable tab - **Networks** or **Updatable objects**.

    iii. Select the applicable objects.

    To select Updatable objects, click **Import** > select objects > click **Save**.

    iv. Click **Select**.

- **Destination**

    i. Click the **+** icon.

    ii. Click the applicable tab - **Networks** or **Updatable objects**.

    iii. Select the applicable objects.

    To select Updatable objects, click **Import** > select objects > click **Save**.

    iv. Click **Select**.

- **Applications / Services**
    1. Click the **+** icon.
    2. Click the applicable tab - **Common**, **Services**, or **Applications**.
    3. Select the applicable objects.
    4. Click **Select**.
- **Behavior**
    1. Click the **Default Breakout** object.
    2. Select the applicable steering behavior object.

c. Click **Save**.

d. To change the priority order of custom rules:

i. Click and hold the applicable table row.

ii. Drag the table row up or down to the required position.

iii. Release the mouse button.

5. **Monitor SD-WAN**

The middle section of the page shows the graph with all SD-WAN Internet connections.

Hover the mouse in the top part of the graph and click the applicable category:

- **Throughput**
- **Packet rate**
- **Connections**
- **All** (appears only for Throughput and Packet rate)
- **Inbound** (appears only for Throughput and Packet rate)
- **Outbound** (appears only for Throughput and Packet rate)
- **Real-time**
- **Trends** - Traffic over a specific time frame

In the Real-time view, hover the mouse on each Internet connection to see the tooltip with additional data - latency, jitter, and packet loss.

## Predefined Steering Behavior Objects

The appliance has several predefined Steering Behavior objects:

1. From the left tree, click **Access Policy**.
2. In the middle pane, expand the section **Firewall** and click **SD-WAN**.
3. Scroll down until you see the tabs **Performance** and **Policy**.
4. Click the **Performance** tab. This tab shows predefined steering objects and how they perform.
5. Click a predefined object to see its complete settings.
   - Icons of the applications this object uses.
   - Internet **SD-WAN** links this object uses.
   - Icons that show the state of each **SD-WAN** link.
   - When you hover on each **SD-WAN** link, the tooltip shows its quality (jitter, latency, packet loss).

   You cannot change the settings of the predefined objects.

## Configuring User-Defined Steering Behavior Objects

The appliance has several predefined Steering Behavior objects:

1. From the left tree, click **Access Policy**.
2. In the middle pane, expand the section **Firewall** and click **SD-WAN**.
3. Scroll down until you see the tabs **Performance** and **Policy**.
4. Click the **Policy** tab.
5. From the top toolbar, click **Manage Behaviors**.
6. From the top toolbar, click **New**.
7. In the **Name** field, enter a descriptive name.
8. **Optional**: In the **Comment** field, enter the applicable text.
9. In the **Thresholds** section, configure the required criteria for the steering behavior.

   **Available options**

   - Select **Predefined** and from the list, select the applicable category (each category has predefined thresholds).

- Select **Custom**, and configure the required thresholds:
  - **Jitter up to**
  - **Latency up to**
  - **Packet loss up to**

10. In the **Steering Candidates** section, select the required SD-WAN interfaces:

    **Available options**

    - Select **All relevant links** to use all SD-WAN interfaces.
    - Select **Specific links** and select the required SD-WAN interfaces (if there are three or more SD-WAN interfaces).

11. In the **Link Utilization** section, configure the required settings:

    **Available options**

    - Select **Link Aggregation** and select the algorithm how to use all SD-WAN interfaces:
      - **Connection hash** - Allocates connections to links based on a hash of their attributes, ensuring all packets of a connection follow the same path.
      - **Round robin** - Distributes connections to available links in a cyclical manner, aiming for a balanced but not necessarily bandwidth-optimized allocation.
      - **Proportionally to upload bandwidth** - Assigns connections to links in proportion to the links' upload bandwidth, optimizing for efficient bandwidth utilization.
      - **Proportionally to download bandwidth** - Allocates connections to links based on their download capacities, aiming to optimize inbound bandwidth usage.
    - Select **Prioritize** and configure the priority order of SD-WAN interfaces (drag and drop to change the order). This option is available when you configure two or more SD-WAN interfaces.

12. In the **Probing** section, you can override the global probing settings.

    The appliance sends pings to all configured hosts in parallel and measures the ISP link quality based on jitter, latency, and packet loss.

    a. Enter the applicable destination IP address or hostname for the **First host**, **Second host**, **Third host**.

   b. In the **Probing mode** field, select the applicable result from these options: **Best**, **Average**, **Worst**.

13. Click **Save**.

# Static Routes and SD-WAN

**Explanation**

When SD-WAN is enabled on the appliance (this is the default), SD-WAN routing decision takes priority over all static routes (configured in the **Device** view > the **Advanced Routing** section > the **Routing Table** page) that send traffic through **Internet Connections**.

This is the default SD-WAN configuration:

1. The **SD-WAN** blade is enabled.
2. Each **Internet** connection is enabled for SD-WAN.

If you do **not** want to use SD-WAN, then to send traffic through Internet Connections based on the configured static routes, follow one of these options:

- Disable the **SD-WAN** blade:

  **Note** - This completely disables SD-WAN on the appliance.

  1. Click the **Access Policy** view > in the **Firewall** section, click the **SD-WAN** page.
  2. At the top of the page, move the slider to the left position (near the text "**SD-WANblade is enabled**").

- In each specific **Internet** connection, clear the option **This Internet connection will be a part of SD-WAN**:

  **Note** - Use this option to disable SD-WAN only in a specific interface and keep using SD-WAN with other interfaces.

  1. Click the **Device** view > in the **Network** section, click the **Internet** page.
  2. Select the Internet connection and click **Edit**.
  3. Go to the right tab **Advanced**.
  4. Expand the last section **SD-WAN Settings**.
  5. Clear the option **This Internet connection will be a part of SD-WAN**.

# Configuring a cluster when SD-WAN is enabled

When you configure a cluster of Quantum Spark Gateways in this scenario:

- The external interfaces on the cluster members must be configured with private IP addresses
- The external Cluster Virtual IP address must be a public IP address
- The external Cluster interface must be configured as an SD-WAN interface

The probing of external servers cannot work until you configure the public Cluster Virtual IP address.

**We recommend this workflow to avoid the SD-WAN probing failure during the cluster configuration:**

1. For each Internet connection that will configured as a Cluster interface:
   - Disable the probing
   - Disable SD-WAN
2. Configure the cluster.
3. For each Internet connection was configured a Cluster interface:
   - Enable the probing
   - Enable SD-WAN

# Advanced - Creating and Editing NAT Rules

In the **Access Policy** > **NAT Manual Rules** page you can create and edit custom NAT rules. If servers with NAT are configured the manual NAT rules do not apply to them. However, they do apply even when Hide NAT is activated.

**Note** - For the majority of cases, manual NAT rules are not necessary. There is no need to use this option unless you are an experienced network administrator. See the **Access Policy** > **NAT Control** page for the commonly used options.

These are the fields that manage the NAT rules.

| Rule Base Field | Description |
|---|---|
| **Original Source** | The network object (a specified IP address) or network group object (a specified IP address range) that is the original source of the connections to translate. |
| **Original Destination** | The network object (a specified IP address) or network group object (a specified IP address range) that is the original destination of the connections to translate. |
| **Original Service** | The original service used for the connections to translate. |
| **Translated Source** | The network object or network group object that is the new source to which the original source is translated. |
| **Translated Destination** | The network object or network group object that is the new destination to which the original destination is translated. |
| **Translated Service** | The new service to which the original service is translated. |

#### To create a new NAT rule:

1. Click the arrow next to **New**.
2. Click one of the available positioning options for the rule: **On Top**, **On Bottom**, **Above Selected**, or **Under Selected**.

   The Add Rule window opens. It shows the rule fields in two manners:

   - A rule summary sentence with default values.
   - A table with the rule base fields in a table.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the Rule Base fields. See the descriptions above.
4. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule in NAT Manual Rules.
5. Select the **Hide multiple sources behind the translated source address/es** if you want the original source to contain multiple IP addresses, IP ranges, networks, etc. and the translated source to be a single IP address.

   When this option is not selected, you can still use an IP range in the Original Source and a different IP range **of the same size** in the Translated Source. This rule does the IP address translation from one range to another, respectively (the first IP in the first range is translated to the first IP in the second range, etc.).
6. Click **Apply**

#### To edit a rule:

**Note** - For Access Policy rules, you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**

#### To delete a rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

**To enable or disable a rule:**

- To disable a manually defined rule that you have added to the rule base, select the rule and click **Disable**.
- To enable a manually defined rule that you have previously disabled, select the rule and click **Enable**.

**To change the rule order:**

1. Select the rule to move.
2. Drag and drop it to the necessary position.

**Note** - You can only change the order of manually defined rules.

# Inspecting VoIP Traffic

## Introduction

Voice over Internet Protocol (VoIP) is a technology to deliver voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. There are two primary delivery methods: private or on-premises solutions, or externally hosted solutions delivered by third-party providers.

Inspection of VoIP traffic is supported on all Quantum Spark appliances.

**To configure VoIP inspection in the WebUI:**

1. Go to **Access Policy** > **VoIP**.
2. Click **On**.

   If VoIP is already configured, you can edit the current configuration.
3. **For the next sections, click the downward arrow to expand.**
4. Click the **Off-premise SIP Provider Service** heading to expand the section.

   Configure the applicable settings:

   a. Click the checkbox for **Use SIP Provider** - The available network objects are shown in a table with a Group name. You can select a single IP or a range of servers with external IP address.

   b. To add a new IP address, click **New**. To remove an IP address, select it and click **Remove**.

   c. Select or clear the option **Log traffic from this provider**.

   d. Select or clear the option **Disable SIP traffic inspection**.

      When you select this option, you allow the application level inspection and NAT for the SIP traffic.

      When you clear this option:

      - You must configure the RTP ports manually.
      - The timeout for UDP SIP connections (the "SIP_UDP" service) is the same as the default timeout for TCP SIP connections (the "SIP_TCP" service).

        **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

e. Select to **Enable bidirectional traffic** when the SIP provider is defined. This allows bidirectional traffic with the SIP service provider.

   If the service does not accept replies, bidirectional traffic is not established. A popup window opens and asks if you want to continue.

5. Click the **On-premise Devices** heading to expand the section.

   The network objects appear in a table, with a Group name.

   Click **New** to add an item.

   Select an item and click **Remove** to delete it.

   Configure the applicable settings.

   - **Use on-premise phones without SIP server (PBX)**.

     When no SIP Server Provider is defined, you do not need to define IP addresses for on-premises phones.

   - **Allow access to PBX management portal from the Internet**.

6. Click the **Off-premise phones** to expand the section.

   **Note** - The relevant topology shows automatically for each selection.

   Select one or more of these options:

   - **Phones are connected via VPN Site to Site**.
   - **Phones are connected by VPN Remote Access**.
   - **Phones are configured with public IP**.

     The network objects appear in a table, with a Group name.

     Click **New** to add an item.

     Select an item and click **Remove** to delete it.

7. Click the **SIP Service** heading to expand the section.

   Select the **SIP UDP/TCP ports**, which by default are 5060.

   All phones should be configured to use the configured ports.

   Click **New** to add a new SIP service.

   Click **Remove** to delete a service.

After you apply these settings, rules are automatically created in the **Firewall Access Policy** page for **Outgoing access to the Internet** and **Incoming, Internal and VPN traffic**.

**Notes:**

- For an on-premises configuration without PBX, the destination should be the `IP_Phones` object.
- If you allow access to the PBX portal, another rule is created:

| Source | Destination | Application / Service | Action | Log | Comment |
|---|---|---|---|---|---|
| Any | PBX-Server | HTTP/S | Accept | None | Generated rule: SIP VOIP |

Forwarding rules are automatically created in the **Access Policy** > **NAT Rules** page.

**Note** - For external phones with remote access, the Office Object is automatically created in the **Network Objects** section and the "`set back connection`" setting is set to "`true`".

Follow these configuration procedures to allow SIP traffic to pass through the gateway when:

- The SIP server is located on external networks. For more advanced topologies, refer to sk113573.
- The gateway's NAT configuration is set to its default settings (with internal networks hidden behind its external IP address).

## Configuration

**To allow the SIP server to connect to internal phones from the Internet:**

1. Go to **Access Policy** > **Policy**.
2. Add a rule to the **Incoming, Internal and VPN traffic** Rule Base that allows SIP traffic:

| Source | Destination | Application / Service | Action | Log |
|---|---|---|---|---|
| A network object that holds the IP address of the SIP server | A network object that holds the IP addresses of the phones behind the gateway | SIP | Accept | Select the applicable option |

For more information, see *"Working with the Firewall Access Policy" on page 258*.

# Smart Accel

On the **Smart Accel** page (versions R81.10.10 and lower), you can bypass the network inspection for specific objects:

- **Services** - Includes Corporate Services, Media Streaming Services, Social Media Services, and Web Conferencing applications.
- **Assets** - Devices such as a computer, audio player, or alarm (from R81.10.05).

This improves connectivity and optimizes the load on the Quantum Spark Security Gateway.

**Important** - You cannot use Smart Accel and SSL Inspection at the same time.

## Configuring Smart Accel in R81.10.05 and higher

### Smart Accel for Services

**To enable Smart Accel for Services**

**Note** - Smart Accel for Services is enabled ("On") by default.

1. Go to the **Access Policy** view > **Firewall** section > **Smart Accel** page.
2. In the section **Smart Accel Services**, click the **Off** toggle.

   Wait for the toggle to change to **On**.
3. To the right of the **On/Off** toggle, click the **services** link that appears in one of these sentences:
   - **All services selected**
   - **X/Y services selected**

   The **Smart Accel Services** window opens.

   By default, all the services are selected.
4. If it is necessary to **inspect** a service, then **clear** its checkbox.

   If it is necessary to **bypass** the inspection for a service, then **select** its checkbox.
5. Click **Apply**

**To disable Smart Accel for Services**

1. Go to the **Access Policy** view > **Firewall** section > **Smart Accel** page.
2. In the section **Smart Accel Services**, click the **On** toggle.

Wait for the toggle to change to **Off**.

## Smart Accel for Assets

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

### To enable Smart Accel for Assets

**Note** - Smart Accel for Assets is disabled ("Off") by default.

1. Go to the **Access Policy** view > **Firewall** section > **Smart Accel** page.
2. In the section **Smart Accel Assets**, click the **Off** toggle.

   Wait for the toggle to change to **On**.
3. To the right of the **On**/**Off** toggle, click the **assets** link that appears in one of these sentences:
   - **All assets selected**
   - **X/Y assets selected**

   The **Smart Accel Services** window opens.

   By default, none of the assets are selected.
4. If it is necessary to **inspect** an asset, then **clear** its checkbox.

   If it is necessary to **bypass** the inspection for an asset, then **select** its checkbox.
5. Click **Apply**

### To disable Smart Accel for Assets

1. Go to the **Access Policy** view > **Firewall** section > **Smart Accel** page.
2. In the section **Smart Accel Assets**, click the **On** toggle.

   Wait for the toggle to change to **Off**.

### To see devices, for which Smart Accel bypasses the inspection

1. Go to the **Access Policy** view > **Firewall** section > **Smart Accel** page.
2. In the section **Smart Accel Assets**, click the **Bypass by MAC** link.
3. WebUI opens the **Logs & Monitoring** view > **Status** section > **Active Devices** page.

# Configuring Smart Accel in R81.10.00

### To enable Smart Accel

1. Go to the **Access Policy** view > **Firewall** section > **Smart Accel** page.
2. Click the **On** toggle.
3. To the right of the **On**/**Off** toggle, click the **services** link that appears in one of these sentences:
   - **All services selected**
   - **X/Y services selected**

   The **Smart Accel Services** window opens.

   By default, all the services are selected.
4. If it is necessary to inspect a service, then **clear** its checkbox.
5. Click **Apply**
6. At the bottom of the page, click **Apply**.

### To disable Smart Accel

1. Go to the **Access Policy** view > **Firewall** section > **Smart Accel** page.
2. Click the **Off** toggle.
3. At the bottom of the page, click **Apply**.

# Fast Accel

The **Fast Accel** page appears in the WebUI of appliances running version R81.10.15 and higher. For version R81.10.10 and lower, see the **Smart Accel** page.

On the **Access Policy** view > **Firewall** section > **Fast Accel** page, you can bypass the network (HTTPS) inspection for:

- Services - Includes Corporate Services, Media Streaming Services, Social Media Services, and Web Conferencing application (in the **Smart Accel** section).
- Selected Network objects (in the **Bypass** section).

This improves connectivity and optimizes the load on the Quantum Spark Security Gateway

## Smart Accel

Smart Accel is on by default. To stop acceleration (bypass traffic inspection), click the radio button **Off**.

In the **Smart Accel** section, select the radio button to accelerate:

- **All services**
- **Specified services**

**To edit the services:**

1. Click **Modify**.
2. In the **Select Smart Accel Services** window, clear or select the relevant services checkboxes.
3. Click **Save**.

## Bypass

In this section, you can specify for which objects to bypass SSL and Firewall policy traffic inspection.

**Use case** - If you have connectivity issues in your office and want to understand the cause (which device), bypass inspection for a particular asset to see if this speeds up packet transmission. Note that bypassing inspection makes the network less secure.

**Bypass all traffic on untrusted network** is enabled by default. You can only disable this option if you enable to bypass traffic inspection for specified objects.

**To add an object to the bypass traffic inspection list:**

1. Move the toggle button next to **Bypass specified objects** to enable bypass traffic inspection for specified objects.
2. Click **Add**.
3. Select the object type:

   **Note** - In addition to selecting an object, you can also create a new object just like on the **Network Objects** page.

   - **Interface** - Select the relevant interface and click **Save**.
   - **IP range** - Select the IP range object and click **Save**.
   - **Asset type** - Select or clear the checkboxes for the relevant assets, for example computer or smart TV, and click **Save**.

     **Note** - All connected assets are listed here and on the **IoT** page.

   - **Single asset** - Specify the device by its MAC address.
     a. In the **New Device Object** window, enter the **Host MAC address**.
     b. Select one of these options:
        - **Use Fast Accel to bypass the host with this MAC address**
        - **Bypass the host with this MAC by SSL Inspection**

     c. Click **Save**.
4. Click **Save**.

**To delete an object from the bypass list:**

Select the item in the table and click **Delete**.

# IoT Protect

IoT devices are often targeted by cyber criminals as these devices may have limited security features. Quantum Spark gateways provide IoT discovery which identifies IoT devices at the customer site and then protects these devices from being compromised.

The **Access Policy** > **Firewall** > **IoT** page shows the automatic policy enforcement for each IoT asset type. All connected devices are automatically displayed on the **Home** > **Monitoring** > **Assets** page. The **IoT** page shows only the IoT devices.

When you enable the **IoT** blade on the appliance, it recognizes each IoT device that connects to the Security Gateway and automatically enforces practices in the preconfigured **IoT** policy.

IoT is enabled by default.

You do not need to configure the policy for each **IoT** device that connects to your appliance.

General rules for **IoT** are preconfigured. For example, the appliance always allows traffic to some domains, and always blocks traffic to other domains. You can make some changes to the policy.

## Getting Started

1. Go to **Access Policy** > **Firewall** > **IoT**.
2. Move the **IoT Protection** slider to **Enable**.
3. **Optional**: Configure advanced policy settings:

a. Click **Advanced policy settings.**

b. Configure the applicable options:

- **Monitor Mode** - Move the slider to enable Monitor Mode for cleanup rule.
- **Newly discovered functions** - Select the policy for newly discovered assets:
  - **Always prevent**
  - **Always detect**
  - **Define IoT mode per function** - You can define the policy per IoT type (function) instead of according to the recommended default.

    **Note** - The default setting for IP cameras and printers is to block traffic which is not part of the IoT policy. For other devices the default is monitor or **Exclude from IoT policy** (IoT policy is disabled).
- **DNS servers to trust** - If the host uses a DNS server which is not the gateway or used by the gateway. Create DNS objects and select **Trust custom DNS servers**. You can also select **Trust all DNS** but this is less secure.
- **Update Practices Now** - The IoT**practice** refers to the policy established by the vendor for an IoT asset. When the vendor updates the policy, the user is notified as part of the periodic updates or can click here to receive an immediate update.

c. Click **Save**.

4. Connect the IoT device to your local network. The appliance automatically recognizes this IoT device and applies the IoT policy to its traffic.

# Monitoring

If the user has multiple IoT devices, it may take a few minutes until the **Home** > **Monitoring** > **Assets** page shows all of the devices.

The same counters on the **Assets** page also appear on the **Home** > **Monitoring** >**IoT** page, with an additional graph for the policy and functions.

When you enable monitoring on an asset, the gateway pings the asset. If the ping fails during the set period of time (default is 2 minutes), a notification is sent.

The devices are grouped according to family. For each family, you can see the policy and drill down to see the vendors, domains, and other information. Click the **Assets graph** on the far right of the page and filter for type.

For example, an IP camera may show multiple assets from a number of different vendors. The policy details include:

- **Access from the internet** - Domains that attempt to connect to your device. Options: **Prevent**, **Monitor**, **Block**, **Exclude from IoT policy**.
- **Access to the internet** - Domains to which your device attempts to connect. Options: **Prevent**, **Monitor**, **Block**, **Exclude from IoT policy**. For IP cameras and printers, the default is **Prevent** but for other devices the default is **Monitor**. For some devices (for example, smart TV), access to the internet is disabled.
- **Approved destinations** - To add a new destination to the approved list, enter a value and click the **+**.
- **Log traffic for this asset** - Send logs for this device or not.

## Configuring

The IoT rules appear on the **Access Policy** > **Firewall Policy** page. General rules for IoT are preconfigured. For example, there are some domains that are always allowed, and some domains that are always blocked. All attempts appear in the logs, and you can receive notifications of this activity.

The policy rules show which domains are allowed. A request to access a blocked domain is dropped. You can make these changes to the policy:

- Do not drop traffic but do monitor if an asset attempts to access a site you do not want it to access.
- Prevent traffic. All domains are now blocked except for the domain where you send the logs.
- Add a custom destination to the allowed domain services. For example, if you want the printer to upload photos to Google Cloud, you can add this destination.

## Limitations

- Approved destinations in IoT support only a single IP address or a single domain. It is not possible to add an approved destination for a specific port or a service.
- IoT Protect for SMB is not supported on Rugged models: 1570R, 1575R, and 1595R.Quantum Rugged supports IoT Protect for Enterprise (see the table below for comparison between the two IoT models).
- If IoT is behind an Access Point (AP) or a Layer 3 device, configure it as a Layer 2 device. Otherwise, IoT policy is not applied on the hosts behind the Layer 3 device.
- IoT policy is not enforced on IPv6 traffic.

**IoT Protect Options**

| Feature | IoT Protect for Enterprise (Centrally Managed) | IoT Protect for SMB (Locally Managed) |
|---|---|---|
| Supported gateways | Quantum Force, Quantum Spark, Quantum Rugged | Quantum Spark |
| IoT Device Discovery | Full | Full |
| OT Device Discovery | Partial (Full using 3rd-party integration vendors) | Partial |
| Medical Device Discovery | No (Full using 3rd-party integration vendors) | No |
| UI | Infinity Portal | Local Spark UI and SMP |
| Cost | Requires add-on license<br>(e.g. CPSB-IOTP-1575R-1Y) | Included with all SNBT service bundles |
| Policy Enforcement | Yes | Yes |
| 3rd-Party Integrations | Yes | No |
| Minimum Version | R81.10.08 | R81.10.10 |
| Risk Analysis | Yes | No |
| Playblocks Integration | Yes | No |

# Working with User Awareness

In the **User Awareness** page you can turn the blade on or off and use the configuration wizard to configure sources to get user identities for logging and configuration purposes.

User Awareness lets you configure the Quantum Spark Appliance to show user based logs instead of IP address based logs and enforce access control for individual users and user groups.

## Workflow

1. Turn on the User Awareness Software Blade.
2. Click the **Configuration wizard** to enable and configure the blade.
3. Select the identification methods to get information about users and user groups and configure the identity sources.
4. After initial configuration, you can select the **Active Directory Queries**, **Browser-Based Authentication**, or **Identity Collector** checkboxes in the **Policy Configuration** section and click **Configure** for more advanced settings.
5. After the gateway acquires the identity of a user, you can enforce user-based rules on the network traffic in the Access Policy.

## Identity Sources

User Awareness can use these sources to identify users:

- **AD Query** (Active Directory Queries) - Seamlessly queries the Active Directory servers to get user information.

  The Quantum Spark Appliance registers to receive security event logs from the AD domain controllers when the security policy is installed. This requires administrator privileges for the AD server. When a user authenticates with AD credentials, these event logs are generated and are sent to the Security Gateway. The Quantum Spark Appliance can then identify the user based on the AD security event log.

- **Browser-Based Authentication** - Uses a portal to authenticate either locally defined users or as a backup to other identification methods.
  - Browser-Based Authentication uses a web interface to authenticate users before they can access network resources or the Internet. When users try to access a protected resource, they must log in to a web page to continue. This identifies locally defined users or users that were not successfully identified by other methods.

- You can configure the Browser-Based Authentication to appear for all traffic. This identification method is commonly configured to appear when you access only specific network resources or the Internet to avoid the overhead required from end users when they identify themselves.
- For traffic that is not HTTP based, you can also configure that all unidentified users are blocked from accessing the configured resources or Internet until they identify themselves first through the Browser-Based Authentication.

- **Identity Collector** - Collects information about identities and their associated IP addresses and sends it to the Security Gateway for identity enforcement.

  **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

## Enabling User Awareness

1. Select the **On** or **Off** option.

   **Note** - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

2. Click the **Configuration wizard** link.

   The **User Awareness Wizard** opens.

3. Select one or more user identification methods and click **Next**.
4. Follow the rest of the steps and click **Finish**.
5. After initial configuration, you can select the **Active Directory Queries** or **Browser-Based Authentication** checkboxes under Policy Configuration and click **Configure** to configure more advanced settings.

## Active Directory Queries:

If you have an existing Active Directory server, click **Use existing Active Directory servers**.

**To add a new Active DirectoryDomain:**

1. Select **Active Directory Queries** and click **Configure**.

   The **Active Directory Queries** window opens.

2. Select **Define a new Active Directory** server.
3. Enter:

- **Domain**
- **IPv4 address**
- **IPv6 address**
- **User name**
- **Password**
- **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually.

4. To select user groups from specific branches, select the checkbox **Use user groups from specific branch only**.

   Click **Add** and enter a branch path in the **AD Branch** field.

5. Click **Apply**

You can also add a new AD Domain in the **Users & Objects** > **Authentication Servers** page.

### Configuring User Awareness to use NTLMv2 protocol for Active Directory Queries

**Follow one of these procedures:**

**In WebUI:**

1. Connect to the WebUI on the Quantum Spark Gateway / each Cluster Member.
2. Click the **Device** view > **Advanced section** > **Advanced Settings** page.
3. In the top search field, enter: `ntlm`
4. Double-click the parameter **User Awareness - Use NTLMv2 protocol for Active Directory Queries**.
5. Select **Use NTLMv2 protocol for Active Directory Queries**.
6. Click **Save**.

**In Gaia Clish**:

1. Connect to the command line on the Quantum Spark Gateway / each Cluster Member.
2. If the default shell is the Expert mode, go to Gaia Clish:

   ```
   clish
   ```

3. Run:

   ```
   set user-awareness advanced-settings use-ntlmv2 true
   ```

# Browser-Based Authentication

### Blocking unauthenticated users

1. To block access for unauthenticated users when the portal is not available, select **Block unauthenticated users when the captive portal is not applicable**.

   This configuration option forces users using non-HTTP traffic to log in first through Browser-Based Authentication.

2. Select if unidentified users are redirected to Captive Portal for **All traffic** or **Specific destinations**.

   In most cases, all traffic is not used because it is not a seamless identification method.

3. Under Specific destinations, select **Internet** or **Selected network objects**.

   If you select **Selected network objects**, select the objects from the list or create new objects.

4. Click **Finish**.

### To edit settings and configure portal customization for Browser-Based Authentication

1. Under **Policy Configuration**, select **Browser-Based Authentication** and click **Configure**.
2. In the **Identification** tab, you can edit settings configured in the wizard if necessary.
3. In the **Customization** tab, select the relevant options:
   - **Users must agree to the following conditions** - You can require that users agree to legal conditions. In the text box, enter the conditions that are shown to the user.
   - **Upload** - Lets you upload a company logo. **Browse** to the logo file and click **Apply**. The logo is shown in the **Displayed Logo** section.
   - **Use Default** - Uses the default logo.
4. In the **Advanced** tab:
   - **Portal Address** - Keep the default setting which is the address the Captive Portal runs on the Quantum Spark Appliance or enter a different portal address.
   - **Session timeout** - Sets for how long an authenticated user can access the network or Internet before they have to authenticate again.

- **Enable Unregistered guests login** - Allow an unregistered, guest user to be identified in the logs by name and not only by IP address.

  An unregistered user is an unmanaged non-AD user, typically a partner or a contractor. To gain access, guests enter their company name, email address, phone number (optional), and name.

  Configure the **Guest Session timeout**. This is the number of minutes for which a guest user can access network resources. The default timeout is 180 minutes.

  Guest access is logged. The name of the guest shows in the **User** column of the **Logs and Monitoring** tab. The other details show in the full log entry.

  Guest access is logged. The name of the guest shows in the **User** column of the **Logs and Monitoring** tab. The other details show in the full log entry.

- **Force quick cache timeout if user closes portal window** - When the portal is closed, the user is logged out within 5 - 10 minutes.

5. Click **Apply**

# Identity Collector

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

Quantum Spark Locally Managed appliances support Identity Collector as an Identity Source in versions R81.10.05 and higher.

**To configure the Identity Collector**

1. In the **Policy Configuration** section, select **Identity Collector** and click **Configure**.

   The **Authorized Clients** window opens.

2. For each client, enter this information:

   - **IPv4 address** - The IP address of the client.
   - **Secret** - Password
     - **Optional** - Click **Show** to display the secret.

3. Click **Apply**

For more information about **Identity Collector** configuration, see *Identity Awareness Clients Administration Guide*.

**Note** - This page is available from **Access Policy** > **User Awareness Blade Control** and **Users & Objects** > **User Awareness**.

# Configuring QoS

## Introduction

The QoS (bandwidth control) policy is a set of rules that lets you set bandwidth parameters that control the flow of traffic to and from your network. They make sure that important traffic is prioritized and your business has minimal disruption when there is network congestion.

QoS can be activated on Internet connections and requires at least one Internet connection is configured with the maximum download and/or upload speeds. You get the speed information from your ISP.

QoS policy rules apply separately on each configured Internet connection.

## Prerequisites

In **Access Policy** > **QoS** > **Blade Control**, make sure the QoS blade is turned on.

## Configuration

1. In **Device** > **Internet**, select an Internet connection and click **Edit**.
2. In the **Advanced** tab, edit the **QoS Settings**.

   These values are used as a 100% percent baseline when you calculate QoS weight. For more details, see *"Configuring Internet Connectivity" on page 87*.
3. You can use these options:
   - A default QoS policy that requires defining only a number of parameters. See *"Configuring the QoS Blade" on page 310*.
   - Define manual rules for further granularity if necessary in **Access Policy** > **QoS** > **Policy**. See *"Configuring the QoS Policy" on page 313*.

# Configuring the QoS Blade

In the **Access Policy** view > **QoS** section > **Blade Control** page you can activate QoS and configure the QoS default policy.

The QoS (bandwidth control) policy is a set of rules that lets you set bandwidth parameters to control the flow of communication to and from your network. These rules make sure that important traffic is prioritized so your business can work with minimum disruption when there is network congestion.

You can configure QoS on Internet connections. This requires at least one Internet connection to be configured with the maximum download and/or upload speeds provided by your ISP. For more information about your download and upload speeds, contact your local ISP.

QoS policy applies to traffic over external interfaces only.

## QoS

Select one of the options to set the Access Policy control level:

- **On** - Enforces the default QoS policy.
- **Off** - QoS default policy is not enforced.

  **Note** - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in the next synchronization between the gateway and Cloud Services.

## QoS Default Policy

Select the options for your QoS default policy. Alternatively, you can define your entire QoS policy through the **Access Policy** > **QoS Policy** page by clearing all of the checkboxes on this page.

- **Ensure low latency priority for delay sensitive services (e.g. VoIP)** - Select this option to make sure that traffic that is very sensitive to delay is prioritized. For example, IP telephony, videoconferencing, and interactive protocols that must have a short response time, such as Telnet.

  Click the **delay sensitive services** link to see the default services included and add new ones or remove existing if necessary. QoS tries to send these packets before other packets. This option adds a rule to the QoS Policy Rule Base.

- **Guarantee X% of the bandwidth to VPN traffic on All services** - Select this option to guarantee a minimum bandwidth for the specified traffic on all services or selected services.

  Enter the bandwidth percentage, change the type of traffic if needed, and if necessary click the **All services** link to edit a list of selected guaranteed services. This option adds a rule to the QoS Policy Rule Base.

- **Limit bandwidth consuming applications** - Select this option to configure applications, for which you want to enforce a limit. Applications that use a lot of bandwidth can decrease performance necessary for important business applications.

  Click the **bandwidth consuming applications** link to see the default applications/categories included, add new ones, or remove existing, if necessary.

  Select **Download** and/or **Upload** to configure the maximum bandwidth in each of the selected options.

  You can also configure these applications limits in the:

  - **Access Policy** view > **Firewall** section > **Blade Control** page.
  - **Access Policy** view > **Firewall** section > **Policy** page.

**To add a guaranteed service to the QoS default policy:**

1. Select the **Guarantee X% of the bandwidth to X traffic on all/selected services** option and click the **services** link.

   The **Edit guaranteed services** window opens.

2. Select **Selected services**.
3. Click the **Select** button to show the full list of available services and select the relevant checkboxes.
4. Click **New** if the existing list does not contain the service you need.

   For information on creating a new service, see the **Users & Objects** view > **Network Resources** section > **Services** page.

5. Click **Apply**.
6. Click **Apply**.

# Configuring the QoS Policy

In the **Access Policy** view > **QoS** section > **Policy** page you can configure the manual QoS policy rules.

The top of the page shows information about these limits:

- **Bandwidth Consuming Applications** - If you set download and upload rates in the **Access Policy** > **QoS Blade Control page** or **Access Policy** > **Firewall Blade Control** page. If you see the **disabled** link, click it to configure the rates here.
- **Low latency traffic** - Shows the maximum percentage of bandwidth that can be reserved for low latency traffic. If you do not set a maximum percentage, traffic that does not require low latency might be starved (might not be handled at all). To change the value, click the **percentage** link.

You can view the QoS Policy Rule Base on this page. For each rule, you see these fields:

| Rule Base Field | Description |
|---|---|
| **No.** | Rule number in the QoS policy. |
| **Source** | Network object that starts the connection. |
| **Destination** | Network object that completes the connection. |
| **Service** | Type of network service for which bandwidth is adjusted based on weight, limit, and guarantee. |
| **Guarantee/Limit** | Lets you set a percentage that limits the bandwidth rate of traffic and/or guarantees the minimum bandwidth for traffic. Another option is to mark the traffic as low latency. This guarantees that it is prioritized accordingly. |
| **Weight** | The unit used to divide available bandwidth when traffic exceeds the maximum bandwidth configured for the Internet connection. See below. |
| **Track** | The tracking and logging action that is done when traffic matches the rule. |
| **Comment** | An optional field that shows a comment if you entered one. For system generated rules of the default policy a Note is shown. |

### Weight

QoS divides available bandwidth across the QoS policy rules based on *weight*. The use of weights instead of specified percentages is a flexible way for the QoS engine to allocate bandwidth if the maximum bandwidth is exceeded based on the specified traffic at that point. This maximizes the usage of the bandwidth.

For example, in an organization, Web traffic is deemed three times as important as FTP traffic. Rules with these services are assigned weights of 30 and 10 respectively. If the lines are congested, QoS keeps the ratio of bandwidth allocated to Web traffic and FTP traffic at 3 to 1.

You can set options for the default policy or you can manually define rules for the QoS policy. If a rule does not use all of its bandwidth, the leftover bandwidth is divided with the remaining rules, based on their relative weights. In the above example, if only one Web and one FTP connection are active and they compete, the Web connection receives 75% (30/40) of the leftover bandwidth, and the FTP connection receives 25% (10/40) of the leftover bandwidth. If the Web connection closes, the FTP connection receives 100% of the bandwidth.

In the **Weight** field, enter a value that shows the services importance relative to other defined services. For example, if you enter a weight of 100 for a service and set 50 for a different service, the first service is allocated two times the amount of bandwidth as the second when lines are congested.

**To create a QoS rule:**

1. Click the arrow next to **New**.
2. Click one of the available positioning options for the rule: **Top Rule**, **Bottom Rule**, **Above Selected**, or **Under Selected**.

   The **Add Rule** window opens. It shows the rule fields in two manners:

   - A rule summary sentence with default values.
   - A table with the rule base fields in a table.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the rule base fields. See the descriptions above.

   **Note** - You can select for a specified rule to have a specified guarantee and/or limit or be marked as low latency traffic. In case of the latter, there is a single maximum limit percentage for ALL low latency traffic which can be configured globally. See above.
4. To match only for encrypted (VPN) traffic, select **Match only for encrypted traffic**. The Service column shows "encrypted" if selected.
5. To limit the rule to a specified time range, select **Apply only during this time** and select the start and end times. Only connections that begin during this time range are inspected.
6. DiffServ Mark is a way to mark connections so a third party handles it. To mark packets that are given priority on the public network based on their DSCP, select **DiffServ Mark (1-63)** and select a value. To use this option, your ISP or private WAN must support DiffServ. You can get the DSCP value from your ISP or private WAN administrator.
7. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule.
8. Click **Apply**

**Note** - You can drag and drop rules to change the order of rules in the QoS Rule Base

**To edit a QoS rule:**

**Note** - For Access Policy rules, you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**

### To delete a QoS rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

### To enable or disable a QoS rule:

- To disable a manually defined rule that you have added to the Rule Base, select the rule and click **Disable**.
- To enable a manually defined rule that you have previously disabled, select the rule and click **Enable**.

### To change the QoS rule order:

1. Select the rule to move.
2. Drag and drop it to the necessary position.

**Note** - You can only change the order of manually defined rules.

# SSL Inspection Policy

## SSL Inspection

The **Access Policy** view > **SSL Inspection** section > **Policy** page lets you enable and configure SSL inspection. When you turn on this setting, you allow different Software Blades that support SSL inspection to inspect traffic that is encrypted by the Secure Sockets Layer (SSL) protocol. To allow the gateway to inspect the secured connections, all hosts behind the gateway must install the gateway CA certificate.

Software Blades that support SSL traffic inspection:

- Application & URL Filtering
- IPS
- Anti-Virus
- Anti-Bot
- Threat Emulation

**Important** - You cannot use Smart Accel and SSL Inspection at the same time.

## Deploying SSL Inspection

**To deploy SSL inspection:**

1. Select **SSL Traffic Inspection**.
2. Click **Download CA Certificate** to download the gateway's internal CA certificate.

   **Note** - The certificate is available for all users on the gateway. You do not need administrator credentials. If you do not have administrator credentials, connect from an internal or wireless network to `http://my.firewall/ica` or `https://<IP_Address_of_Appliance>/ica`.

   You must install this certificate on every client behind the gateway.

**To install the certificate:**

1. Manually copy the certificate file to your PC.
2. In the Windows PC, click the file and follow the wizard instructions to add the certificate to the Trusted Root Certification Authorities repository.

   **Note** - This is not the default repository in the Certificate Import Wizard.

   Certificate installation varies according to the OS. To learn how to install the certificate in your machine, see your OS vendor instructions.

SSL inspection uses the existing internal CA by default. To use your own certificate, you must replace the internal CA.

**To replace the internal CA:**

1. Go to **Certificates** > **Internal Certificate**.
2. Click **Replace Internal CA**.

   The **Upload a P12 Certificate** window opens.
3. Click **Browse** to select the certificate file.
4. Enter the **Certificate name** and **Password**.
5. Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.
6. Click **Apply**

# SSL Inspection Bypass Policy

You can select categories that are bypassed for all possible traffic regardless of its source and destination. To configure more advanced exceptions, go to the **SSL Inspection Exceptions** page.

**To configure the SSL inspection bypass policy:**

- In the section **Protocols to inspect** - Select to inspect **HTTPS**, **IMAPS**, or **POP3S** protocols.
- In the section **Assets to Inspect** - Select to inspect devices by type: **Desktop**, **Laptop**, **Computer** (R81.10.05 and higher), **Other assets**, and **All assets**. Devices are inspected only if they were not bypassed by other settings.
- In the section **Wireless networks to bypass** - Select or clear which wireless networks to bypass. **Untrusted networks** are selected by default.

  **Note** - Wireless networks must be assigned to **Separate Network**, not switch or bridge.

- In the section **Bypass SSL inspection for the following categories** > **Categories** - Categories include **Health**, **Government/Military**, **Financial services**, and **Well known update services**. Select or clear the privacy related categories that are not inspected. All categories except for **Media Streams** are selected by default.
- In the section **Bypass SSL inspection for the following categories** > **Assets to bypass** - Select the **MacOS** checkbox to bypass macOS devices. This accelerates the connection.
  - **Bypass by MAC** - Click to select devices from the **Active Devices** table by their MAC addresses.
  - **Bypass by IP** - Click to configure exceptions to bypass SSL inspection policy for specific IP addresses on the **SSL Inspection Exceptions** table.
- In the section **Tracking** - Select to enable logs to see the SSL inspection policy decision ("**Inspect**" or "**Bypass**").

  **Note** - The SSL Inspection generates these logs in addition to the Software Blades logs.

**To add other categories:**

**Note** - The **Bypass** checkbox is selected by default.

1. Click **other categories and sites**.

   The **SSL Inspection Bypass Other** window opens.

2. Select the desired items.
3. **Optional** - Click **New** to add URLs or custom applications.
4. Click **Apply**

# HTTPS Categorization

As an alternative to SSL inspection, you can enable HTTPS categorization.

HTTPS categorization allows filtering specified HTTPS URLs and applications without activating SSL traffic inspection.

For more information, see the *HTTPS Inspection video* on the *Small Business Security video channel*.

**To enable HTTPS categorization:**

1. Select **HTTPS Categorization**.

   **Note** - When you enable HTTPS categorization, the SSL options are not available.

2. Click **Configure**.

   The **Access Policy** > **Firewall Blade Control** page opens.

3. Configure the settings for URL Filtering.

   **Note** - HTTPS categorization only applies when the URL Filtering blade is turned on.

**To disable SSL inspection and HTTPS categorization:**

Select **Off**.

Upgrades in the SSL Bypass mechanism include:

- Stop the inspection of the first connection to bypassed sites.
- Allow bypass of Non-Browser Applications connections.
- Allow Bypass of connections to servers that require client certificate.
- New probing mechanism eliminates the need to inspect the first connection to an IP address unless it is required by the policy.

## IMAPS

Internet Message Access Protocol (IMAP) is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. IMAPS refers to IMAP over SSL.

SSL traffic inspection must be activated to scan HTTP and IMAP encrypted traffic.

# SSL Inspection Exceptions

On the **SSL Inspection Exceptions** page, you can define manual rules to configure exceptions to bypass SSL inspection for specific traffic. You can also add rules to include updatable objects and FQDN as your source or destination. For more information on how to import, see *"Updatable Objects" on page 264*.

You can configure more advanced exceptions with specific scope, category, and tracking options.

**To add bypass exceptions:**

1. In the **Access Policy** > **SSL Inspection Policy** page:
   a. Download and install the CA Certificate.
   b. Turn on SSL traffic inspection.
2. Click **New** to create a new rule to bypass the source/destination.

   **Note** - Everything that is not included in a rule is inspected.

3. For each exception, enter:
   - **Source**
   - **Destination**
   - **Category/Custom Application**
   - **Track**

**Note** - Starting from R81.10.05, a policy rule with an application and action that redirects to the user portal (ask, block and inform, accept and inform) fails to redirect when SSL Inspection is on and the default bypass rule in the SSL Inspection Exception page is enabled.

# SSL Inspection Advanced

To enable SSL web traffic inspection, you must first establish trust between the clients and the gateway.

An important part of the HTTPS inspection support is the validation of the server's certificate. This requires validating the signing CA of the server certificates.

On the **SSL Inspection Advanced** page, you can manage trusted certificate authorities. The gateway has a built-in predefined list of trusted CAs, based on the Mozilla/LibCurl Trusted CA list. Only a server certificate signed by one of those CAs is recognized as a valid certificate. The table shows the list of trusted CAs.

Trusted CA types:

- Default from the gateway - These CAs can be disabled but not deleted.
- Added by user - These CAs can be deleted.

### To add a CA manually to the trusted CA list:

1. Click **Add**.

   The **Add a Trusted CA** window opens.
2. Click **Browse** to select a trusted CA file.
3. **Optional** - Click **Preview** to view the CA.
4. Click **Apply**

### To delete a trusted CA:

1. Click the icon next to the CA.
2. Click **Delete**.

   **Note** - You can only delete a CA that was added by a user.

### To disable/enable a trusted CA:

1. Click the icon next to the CA.
2. Click **Disable/Enable**.

# Managing Threat Prevention

This section describes how to set up and manage the Intrusion Prevention System (IPS), Anti-Virus, Anti-Bot, Threat Emulation, and Anti-Spam blades.

## Configuring Threat Prevention Blade Control

In the **Threat Prevention** > **Threat Prevention Blade Control** page you can activate:

- **Intrusion Prevention System (IPS)**. Blocks potentially malicious attempts to exploit known vulnerabilities in files and network protocols.
- **Anti-Virus**. Blocks potentially malicious files that are infected with viruses.
- **Anti-Bot**. Detects bots, prevents communication between the bot and its Command & Control center, and gives threat visibility. A *bot* is malicious software that can infect your computer with malware. A bot infected device can then be used by a Command & Control server to execute different types of attacks (send out SPAM messages or Denial-of-Service attacks against web sites). There are many infection methods. These include if you open attachments that exploit a vulnerability or access a web site that results in a malicious download.
- **Threat Emulation**. Gives networks protection against unknown threats in files that are downloaded from the Internet or attached to emails. In emulation, the file is opened on more than one virtual computer with different operating system environments. These virtual computers are closely monitored for unusual and malicious behavior. Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network. Information about malicious files is shared with Check Point ThreatCloud.

You configure all the settings for these blades in the same place and set a single profile for all of them.

### Enabling and Disabling Threat Prevention

Move the slider to **ON** or **OFF**.

# Enabling Threat Emulation Policy for the FTP Protocol

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

Move both the Anti-Virus and Threat Emulation sliders to **ON**.

**Note** - When the blade is managed by Cloud Services, a lock icon appears. You cannot toggle between the "**ON**" and "**OFF**" states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

The update status is displayed next to each blade:

- Up to date
- Update available
- Update service unreachable

You can activate the blades to prevent attacks/infection or set them to detect-mode only on the **Threat Prevention Engine Settings** page.

A warning message shows if a blade is in configured in the Detect-only mode.

The top of the page shows the number of infected devices. For more information, click **More details**.

One policy is configured for all the blades:

- **Strict** - Focuses on security.
- **Recommended** - The default option, which gives the best mixture of security and performance for small/medium sized business.

  **Note** - The performance impact for the "Suspicious Mail Activity" protection in Anti-Bot was changed to High and is now **off** by default. To enable this protection, you must configure it in a custom policy.

- **Custom** - Manually defined by the user.

# Configuring a Custom Policy for Threat Prevention

1. In the **Threat Prevention Blade Control** page, under **Policy**, select **Custom**.
2. For **Tracking options**, select one of these options:
   - **None** - Do not log.
   - **Log** - Create a log.
   - **Alert** - Log with an alert.

3. Under **Protection Activation**, for each confidence level (**High confidence**, **Medium confidence**, and **Low confidence**), select the applicable action from the list:
   - **Ask** - Traffic is blocked until the user confirms it is allowed.
   - **Prevent** - Blocks identified virus or bot traffic, or identified malicious files, from passing through the gateway.
   - **Detect** - Allows identified virus or bot traffic, or identified malicious files, to pass through the gateway. This traffic is detected and logged.
   - **Inactive** - The protection is deactivated.
4. For **Severity**, select the level:
   - **Low or above**
   - **Medium or above**
   - **High or above**
   - **Critical**
5. For **Performance impact**, select the allowed impact level:
   - **Low**
   - **Medium or lower**
   - **High or lower**
6. To load the policy default values, click **Load default settings**:
   - **Recommended**
   - **Strict**
7. To save all settings on the **Threat Prevention Blade Control** page, click **Apply**.

# Scheduling Threat Prevention Updates

1. Click **Schedule**.

   The **Activate Automatic Updates** window opens.

2. Select the Software Blades to receive automatic updates:

   - IPS
   - Anti-Virus
   - Anti-Bot
   - Application Control

3. Select the **Recurrence** and **Time of day**.

4. Click **Apply**

# Configuring Threat Prevention Policy Exceptions

In the **Threat Prevention** > **Threat Prevention Exceptions** page you can configure exception rules for traffic which the IPS engine and malware engine for Anti-Virus and Anti-Bot do not inspect.

## Threat Prevention Exceptions

**To add a new Threat Prevention exception rule:**

1. In the **IPS Exceptions** section, click **New** > **Add**.
2. Click one of the available positioning options for the rule: **Top Rule**, **Bottom Rule**, **Above Selected**, or **Under Selected**.
3. Configure these fields:
   - **Scope** - For Threat Prevention blades only. Threat Prevention inspects traffic to and/or from all objects specified in the Scope, even when the specified object did not open the connection. Can include network object, network object groups, IP address ranges and local users.

     Select either Any or a specific scope from the list. If necessary, you can create a New network object, network object group, or local user.

     If it is necessary to negate a specified scope, select the scope and select the Any Scope except checkbox.

     For example, if the scope of the exception should include all scopes except for the DMZ network, select DMZ network and select the Any Scope except checkbox.
   - **Source** - Network object that initiates the connection.
   - **Destination** - Network object that is the target of the connection.

     Options include: FQDN, Updatable objects

     To add an updatable object, double click and import the new updatable object. For more information, see *"Updatable Objects" on page 264*.

     **Note** - This relies on an external database for updatable objects and some IPs might not be listed under FQDN or updatable objects.
   - **Protection** - In the Blades tab, select Any for all or for a specific blade. In the IPS protections tab, select a specific IPS protection from the list.

- **Service/Port** - Type of network service. If you make an exception for a specified protection on a specific service/port, you might cause the protection to be ineffective.
- **Action** - Select the applicable action to enforce on the matching traffic: **Ask**, **Prevent**, **Detect** or **Inactive**. See the Threat Prevention > **Threat Prevention Blade Control** page for a description of the action types.
- **Log** - Select the tracking option: **None**, **Log**, or **Alert**. Logs are shown on the **Logs & Monitoring** > **Security Logs** page. An alert is a flag on a log. You can use it to filter logs.

4. **Optional** - Add a comment in the Write a comment field.
5. Click **Apply**

## allowlists

You can set specified files and URLs that the Anti-Virus, Anti-Bot and Threat Emulation blades do not scan or analyze. For example, if there are files that you know are safe but can create a false positive when analyzed, add them to the Files allowlist.

Threat Emulation only: You can set specified email addresses that the blade does not scan and add them to the Email Addresses allowlist.

**To add a file or URL to the allowlist:**

1. Select **Files allowlist** or **URLs allowlist**.
2. Click **New**.

   The **Add File** or **Add URL** window opens.
3. For a file, enter the **MD5 checksum** that gives the digital signature for a specified file.
4. For a URL, enter the **URL**.
5. Click **Apply**

**To add an email address to the allowlist:**

1. Select **Email Addresses allowlist**.
2. Click **New**.

   The **Add Email Address** window opens.
3. Enter the email address.
4. For **Type**, select Sender or Recipient.
5. Click **Apply**

**To edit or delete an exception rule:**

1. Select the relevant rule.
2. Click **Edit** or **Delete**.

# Threat Prevention - Horizon SOC

The Check Point Horizon SOC is supported from R81.10.00 in the Locally Managed mode. Horizon SOC enables cybersecurity teams to effectively and efficiently prevent, detect and respond to all threats. Horizon SOC doubles the effectiveness of SOC teams by automating time-consuming tasks, allowing security teams to focus on remediation and attack prevention.

You can enable the Horizon SOC feature in the WebUI or through Gaia Clish commands.

**To enable the Horizon SOC feature in the WebUI:**

1. Click **Device** > **Advanced Settings**.
2. In the **Privacy Settings Attribute** section, select the attribute **Help Check Point improve its products by sending data**.
   a. Click **Edit**.
   b. Select **Help us improve product experience by sending data to Check Point**.
   c. Click **Apply**
3. In the **Threat Prevention Policy Attribute** section, select the attribute **Allow me to view attack statistics in my User Center account**.
   a. Click **Edit**.
   b. Select **Allow me to view attack statistics in my User Center Account**.
   c. Click **Apply**
4. **Optional**: In the **Threat Prevention Policy** section, select the attribute Allow **IP address information in attack statistics**.
   a. Click **Edit**.
   b. Select **Allow IP address information in attack statistics**.
   c. Click **Apply**

**To enable the Horizon SOC feature in Gaia Clish:**

1. Allow the appliance to send data to Check Point:

   ```
   set privacy-settings advanced-settings customer-consent true
   ```

2. Allow viewing attack statistics in your User Center Account:

   ```
   set threat-prevention policy advanced-settings allow-attack-stats true
   ```

3. **Optional**: Enable the real IP address information in the attack reports:

   ```
   set threat-prevention policy advanced-settings allow-ipaddr-in-stats true
   ```

# Viewing Infected Devices

In the **Infected Devices** page you can see information about infected devices and servers in the internal networks. You can also directly create an exception rule for a specified protection related to an infected or possibly infected device or server.

You can access this page from the **Threat Prevention** tab > **Threat Prevention** section, or from the **Logs and Monitoring** tab > **Status** section.

The Infected Devices table shows this information for each entry:

- **Icon** - Shows icons for the different classifications of infected devices and servers.

| Description | Host Icon | Server Icon |
|---|---|---|
| Infected device or server - When the Anti-Bot blade detects suspicious communication between the host or server and an external Command & Control center due to a specified triggered protection | 🖥 | 🗄 |
| Possibly infected device or server - When the Anti-Virus blade detects an activity that *may* result in host or server infection. For example:<br>• When you browse to an infected or a potentially unsafe Internet site, there is a possibility that malware was installed.<br>• When you download an infected file, there is a possibility that the file was opened or triggered and infected the host or server. | 🖥❓ | 🗄❓ |

- **Object name** - Shows the object name if the host or server was configured as a network object.
- **IP/MAC address** - Shows the IP and MAC address of the infected device.
- **Device/User Name** - Shows a device or user name if the information is available to the appliance through DHCP or User Awareness.
- **Incident type** - Shows the detected incident type:
  - Found bot activity
  - Downloaded a malware
  - Accessed a site known to contain malware
- **Severity** - Shows the severity of the malware:

  - Low
  - Medium
  - High
  - Critical
- **Protection name** - Shows the Anti-Bot or Anti-Virus protection name.
- **Last incident** - The date of the last incident.
- **Incidents** - Shows the total number of incidents on the device or server in the last month. If there is a large amount of records, the time frame may be shorter.

**To filter the infected devices list**

1. Click **Filter**.
2. Select one of the filter options:
   - **Servers only** - Shows only machines that were identified as servers (and not any machine/device).

     Servers are defined as server objects in the system from the **Access Policy** > **Servers** page.
   - **Possibly infected only** - Shows only devices or servers classified as possibly infected.
   - **Infected only** - Shows only devices or servers classified as infected.
   - **High and above severity only** - Shows devices and servers that are infected or possibly infected with malwares that have a severity classification of high or critical.

**To add a malware exception rule for a specified protection**

1. Select the list entry that contains the protection for which to create an exception.
2. Click **Add Protection Exception**.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the exception rule fields.
   - **Scope** - Select either **Any** or a specific scope from the list. If necessary, you can create a **New** network object, network object group, or local user.

     If it is necessary to negate a specified scope, select the scope and select the **Any Scope except** checkbox.

     For example, if the scope of the exception should include all scopes *except* for the DMZ network, select DMZ network and select the **Any Scope** except checkbox.

     **Note** - DMZ is not supported in 1530 / 1550 appliances.

   - **Action** - Select the applicable action to enforce on the matching traffic: **Ask**, **Prevent**, **Detect** or **Inactive**.

     See the **Threat Prevention** > **Threat Prevention Blade Control** page for a description of the action types.

   - **Log** - Select the tracking option: **None**, **Log**, or **Alert**.

     Logs are shown on the **Logs & Monitoring** > **Security Logs** page.

     An alert is a flag on a log. You can use it to filter logs.

4. **Optional** - Add a comment in the **Write a comment** field.
5. Click **Apply**

   The rule is added to **Malware Exceptions** on the **Threat Prevention** > **Exceptions** page.

**To view the logs of a specified entry:**

1. In the Logs and Monitoring tab, select the list entry for which to view logs.
2. Click **Logs**.

   The **Security Logs** page opens and shows the logs applicable to the IP/MAC address.

# Viewing the IPS Protections List

In the **Threat Prevention** > **IPS Protections List** page you can monitor specific protections, or manually configure a specific protection to override the general policy.

**To search for a specified protection:**

1. Enter a name in the **filter** box.
2. Scroll the pages with the next and previous page buttons at the bottom of the page.

To configure the IPS policy, go to the **Threat Prevention** > **Threat Prevention Blade Control** page.You can see the details of each protection and also configure a manual override for individual protections' action, and tracking options.

# Advanced Threat Prevention Engine Settings

In the **Threat Prevention** > **Threat Prevention Engine Settings** page you can configure advanced configuration settings for the Anti-Virus, Anti-Bot, Threat Emulation, and IPS engines.

**Note** - Many of the configurations below are advanced and should only be used by experienced administrators.

## IPS

Configure the settings for newly downloaded protections:

- **Active**
- **Detect**
- **Inactive**

**To enable Detect-only mode:**

Select the checkbox.

**To import IPS protections:**

Click the link.

## Anti-Virus

Anti-Virus scans incoming files for viruses.

The mail settings include:

- SMTP - Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.
- POP3 - Uses the POP3 protocol to send and receive emails with TLS encryption.
- IMAP - Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. It allows you to access your email from any device.

**To enable POP3S or IMAP scans:**

1. On the **Threat Prevention** > **Engine Settings** page, under **Anti-Virus Scanned protocols**, select the **Mail (SMTP, POP3 and IMAP)** checkbox.
2. On the **Access Policy** > **SSL Inspection Policy** page, select the checkbox to **enable SSL traffic inspection**.
3. Under **Protocols to inspect**, select **POP3S** or **IMAP**.
4. Click **Apply**

**To configure the Anti-Virus settings:**

1. Select one of the protected scope options:
   - **Scan incoming files from** - Select one of these interfaces from which to scan incoming files:
     - **External and DMZ** - Files that originate from external and the DMZ interfaces are inspected.

       **Note** - DMZ is not supported in 1530 / 1550 appliances.
     - **External** - Files that originate from external interfaces are inspected.
     - **All** - Files transferred between all interfaces are inspected.
   - **Scan both incoming and outgoing files** - Files that originate from outside the organization and from within the organization to the Internet are inspected.
2. Select the protocols to scan for the selected scope:
   - **HTTP (on any port)**
   - **Mail (SMTP**, **POP3** and **IMAP**

- **FTP** - Disabled by default.

  **To activate FTP:**

  a. In the WebUI go to **Home** > **Security Dashboard** and turn on the Anti-Virus Software Blade.

  b. Connect to the command line and run this command:

  ```
  set threat-prevention anti-virus policy protocol-ftp
  true
  ```

  c. Install Policy.

You must activate the **SSL traffic inspection** to scan HTTP and **IMAP** encrypted traffic. To activate, click the link or go to **Access Policy** > **SSL Inspection Policy**.

3. Select one of the file type policy options:

   - **Process file types known to contain malware**
   - **Process all file types**
   - **Process specific file type families** - Click **Configure** for a list of file types and set prescribed actions to take place when these files pass through the Anti-Virus engine. To edit an action for a specified file type, right-click the row and click **Edit**.

     The available actions are:

     - **Scan** - The Anti-Virus engine scans files of this type.
     - **Block** - The Anti-Virus engine does not allow files of this type to pass through it.
     - **Pass** - The Anti-Virus engine does not inspect files of this type and lets them pass through.

       You cannot delete system defined file types. System defined file types are recognized by built-in signatures that cannot be edited. Manually defined file types are recognized by their extension and are supported through the web and mail protocols.

4. You can set **policy overrides** to override the general policy setting defined on the Threat Prevention Blade Control page. For each of the below protection type options, you can set the applicable override action: Ask, Prevent, Detect, Inactive, or According to policy (no override). See the **Threat Prevention** > **Threat Prevention Blade Control** page for a description of the action types.

   - **URLs with malware** - Protections related to URLs that are used for malware distribution and malware infection servers.

- **Viruses** - Real-time protection from the latest malware and viruses by examining each file against the Check Point ThreatCloud database.

### To enable Detect-only mode:

Select the checkbox.

## Anti-Bot

You can set **policy overrides** to override the general policy settings defined on the **Threat Prevention Blade Control** page. For each of the below protection type options, you can set the applicable override action: Ask, Prevent, Detect, Inactive, or According to policy (no override). See the **Threat Prevention** > **Threat Prevention Blade Control** page for a description of the action types.

- **Malicious activity** - Protections related to unique communication patterns of botnet and malware specified families.
- **Reputation domains** - Protections related to Command & Control (C&C) servers. Each host is checked against the Check Point ThreatCloud reputation database.
- **Reputation IPs** - Protections related to Command & Control (C&C) servers. Each IP is checked against the Check Point ThreatCloud reputation database.
- **Reputation URLs** - Protections related to Command & Control (C&C) servers. Each URL is checked against the Check Point ThreatCloud reputation database.
- **Unusual activity** - Protections related to the behavioral patterns common to botnet and malware activity.

### To enable Detect-only mode:

Select the checkbox.

# Threat Emulation

**To configure the Threat Emulation settings:**

1. Select one of the protected scope options:
   - Scan Incoming files from - Select one of these interfaces from which to scan incoming files:
     - **External and DMZ** - Files that originate from external and the DMZ interfaces are inspected.

       ⓘ **Note** - DMZ is not supported in 1530 / 1550 appliances.
     - **External** - Files that originate from external interfaces are inspected.
     - **All** - Files transferred between all interfaces are inspected.

       ⓘ **Note** - LAN to LAN scanning is not supported.
   - **Scan both incoming and outgoing files** - Files that originate from outside the organization and from within the organization to the Internet are inspected.
2. Select the protocols to scan for the selected scope:
   - HTTP (on any port)
   - **Mail (SMTP**, **POP3** and **IMAP**.

     You must activate the **SSL traffic inspection** to scan HTTP and IMAP encrypted traffic. To activate, click the link or go to **Access Policy** > **SSL Inspection Policy**.
3. For file type policy:

   **Process specific file type families** - Click **Configure** for a list of file types and set prescribed actions to take place when these files pass through the Threat Emulation engine.

   To edit an action for a specified file type, right-click the row and click **Edit**. You can also click the file type so it is selected and then Click **Edit**.

   The available actions are:

- **Inspect** - The Threat Emulation engine inspects files of this type.
- **Bypass** - The Threat Emulation engine does not inspect files of this type and lets them pass through.

  You cannot delete system defined file types. System defined file types are recognized by built-in signatures that cannot be edited.

4. Select the HTTP connection emulation handling mode:
   - **Background** - Connections are allowed until emulation is complete.
   - **Hold** - Connections are blocked until emulation is complete.

In Threat Emulation, each file is run in the Check Point Public ThreatCloud to see if the file is malicious. The verdict is returned to the gateway.

You can change the emulator location to a local private SandBlast appliance in the **Advanced Settings** page.

You must first enable the Threat Emulation blade and then configure it for remote emulation.

### To enable the Remote Private Cloud Threat Emulation emulator:

1. Go to **Device** > **Advanced Settings**.
2. Search for **Threat Prevention Threat Emulation policy - Emulation location**.
3. Select **Emulation is done on remote (private) SandBlast**.
4. Add or update the emulator IP address.
5. Click **Apply**

### To disable the Remote Private Cloud Threat Emulation emulator:

1. Go to **Device** > **Advanced Settings**.
2. Search for **Threat Prevention Threat Emulation policy - Emulation location**.
3. Select **Emulation is done on Public ThreatCloud**.
4. Click **Apply**

To configure multiple remote emulators, you must use CLI commands.

For more information on Threat Emulation, see the *Threat Emulation video* on the *Small Business Security video channel*.

### To enable Detect-only mode:

Select the checkbox.

## User Messages

You can customize messages for protection types set with the Ask action. When traffic is matched for a protection type that is set to Ask, the user's internet browser shows the message in a new window.

These are the Ask options and their related notifications:

| Option | Anti-Virus Notification | Anti-Bot Notification |
|---|---|---|
| **Ask** | Shows a message to users and asks them if they want to continue to access a site or download a file that was classified as malicious. | Shows a message to users and notifies them that their computer is trying to access a malicious server. |
| **Block** | Shows a message to users and blocks the site. | Anti-Bot blocks background processes. If a specified operation from a browser to a malicious server is blocked, a message is shown to the user. |

**To customize messages:**

1. Click **Customize Anti-Virus user message** or **Customize Anti-Bot user message.**
2. Configure the options in each of these tabs:
   - Ask
   - Block
3. Configure the applicable fields for the notifications:
   - **Title** - Keep the default or enter a different title.
   - **Subject** - Keep the default or enter a different subject.
   - **Body** - Keep the default or enter different body text. You can click **Optional keywords** for a list of keywords that you can add in the body text to give the user more information.
   - **Ignore text** (only for Ask) - If the user decides to ignore the message, this is the text that is shown next to the checkbox. Keep the default text or enter different text.
   - **User must enter a reason** (only for Ask) - Select this checkbox if users must enter an explanation for their activity. The user message contains a text box to enter the reason.

- **Fallback action** (only for Ask) - Select an alternative action (Block or Accept) for when the notification cannot be shown in the browser or application that caused the notification, most notably in non-web applications.
    - If the Fallback action is **Accept** - The user can access the website or application.
    - If the Fallback action is **Block** - The website or application is blocked, and the user does not see a notification.
- **Frequency** - You can set the number of times that the Anti-Virus, Anti-Bot, or Threat Emulation Ask user message is shown.
    - **Once a day**
    - **Once a week**
    - **Once a month**
- **Redirect the user to a URL (only for block) -**

  You can redirect the user to an external portal, not on the gateway. In the URL field, enter the URL for the external portal. The specified URL can be an external system. It gets authentications credentials from the user, such as a user name or password. It sends this information to the gateway.

4. Click the **Customize** tab to customize a logo for all portals shown by the appliance (Hotspot and captive portal used by User Awareness). Click **Upload**, browse to the logo file and click **Apply**. If necessary, you can revert to the default logo by clicking **Use Default**.
5. Click **Apply**

# Configuring the Anti-Spam Blade Control

In the **Threat Prevention** > **Anti-Spam Blade Control** page you can activate the Anti-Spam engine to block or flag emails that contain known or suspected spam content.

Select to inspect based on:

- The sender's source address.
- The email content.

Use the logs to understand if your system is experiencing spam attacks.

You can handle suspected spam the same way as known spam, or select to handle suspected spam separately (see below).

### To enable or disable Anti-Spam:

1. Select **On** or **Off**.
2. Click **Apply**

**Note** - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in the next synchronization between the gateway and Cloud Services.

### To configure Detect-only mode:

In **Detect-only** mode, logs appear but the blade does not block any emails.

1. Select the **Detect-only mode** checkbox.
2. Click **Apply**

**To configure the Anti-Spam Policy:**

1. Select the action to perform on emails whose content was found to contain spam:
   - **Block spam emails**
   - **Flag spam email subject with** - The default is **SPAM** or you can enter a new text to add to the subject line.
   - **Flag spam email header** - This option identifies email as spam in the email message header.
2. Select the relevant **tracking option**:
   - **Log**
   - **Alert**
   - **None**

**To handle suspected spam separately from known spam:**

1. Click **Handle suspected spam separately**.
2. Select an option:
   - **Block**
   - **Flag email subject with** - The default is **SUSPECTED SPAM** or you can enter a new text to add to the subject line.
   - **Flag email header**
3. Select a tracking option:
   - **Log**
   - **Alert**
   - **None**
4. Click **Apply**

# Configuring Anti-Spam Exceptions

In the **Threat Prevention** > **Anti-Spam Exceptions** page you can configure:

- Safe senders (email addresses) and/or domains or IP addresses from which emails are not inspected.
- Specific senders and/or domains or IP addresses that Anti-Spam engine blocks regardless of its own classification.

To block or allow by senders requires the Anti-Spam engine to be configured to filter based on **Email content** in the **Threat Prevention** > **Anti-Spam Blade Control** page.

**Note** - IP address exceptions are ignored for POP3 traffic.

### To add a new sender/domain/IP address to the Allow or Block list:

1. Click **Add** or **New** in the Allow or Block list.
2. Enter the **IP address** or **Sender/Domain**.
3. Click **Apply**

### To edit or delete a sender/domain/IP address from the Allow or Block list:

1. Select the relevant row in the Allow or Block list.
2. Click **Edit** or **Delete**.

   If the options are not visible, click the arrows next to the filter box.

# Managing VPN

This section describes how to set up and manage Remote Access and Site to Site VPN.

# Configuring VPN

This section describes how to configure these VPN configuration scenarios:

- Remote Access VPN
- Site to Site VPN using a preshared secret
- Site to Site VPN using a certificate

**Note** - VPN does not work with pure IPv6, only with dual IP stack.

## Configuring Remote Access VPN

### Introduction

Use these options for remote access:

- Check Point VPN clients
- Check Point Mobile clients
- Check Point SSL VPN
- L2TP VPN client

### Prerequisites

- In **VPN** > **Blade Control**, make sure:
  - To set the Remote Access control to **On**.
  - To select the **Allow traffic from Remote Access users (by default)** option.
  - To select the applicable connection methods.

  For more details, see *"Configuring the Remote Access Blade" on page 355*.
- If the gateway uses a dynamic IP address, we recommend you use the DDNS feature. See *"Configuring DDNS and Access Service" on page 180*.
- For the Check Point VPN client or Mobile client method, make sure that the applicable client is installed on the hosts. Click **How to connect** for more information.

## Remote Access Configuration

These are the methods to configure remote access users:

- Local users
- RADIUS users
- AD users

To allow only specified users to connect with a remote access client, set group permissions for the applicable user type. Select the arrow next to the **Add** option and select the relevant group option. See *"Configuring Remote Access Users" on page 374*.

### To configure new local users:

1. Go to **VPN** > **Remote Access Users**.
2. Click **Add** to add local users.
3. Make sure that the **Remote Access permissions** checkbox is selected.

For more information, see *"Configuring Remote Access Users" on page 374*.

### To configure existing users:

1. Go to **VPN** > **Remote Access Users**.
2. Click **Edit** to make sure that the **Remote Access permissions** checkbox is selected.

For more information, see *"Configuring Remote Access Users" on page 374*.

### To configure RADIUS users:

1. Go to **VPN** > **Authentication Servers.**
2. Click **Configure** to add a RADIUS server. See *"Configuring Authentication Servers for Remote Access" on page 384*.
3. Click **permissions for RADIUS users** to set access permissions.

### To configure AD users:

1. Go to **VPN** > **Authentication Servers** and click **New** to add an AD domain. See *"Configuring Authentication Servers for Remote Access" on page 384*.
2. Click **permissions for Active Directory users** to set access permissions.

## L2TP VPN Client configuration

For L2TP VPN Client configuration, click **L2TP Pre-shared key** to enter the key after you enable the L2TP VPN client method.

### Advanced Options

For more information on advanced Remote Access options, for example Office Mode network, see *"Configuring Advanced Remote Access Options" on page 399*.

### Monitoring

**To make sure Remote Access is working:**

Use the configured client to connect to an internal resource from a remote host.

# Configuring Site to Site VPN with a Preshared Secret

## Introduction

In this Site to Site VPN configuration method a preshared secret is used for authentication.

## Prerequisites

- Make sure the Site to Site VPN blade is set to On and **Allow traffic from remote sites (by default)** is selected. See *"Configuring the Site to Site VPN Blade" on page 404*.
- The peer device that you connect to must be configured and connected to the network. If it is a DAIP gateway, its host name must be resolvable.

## Configuration

Enter a host name or IP address and enter the preshared secret information. For more information, see *"Configuring VPN Sites" on page 407*.

## Monitoring

**To make sure the VPN is working:**

1. Send traffic between the local and peer gateway.
2. Go to **VPN** > **VPN Tunnels** to monitor the tunnel status. See *"Viewing VPN Tunnels" on page 417*.

# Configuring Site to Site VPN with a Certificate

## Introduction

In this Site to Site VPN configuration method a certificate is used for authentication.

## Prerequisites

- Make sure the Site to Site VPN blade is set to On and **Allow traffic from remote sites (by default)** is selected. See *"Configuring the Site to Site VPN Blade" on page 404*.
- The peer device that you connect to must be configured and connected to the network. If it is a DAIP gateway, its host name must be resolvable.
- You must reinitialize certificates with your IP address or resolvable host name. Make sure the certificate is trusted on both sides.
- VPN encryption settings must be the same on both sides (the local gateway and the peer gateway). This is especially important when you use the Custom encryption option.

## Configuration

1. Reinitialize certificates - Use the **Reinitialize certificates** option described in *"Managing Installed Certificates" on page 215*. Make sure this is done on both the local and peer gateway (if they both use locally managed Check Point appliances).
2. Trust CAs on the local and peer gateways - Use one of these procedures:
   - Exchange CAs between gateways
   - Sign a request using one of the gateway's CAs.
   - Authenticate by using a 3rd party CA.
   - Authenticate with an existing 3rd party certificate.
3. Use certificate authentication to create the VPN site.
   a. Follow the instructions in *"Configuring VPN Sites" on page 407*.
   b. To make sure the specified certificate is used, enter the peer gateway's certificate information in **Advanced** > **Certificate Matching**.

## Trust Procedures

Exchange CAs between gateways:

Click **Add** to add the Trusted CA of the peer gateway. This makes sure the CA is uploaded on both the local and peer gateways. See *"Managing Trusted CAs" on page 424*.

Sign a request using one of the gateway's CAs:

You create a request from one gateway that must be signed by the peer gateway's CA:

1. Use the **New Signing Request** option in *"Managing Installed Certificates" on page 215*.

2. Export this request using the **Export** option.

3. Use the peer gateway's internal CA to sign the request on the peer gateway.

   If the peer gateway is a locally managed Check Point gateway, go to **VPN** > **Trusted CAs** and use the **Sign a Request** option.

   For more information, see *"Managing Trusted CAs" on page 424*.

4. Upload the signed request to the local gateway.

   a. Go to **VPN** > **Installed Certificates**.

   b. Select the installed certificate that you asked the remote peer to sign.

   c. Upload the certificate with the **Upload Signed Certificate** option.

      See *"Managing Installed Certificates" on page 215*.

5. Make sure that the CA is installed on both of the gateways. Use the **Add** option in *"Managing Trusted CAs" on page 424*.

**To authenticate by using a 3rd party CA:**

You create a signing request from each peer gateway. Follow the steps above in *Sign a request using one of the gateway's CAs* to sign it with a 3rd party CA.

Note that a 3rd party CA can issue `*.crt`, `*.p12`, or `*.pfx` certificate files.

1. Upload the certificate using the appropriate upload option.

   a. Go to **VPN** > **Installed Certificates**.

   b. Select the installed certificate that you asked the remote peer to sign.

   c. Upload the certificate with the **Upload Signed Certificate** or **Upload P12 Certificate** option.

      See *"Managing Installed Certificates" on page 215*.

2. Make sure that the 3rd party CA is installed on both of the gateways.

   Use the **Add** option in *"Managing Trusted CAs" on page 424*.

**To authenticate with an existing 3rd party certificate:**

1. Create a P12 certificate for the local and peer gateway.
2. Upload the P12 certificate using the **Upload P12 Certificate** option on each gateway.
3. Make sure that the 3rd party CA is installed on both of the gateways.

   Use the **Add** option in *"Managing Trusted CAs" on page 424*.

# Monitoring VPN

**To make sure the VPN is working:**

1. Pass traffic between the local and peer gateway.
2. Go to **VPN** > **VPN Tunnels** to monitor the tunnel status.

   See *"Viewing VPN Tunnels" on page 417*.

# Configuring the Remote Access Blade

On the **VPN** view > **Remote Access** section > **Blade Control** page you can establish secure encrypted connections between devices such as mobile devices, home desktops and laptops, and the organization through the Internet.

For Remote Access VPN, you must configure users on the appliance with credentials and configure the required permissions for specified users. The appliance must be accessible from the Internet.

We highly recommend that you first configure DDNS or an Internet connection with a static IP address on the appliance. If you do not use a static IP address, your appliance's IP address can change based on your Internet Service Provider. DDNS lets home users connect to the organization by hostname and not IP address that can change. See **Device** view > **System** section > **DDNS & Device Access** page > **DDNS** section for more details.

To configure DDNS, see *"Configuring DDNS and Access Service" on page 180*.

To configure the static IP address, see *"Configuring Internet Connectivity" on page 87*.

**Note** - Remote Access VPN supports connections from IPv4 addresses only.

## Getting Started with Remote Access VPN

1. **Enable the Remote Access VPN Blade and configure its features**

a. Go to the **VPN** view > **Remote Access** section > **Blade Control** page.

b. Select **On**.

c. **Mandatory:** Select **Allow traffic from Remote Access users**.

d. **Optional:** Select **Log traffic from Remote Access users**.

e. **Optional:** Select **Require users to confirm their identity using Two-Factor Authentication**.

**Procedure**

Two-Factor Authentication, also called multi-factor authentication, is an extra layer of security to prevent unauthorized access to your system. The gateway sends a passcode to the user by email or SMS to allow the user to connect through VPN. Starting from R81.10.07, you can also select to use Google Authenticator.

To use Two-Factor Authentication, you must have Remote Access permissions configured, with an email address and mobile phone number.

For SMS, you can use the Check Point SMS provider, or an external SMS provider. If a customer uses a public SMS server, the administrator must provide the username and password for the SMTP server and a Dynamic URL that contains the API of the external service provider.

**Notes**:

- By default, the gateway sends the passcode by both email and SMS.
- L2TP and SNX do not support Two-Factor Authentication.
  To make sure these connection work, run this command in Gaia Clish:

  ```
  set vpn remote-access advanced allow-older-
  clients true
  ```

**To configure Two-Factor Authentication:**

i. On the **VPN** view > **Remote Access** section > **Blade Control** page, select **Require users to confirm their identity using Two-Factor Authentication**.

ii. Click **configure**.

   The **Two-Factor Authentication Settings** window opens.

iii. Select the applicable option:

**Note** - The authentication methods are **global settings**, which means they are enforced for all users and groups.
Starting from R81.10.15, you can select to override global settings for **Two-Factor Authentication** and **Route All Traffic** for local users and AD groups. . Set policy per individual user (local or AD group) on the *"Configuring Remote Access Users" on page 374* page.

To select to receive by both SMS and email, select both checkboxes.

**To receive authentication by SMS**

i. Select the **SMS** checkbox.

ii. To use Check Point SMS, select **Use Check Point SMS provider service**.

iii. If you select **Use External SMS provider**, enter the information for these fields:

- **DynamicID URL**
- **Provider user name**
- **Provider password**
- **API ID**
- **Message** to display (optional).

**To receive authentication by Email**

i. Select the **Email** checkbox.

ii. **Optional:** Enter the **Message** to send.

**To receive authentication by SMB Cloud Service (Google Authenticator application)**

**Note** - Users must have Remote Access permissions configured for this option.

i. Select the **Use Google Authenticator** checkbox.

ii. Click **Save**.

The SMB Cloud Service sends an email that contains a QR code to the email address configured for the user.

iii. Scan the QR code with the Google Authenticator application.

    iv. The one-time password (OTP) appears.

    **Note** - The OTP expires after 30 seconds.

    v. On your computer, connect to the VPN. Enter your username and password.

    vi. For the second authentication, enter the OTP in the Response field.

    vii. The Cloud Service compares the OTP to the one represented by the QR code in the application. If it matches, you are connected to VPN.

  The Cloud Service sends a QR code with an OTP when:

  - A new user is configured.
  - The information for an existing user is edited, such as a new email address is added or the user receives Remote Access permissions.
  - The administrator decides that all users must use Cloud Authentication.

iv. On the **Advanced** tab, below **Dynamic ID Settings**, enter the:

- Length of the one-time password.
- Amount of time in minutes until the password expires.
- Maximum number of retries.

v. Below **Country Code**, enter the Default country code.

vi. Click **Save**.

**To sign in with Two-Factor Authentication:**

i. Connect to your VPN.

ii. You get a prompt for a DynamicID One Time Password (OTP) sent to your mobile phone as an SMS, or directly to your email account, or by scanning the QR code.

**Notes**:

- VPN Two-Factor Authentication is per gateway, not administrator.
- When you turn on Two-Factor Authentication, you enable it for all VPN clients. This means all VPN users must have a configured mobile phone number and email address with which to connect.

f. **Optional:** In R81.10.15 and higher: Configure the schedule to enable or disable the Remote Access VPN blade. See *"Remote Access VPN Scheduler" on page 367*.

g. **Optional:** In R81.10.15 and higher: Configure the Allow/Block List to allow or block the Remote Access VPN traffic from specific sources. See *"Allow or Block Remote Access VPN Traffic from Specific Sources" on page 369*.

h. In the section "**VPN Remote Access users can connect via**", select the applicable Remote Access VPN clients.

**Procedure**

The supported Remote Access VPN clients are:

- **Check Point VPN clients** - Install a VPN client on your desktop or laptop.
- **Mobile client** - To connect on your smartphone or tablet (iOS or Android).
- **SSL VPN** - To connect through SSL VPN. Enter the IP address in your web browser.
- **Windows VPN client** - L2TP. For either Windows or macOS, connect with a pre-shared key. For instructions, click **How to connect**.

**To configure Remote Access VPN methods:**

i. Select the checkbox next to the desired method and click **How to connect**.

   The **Usage** window opens.

ii. Follow the instructions on the screen.

iii. Close the window.

iv. Click **Save**.

i. At the bottom of the page, click **Save**.

**Note** - When the Remote Access VPN blade is managed by Cloud Services, a lock icon appears. You cannot toggle between the **On** and **Off** states. If you change other policy settings, the change is temporary. Any changes you made locally are overridden in the next synchronization between the gateway and Cloud Services.

2. **Configure users and user groups for the Remote Access VPN**

Follow the applicable procedure:

**Adding a new local user**

a. Go to the **VPN** view >**Remote Access** section > **Remote Access Users** page.

b. Click **Add**.

   The **New Local User** window opens.

c. Enter the required information in the fields.

> **Note** - The **Email** and **Phone number** fields are optional. However, if you want to give this user Remote Access VPN permissions, this information is necessary for Two-Factor Authentication during the Remote Access VPN connection.

d. In the **Remote Access permissions**, select the applicable options.

e. Click **Save**.

### Adding new users from Active Directory / RADIUS

You can use the Active Directory or RADIUS servers to automatically populate your users and groups.

See *"Configuring Authentication Servers for Remote Access" on page 384*.

To see a table of the defined authentication servers, go to the **VPN** view > **Remote Access** section > **Authentication Servers** page.

### Configuring an existing local user

a. Click the username in the table and click **Edit**.

   You can also double-click the username.

b. Select **Remote Access permissions**.

c. Click **OK**.

### Configuring the permissions for existing local users / user groups

a. Click **Edit permissions**.

b. At the top, click the applicable filter:

   - Click **Users** to see the locally configured users.
   - Click **Active Directory** to see the user groups configured on an Active Directory server.

c. In the left column, select the checkbox near the applicable usernames / user groups.

d. Click **Save**.

3. **Monitor Remote Access VPN**

- To see the currently connected Remote Users, go to the **VPN** view > **Remote Access** section > **Connected Remote Users** page.
- To see the current Remote Access VPN tunnels, go to the **Logs & Monitoring** view > **Status** section > **VPN Tunnels** page.
- To see the traffic from the currently connected Remote Access VPN users, go to the **Logs & Monitoring** view > **Logs** section > **Security Logs** page.

  Note - On the **VPN** view > **Remote Access** section > **Blade Control** page, you must select **Log traffic from Remote Access users**.

# Remote Access VPN Scheduler

Starting from R81.10.15: With the Remote Access VPN Scheduler, you can configure the VPN Remote Access to be active only during specific hours, for example during normal business hours.

On the **VPN Remote Access Control** page, the Remote Access VPN status is shown at the bottom of the **Remote Access** section.

- VPN Remote Access is active
- VPN Remote Access is inactive due to VPN Scheduler
- VPN Remote Access VPN scheduler is not configured

**To configure a new Remote Access VPN schedule**

In the **Remote Access** section of the **VPN Remote Access Control** page:

1. Click the available option:
   - If you did not enable the scheduler yet, WebUI shows this line:

     **The Remote Access VPN scheduler is not configured**

     Click **Configure** at the end of this line.
   - If you already enabled the scheduler, WebUI shows this line:

     **Remote Access VPN is inactive due to the current scheduler configuration**

     Click the link **scheduler** in this line.

   The **Remote Access VPN Scheduler** window opens.
2. To enable this feature, move the slider **Remote Access VPN scheduler is enabled**.

   The slider becomes green.
3. In the line **In the defined time intervals, Remote Access VPN will be**, select the applicable action:
   - **Active** - Enables the Remote Access VPN blade during the configured hours and days.
   - **Inactive** (this is the default) - Disables the Remote Access VPN blade during the configured hours and days.
4. **Optional:** Select **Disconnect VPN users when Remote Access VPN is turned off by the scheduler**.
5. Click **New**.
6. Configure the schedule and click **Save**:

   a. Start time
   b. End time
   c. Days

7. Click **Save**.

### To edit an existing Remote Access VPN schedule

In the **Remote Access** section of the **VPN Remote Access Control** page:

1. In the line **Remote Access VPN is inactive due to the current scheduler configuration**, click the link **scheduler**.
2. Click the schedule.
3. Click **Edit**.
4. Configure the applicable settings and click **Save**.
5. Click **Save**.

### To delete an existing Remote Access VPN schedule

In the **Remote Access** section of the **VPN Remote Access Control** page:

1. In the line **Remote Access VPN is inactive due to the current scheduler configuration**, click the link **scheduler**.
2. Click the schedule.
3. Click **Delete**.
4. Click **Delete** to confirm.
5. Click **Save**.

# Allow or Block Remote Access VPN Traffic from Specific Sources

Starting from R81.10.15, you can block or allow traffic from selected objects, including Network Objects and Updatable Objects (Geo Locations).

**Procedure to add objects to the allow/block list**

In the **Remote Access** section of the **VPN Remote Access Control** page:

1. Click the available option:
   - If you did not enable the allow/block list yet, WebUI shows this line:

     **Access is not allowed/blocked for specific objects**

     Click **Configure** at the end of this line.
   - If you already enabled the allow/block list, WebUI shows this line:

     **Only access from selected objects is allowed**

     Click the link **selected objects** in this line.

   The **Remote Access VPN Allow/Block Lists** window opens.
2. To enable this feature, move the slider **Remote Access VPN Allow/Block lists are enabled**.

   The slider becomes green.
3. In the line **Traffic from the following sources will be**, select the applicable action:
   - **Allowed** (this is the default) - Allows traffic only from the selected objects and blocks traffic from all other sources.
   - **Blocked** - Blocks traffic only from the selected objects and allows traffic from all other sources.
4. Click **+Add** and select **Network object** or **Geo Location**.

   **Important** - By default, this list is empty. Make sure to select the applicable objects to prevent unwanted behavior - allowing all traffic or blocking all traffic.

**For Geo Locations**

a. Click **Geo Locations**.

The **Import Updatable Object** window opens.

b. Enter the applicable text in the **Search** field and select the checkboxes next to the relevant continents and countries that appear.

**Note** - The maximum supported number of selected Geo Location objects in this list is 100. See sk182654.

c. Click **Save**.

**For Network Objects**

a. Click **Network Objects**.

The **Select Network Objects** window opens.

b. Click **New**.

The **New Network Object** window opens.

c. For **Type**, select one of these from the menu:

- **Single IP**
- **IP Range**
- **Network**
- **Wildcard**

d. Enter the **Name** of the object.

e. Enter the **Network address** and the **Subnet mask**.

f. Click **Save**.

### Procedure to delete objects from the allow/block list

In the **Remote Access** section of the **VPN Remote Access Control** page:

1. In the line **Only access from selected objects is allowed**, click the link **selected objects**.
2. In the list, click the object you want to delete.

   You can select only one object at a time.
3. From the toolbar, click **Delete**.
4. Click **Save**.

## Advanced Options

For more information, see *"Configuring Advanced Remote Access Options" on page 399*.

## Changing the Default Remote Access VPN Port

### Procedure

The default Remote Access VPN port on the Quantum Spark Gateway is TCP 443. If you configured the WebUI on the appliance to work on the TCP port 443 as well, a **conflict message** appears on the **VPN** view > **Remote Access** section > **Blade Control** page.

If you enabled one of these Remote Access VPN clients:

- Check Point VPN clients
- Mobile client
- SSL VPN

then you must change the default Remote Access VPN port:

1. Click the **Change port** link.

   The **Remote Access Port Settings** window opens.

2. In the **Remote Access port** field, enter a new port number.
3. Select **Reserve port 443 for port forwarding**.
4. Click **Save**.

# Connections Between Remote Access VPN Clients in the Same Office Mode Pool

Follow this procedure to allow connections between Remote Access VPN clients that get an IP address from the same Office Mode Pool.

**Procedure**

1. Go to the **Users & Objects** view > **Network Resources** section > **Network Objects** page.
2. Click **New** to create a new Network object for the Office Mode network:
   a. In the **Type** menu, select **Network**.
   b. In the **Network address** field, enter the applicable network IP address.
   c. In the **Subnet mask** field, enter the required subnet mask.
   d. In the **Object name** field, enter the applicable name.

      For example: `OMPOOL`.
   e. Click **Save**.
3. Go to the **Device** view > **Advanced** section > **Advanced Settings** page.
4. Configure the parameter **VPN Remote Access - Back Connections enable**:
   a. In the top search field, enter:

      **VPN Remote Access - Back Connections enable**.
   b. Select the parameter **VPN Remote Access - Back Connections enable** and click **Edit**.
   c. Select the option **Back connections enable**.
   d. Click **Save**.
5. Configure an Access Policy rule to allow traffic between computers in the Office Mode network:

a. Go to the **Access Policy** view > **Firewall** section > **Policy** page.

b. In the section **Incoming, Internal and VPN traffic**, click **New**.

c. Configure this rule:

| Source | Destination | Service | Action | Log |
|---|---|---|---|---|
| *OMPOOL* | *OMPOOL* | `*Any` | `Accept` | `Log`, or `None` |

d. Click **Save**.

6. Configure the NAT Policy rule to disable NAT on the traffic between computers in the Office Mode network:

a. Go to the **Access Policy** view > **Firewall** section > **NAT** page.

b. In the section **NAT Rules**, click **View NAT rules**.

c. Click **New**.

d. Configure this rule:

| Original Source | Original Destination | Original Service | Translated Source | Translated Destination | Translated Service |
|---|---|---|---|---|---|
| *OMPOOL* | *OMPOOL* | `*Any` | `*Original` | `*Original` | `*Original` |

e. Click **Save**.

# Configuring Remote Access Users

On the **VPN** > **Remote Access** section > **Remote Access Users** page, you can configure Remote Access VPN permissions for individual users and user groups.

You can configure users and user groups on the **Users & Objects** view > **Users Management** > **Users** page.

The **Remote Access Users** page is dedicated to users with Remote Access VPN permissions.

You can configure:

- Local users
- Local user groups
- Active Directory users (R81.10.15 and higher)
- Active Directory user groups
- Active Directory permissions
- Azure AD (now known as Microsoft Entra ID) (in versions R81.10.15 and higher
- RADIUS groups
- RADIUS users ( in versions R81.10.15 and higher)

You can also configure SSL VPN bookmarks by user, user group, RADIUS users and Active Directory group.

**Best Practice** - If no authentication servers are defined, click the **Active Directory / RADIUS** link at the top to define them.

**Note** - When **User Awareness** is turned off, there is no user identification based on Browser-Based Authentication and Active Directory Queries.

# Adding Remote Access Permissions to a Specific Local User

### Procedure

1. Near the **Add** button, click the downward arrow > click **New Local User**.
2. In the **Remote Access** tab:
    a. In the **Name** field, enter a username.
    b. In the **Password** field, enter a password.

        **Note** - The password can be up to 100 characters.

    c. In the **Confirm Password** field, enter the password again.
    d. In the **Email** field, enter the user's email. This is required for Two-Factor Authentication.
    e. In the **Mobile phone number** field, enter the user's phone number. This is required for Two-Factor Authentication.
    f. **Optional:** In the **Comments** field, enter the applicable description for this user.
    g. Select **Temporary user** if you configure a temporary user.

        Enter the expiration date and time.

h. Select **Remote Access permissions.**

   Starting from R81.10.15, two additional checkboxes appear:

   i. **Optional:** Select **Use Office Mode static IP address** and enter the desired IP address for Office Mode. Instead of getting the WAN IP address allocated dynamically from the gateway, the user receives the static IP address associated with that user.

   ii. **Optional:** Select **Override global settings** to configure policy per individual user instead of applying the settings on the gateway.

      Two additional checkboxes appear:

      - **Optional:** Select **Route all traffic for this user through VPN** to route the traffic for this user through the VPN tunnel.
      - **Optional:** Select **Enable Two-Factor Authentication (2FA) enforcement** to enforce Two-Factor Authentication for this user.

        Select the applicable option:

        - **Use SMS/email**
        - **Use an Authenticator app**

3. **Optional:** In the **SSL VPN Bookmarks** tab:

   a. Click **Add** > **New Local User/Users Group/Active Directory Group** > **SSL VPN Bookmarks** tab.

   b. In the new window, enter new bookmarks or select existing bookmarks.

      **Note** - If you select the **Global bookmark**, this bookmark always appears.

   c. Click **Save**.

4. Click **Save**.

## Adding Remote Access Permissions to a Local User Group

### Procedure

1. Near the **Add** button, click the downward arrow > click **New Users Group**.
2. In the **Remote Access** tab:
   a. In the **Group name** field, enter the group name.
   b. Select **Remote Access permissions**.
   c. Select initial users to add to the group by selecting the relevant checkboxes in the user list or by clicking **New** to create new users.

      You can see a summary of the group members above the user list.

      You can remove members by clicking the **X** next to the relevant user name.
3. **Optional:** In the **SSL VPN Bookmarks** tab:
   a. Click **Add** > **New Local User/Users Group/Active Directory Group** > **SSL VPN Bookmarks** tab.
   b. In the new window, enter new bookmarks or select existing bookmarks.

      ⓘ **Note** - If you select the **Global bookmark**, this bookmark always appears.

   c. Click **Save**.
4. Click **Save**.

# Adding Remote Access Permissions to Active Directory Users

### Procedure to add Remote Access permissions to an Active Directory specific user

**Note** - This feature is available in R81.10.15 and higher.

1. Near the **Add** button, click the downward arrow > click **Active Directory** > click **Active Directory User**.
2. If no Active Directory was defined, you are prompted to configure one.

   For more information on configuring Active Directory see *"Configuring Authentication Servers for Remote Access" on page 384*.
3. In the **Name** field, enter the username as configured in Active Directory.
4. In the **Email** field, enter the user's email as configured in Active Directory.
5. **Optional:** Select **Override global settings** to configure policy per individual user instead of applying the settings on the gateway.

   Two additional checkboxes appear:

   - **Optional:** Select **Route all traffic for this user through VPN** to route the traffic for this user through the VPN tunnel.
   - **Optional:** Select **Enable Two-Factor Authentication (2FA) enforcement** to enforce Two-Factor Authentication for this user.

     Select the applicable option:

     - **Use SMS/email**
     - **Use an Authenticator app**

     When this Remote Access VPN user connects to the Quantum Spark Gateway for the first time, the credentials are sent to the Active Directory server. After confirmation from the Active Directory server, the Quantum Spark Gateway sends a one-time code in an SMS or Email, or the user must enter a one-time from an Authenticator app.
6. Click **Save**.

In addition, refer to *"Procedure to add Remote Access permissions to all users defined in an Active Directory" on the next page*.

### Procedure to add Remote Access permissions to an Active Directory user group

1. Do one of these:
   - From the toolbar, click **Edit Permissions**.
   - Near the **Add** button, click the downward arrow > click **Active Directory** > click **Active Directory Group**.
2. Near the **Add** button, click the downward arrow > click **Active Directory** > click **Active Directory Group**.
3. If no Active Directory was defined, you are prompted to configure one.
4. When an Active Directory has been defined, you see a list of available user groups defined in the server.
5. Select one of the user groups.
6. Click **Save**.

### Procedure to add Remote Access permissions to all users defined in an Active Directory

1. Near the **Add** button, click the downward arrow > click **Active Directory** > click **Active Directory Permissions**.
2. Select the applicable option:
   - **All users in Active Directory**

     **Note** - Most Active Directory domains contain a large list of users. Consider limiting the Remote Access VPN permissions only to specific user groups.
   - **Selected Active Directory user groups** (this is the default)

     **Note** - Requires additional configuration.
3. Click **Save**.
4. If you selected the option **Selected Active Directory user groups**, then follow *"Procedure to add Remote Access permissions to an Active Directory specific user" on the previous page*.

### Procedure to add Remote Access permissions to an Azure AD (now known asMicrosoft Entra ID) user group

**Note** - This feature is available in R81.10.15 and higher.

1. Near the **Add** button, click the downward arrow > click **Active Directory** > click **Azure AD Group**.
2. In the **Name** field, enter the user group name as configured in Microsoft Entra ID.

   **Important** - On the Quantum Spark Gateway, this name must always start with the prefix "`EXT_ID_`".
   Example:
   If the Azure AD group is called "`VPN_Users`", then you must enter "`EXT_ID_VPN_Users`".
3. **Optional:** In the **Comments** field, enter the applicable description for this Microsoft Entra ID user group.
4. **Optional:** Select **Override global settings** to configure policy per individual user instead of applying the settings on the gateway.

   **Optional:** Select **Route all traffic for this Azure AD group through VPN** to route the traffic for this user group through the VPN tunnel.

For more information, see *"Configuring SAML Authentication for Remote Access VPN" on page 390*..

# Adding Remote Access Permissions to RADIUS Users

### Procedure to add Remote Access permissions to a RADIUS user group

1. Near the **Add** button, click the downward arrow > click **RADIUS** > click **RADIUS Group**.
2. Select **Enable RADIUS authentication for User Awareness, Remote Access and Hotspot**.
3. **Optional: Select For Remote Access use specific RADIUS groups only**.

   In the field **RADIUS groups for authentication**, enter the applicable RADIUS groups.
4. Click **Save**.

### Procedure to add Remote Access permissions to a RADIUS specific user

**Note** - This feature is available in R81.10.15 and higher.

1. Near the **Add** button, click the downward arrow > click **RADIUS** > click **RADIUS User (Two-Factor Authentication)**.
2. In the **Name** field, enter a username.
3. In the **Email** field, enter the user's email. This is required for Two-Factor Authentication.
4. In the **Phone number** field, enter the user's phone number. This is required for Two-Factor Authentication.
5. **Optional:** Select **Override global settings** to configure policy per individual user instead of applying the settings on the gateway.

   Two additional checkboxes appear:

   - **Optional:** Select **Route all traffic for this user through VPN** to route the traffic for this user through the VPN tunnel.
   - **Optional:** Select **Enable Two-Factor Authentication (2FA) enforcement** to enforce Two-Factor Authentication for this user.

     Select the applicable option:

     - **Use SMS/email**
     - **Use an Authenticator app**
6. Click **Save**.

# Deleting an Existing User or User Group

### Procedure

1. Click the user or user group object.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

# Viewing Connected Remote Access Users

On the **VPN** view > **Remote Access** section > **Connected Remote Users** page, you can see the currently connected Remote Access VPN users:

- Username
- IP address
- Connection Time

# Configuring Authentication Servers for Remote Access

On the **VPN** view > **Remote Access** section > **Authentication Servers** page, you can configure and view different authentication servers for Remote Access VPN users who connect to the Quantum Spark Gateway (with the **Remote Access** blade enabled - see *"Configuring the Remote Access Blade" on page 355*).

You can configure these authentication methods:

| Authentication Method | Description |
|---|---|
| **RADIUS** | When a Remote Access VPN user connects, the Quantum Spark Gateway connects to the configured RADIUS servers to authenticate the user.<br>You configure the RADIUS servers on the **VPN** view > **Remote Access** section > **Remote Access Users** page. |
| **Active Directory** | When a Remote Access VPN user connects, the Quantum Spark Gateway connects to the configured Active Directory servers to authenticate the user.<br>You configure the Active Directory servers on the **VPN** view > **Remote Access** section > **Remote Access Users** page. |
| **SAML Identity Provider** | **Note** - This feature is available in versions R81.10.15 and higher.<br>When a Remote Access VPN user connects, the Quantum Spark Gateway connects to the configured SAML Identity Provider to authenticate the user.<br>You must configure the required settings in the SAML Identity Provider portal. |

## Configuring RADIUS Authentication for Remote Access VPN

**Configuring new RADIUS servers**

1. In the **RADIUS Servers** section, click **Configure**.
2. In the **Primary** tab, configure the Primary RADIUS server:

- **IP address** - The IP address of the Primary RADIUS server.
- **Port** - The number of the listening port on the Primary RADIUS server. The default is 1812.
- **Shared secret** - The secret (pre-shared information used for message "encryption") between the Primary RADIUS server and the Quantum Spark Gateway.

  **Notes:**
  - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)
  - Select **Show** to see the shared secret.
- **Timeout (seconds)** - A timeout value in seconds for communication with the RADIUS server. The default timeout is 3 seconds.

**Note** - To remove all settings, click **Clear**.

3. **Optional:** In the **Secondary** tab, configure the Secondary RADIUS server:
   - **IP address** - The IP address of the Secondary RADIUS server.
   - **Port** - The number of the listening port on the Secondary RADIUS server. The default is 1812.
   - **Shared secret** - The secret (pre-shared information used for message "encryption") between the Secondary RADIUS server and the Quantum Spark Gateway.

     **Notes:**
     - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)
     - Select **Show** to see the shared secret.
   - **Timeout (seconds)** - A timeout value in seconds for communication with the RADIUS server. The default timeout is 3 seconds.

   **Note** - To remove all settings, click **Clear**.
4. Click **Save**.
5. Enable the Remote Access permissions for RADIUS users:

   a. In the line **Remote Access permissions for RADIUS users are disabled**, click the link **permissions for RADIUS users**.

   The **RADIUS Authentication** window opens.

b. Select **User Awareness, Remote Access and Hotspot**.

c. **Optional:** Select **For Remote Access use specific RADIUS groups only** and enter the names of the applicable RADIUS groups.

d. Click **Save**.

### Editing an existing RADIUS server

1. In the **RADIUS Servers** section, click the IP address link of the RADIUS server you want to edit.
2. Make the necessary changes.
3. Click **Save**.

### Deleting an existing RADIUS server

In the **RADIUS Servers** section, click the **Remove** link next to the RADIUS server you want to delete

# Configuring Active Directory Authentication for Remote Access VPN

### Configuring new Active Directory Domain

1. In the **Active Directory** section, click **New**.
2. Configure the **Active Directory Domain** settings:
   - **Domain** - The domain name.

     You can configure this domain only one time.
   - **IP address** - The IPv4 address of one of the Active Directory domain controllers of your domain.
   - **User name** - The username to connect to the Active Directory domain controller. This user must have administrator privileges to ease the configuration process and create a user-based policy using the users defined in the Active Directory.

     **Note**
     The **Full Name** and **User Logon Name** must begin with a letter and have a maximum length of 20 characters. Only the following characters can be used, with no spaces in between:
     - a-z (lower-case letters)
     - A-Z (upper-case letters)
     - 0-9 (digits)
     - '_' (underscore)
     - '-' (minus)
     - '~' (tilde)
     - ',' (comma)

     The **Display Name** can contain any characters.
   - **Password** - The user's password to connect to the Active Directory domain controller.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ‵ " \ (maximum number of characters: 255)
   - **User DN** - The user's FQDN. Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually.

     For example: CN=John James,OU=RnD,OU=Germany,O=Europe,DC=Acme,DC=com

- **Optional:** Select **Use user groups from specific branch only** if you want to use only part of the user database defined in the Active Directory:
    a. Click **New**.

    b. Enter the full DN of the applicable Active Directory branch.

    - For an AD branch that is the default folder of the AD server (usually "Users") enter:

      CN=<branch name>,DC=<Domain name>,DC=<Domain suffix>

    - For other branches enter:

      OU=<branch name>,DC=<Domain name>,DC=<Domain suffix>

    c. Click **Save**.

3. Click **Save**.

4. Configure how to synchronize Active Directory groups from the Active Directory domain controller:

    a. In the **Active Directory** section, click **Configure**.

    b. Select the applicable option:

    - **Automatic synchronization** (this is the default, runs every 24 hours)
    - **Manual synchronization**

    **Note** - You can synchronize the user database in all locations in WebUI where this user database can be viewed.
    For example:
    - The **Users & Objects** view > **Users Management** section > **Users** page.
    - The **Access Policy** view > **Firewall** section > **Policy** page.
      In the **Incoming, Internal and VPN Traffic** section > the **Source** column > click **[+]**.
      Note - You cannot select a user from the Active Directory, only an Active Directory user group.

    c. Click **Save**.

5. Enable the Remote Access permissions for Active Directory users:

    a. In the line **Remote Access permissions for Active Directory users are set in the Remote Access Users page**, click the link **permissions for Active Directory users**.

    The **Active Directory Global Permissions** window opens.

b. Select the applicable option:

- **All users in Active Directory**

  **Note** - Most Active Directory domains contain a large list of users. Consider limiting the Remote Access VPN permissions only to specific user groups.

- **Selected Active Directory user groups** (this is the default)

  **Note** - Requires additional configuration. Follow *"Configuring Remote Access Users" on page 374*.

c. Click **Save**.

### Editing an existing Active Directory Domain

1. In the **Active Directory** section, click the Active Directory Domain you want to edit.
2. Click **Edit**.

   The Domain information is read-only and cannot be changed.
3. Make the necessary changes.
4. Click **Save**.

### Deleting an existing Active Directory Domain

1. In the **Active Directory** section, click the Active Directory Domain you want to delete.
2. Click **Delete**.

# Configuring SAML Authentication for Remote Access VPN

Starting from R81.10.15, you can configure a SAML Identity Provider (IdP) to authenticate Remote Access VPN users on a Quantum Spark Gateway.

**Note** - The R81.10.15 version supports only Microsoft Entra ID (formerly Azure AD).

### Use Case

Remote Access VPN users enter their Microsoft Entra ID credentials to connect to the Quantum Spark Gateway and access the internal resources.

This is easier than using specific credentials only for the Quantum Spark Gateway.

The administrator can manage user groups and enforce authentication methods such as Single Sign-On (SSO) and Two-Factor Authentication (2FA) in the Microsoft Entra ID portal.

In the advanced use case, you can override the **Route Internet traffic from connected clients through this Security Gateway** global configuration for specific groups in Microsoft Entra ID. For more information about **Route Internet traffic from connected clients through this Security Gateway**, see *"Configuring Advanced Remote Access Options" on page 399*.

### User Experience

1. A Remote Access VPN user wants to access internal resources located behind the Quantum Spark Gateway using Remote Access VPN.
2. The SAML portal of the Quantum Spark Gateway redirects the user to the SAML Identity Provider (IdP) for authentication.
3. The IdP asks the remote user for credentials according to the policy you configure in the IdP portal.

   For example, you can configure Single Sign-On (SSO) to recognize that a user is already signed in, or require Two-Factor Authentication (2FA).
4. The IdP authenticates the user and sends a SAML assertion to the user's web browser.
5. The remote user's web browser sends the SAML assertion to the Quantum Spark Gateway.
6. The Quantum Spark Gateway validates the SAML assertion and allows the remote user to access internal resources.

### Known Limitations

- Only one IdP configuration is supported. For example, if your organization has two Microsoft Entra ID environments, you can use only one of them as a SAML Identity Provider
- It is not supported to create Access Control Rules for users who authenticate with the SAML Identity Provider.
- Microsoft Entra ID Identity Tags are not supported.

**Important** - The admin must notify Remote Access users to save the Azure credentials they receive. These credentials are required for their first login using the **SAML User** authentication method.

### Basic Configuration

Keep the Azure Portal and the Quantum Spark Gateway WebUI open throughout this procedure.

1. In the Azure Portal, create a SAML application for the Quantum Spark Gateway:
   a. Click **Enterprise Application**.
   b. Click **New application**.
   c. Click **Create your own application**.

      The **Create your own application** window opens.
   d. Enter a name for the application.
   e. Make sure this default option is selected:

      **Integrate any other application you don't find in the gallery (Non-gallery)**
   f. Click **Create**.
2. In the Azure Portal, assign users or groups of users to the SAML application:
   a. On the **Overview** page for the application, in the **Getting Started** section, click **Assign users and groups**.
   b. Click **add user/group**.
   c. Select users and groups.
   d. Click **Assign**.
3. In the Azure Portal, navigate to the **SAML-based Sign-on** screen for your application:

  a. In the left menu, expand **Manage**.
  b. Click **Single sign-on**.
  c. Select **SAML**.
  d. In the **Basic SAML Configuration** section, click the edit (pencil) icon.

     The **Basic SAML Configuration** window opens.

4. In the Quantum Spark Gateway WebUI, from the left navigation panel, click the **VPN** view.
5. In the **Remote Access** section, click the **Authentication Servers** page.
6. In the **Identity Provider** section, click **Configure**.

   The **Configure Identity Provider** window opens.

7. In the **Data required by the SAML Identity Provider** section, follow these steps:
   a. Copy these values from the Quantum Spark Gateway WebUI and paste them in the Azure portal > **Basic SAML Configuration** window:
      - Copy the **Unique identifier URL** value from the Quantum Spark Gateway WebUI and paste it in the Azure portal in the **Identifier (Entity ID**) field.
      - Copy the **Reply URL** from the Quantum Spark Gateway WebUI and paste it in the Azure portal in the **Reply URL** (**Assertion Consumer Service URL**) field.

      **Note** - By default, the WebUI generates these values based on the DDNS settings in the **Device** view > **System** section > **DDNS & Device Access** page. If you did not configure DDNS, these values are based on the appliance's public IP address. If you did not configure DDNS for a cluster, these values are based on the cluster's Virtual IP Address (VIP).

b. **Optional:** You can override the DDNS or IP address of the Quantum Spark Gateway:

   - To use a static IPv4 address instead of DDNS, select **Override DDNS/IP** and enter an IPv4 address.

     The Quantum Spark Gateway WebUI generates a new **Unique identifier URL** and **Reply URL** based on the IPv4 address.These fields are automatically generated the first time the user configures the identity provider object on the gateway.

     If DDNS was configured before, these fields are created with the domain name. Otherwise, they are created with the gateway's IP.

   - To use DDNS instead of a static public IP address for the **Unique identifier URL** and **Reply URL**, select **Override DDNS/IP** and enter a DDNS.

   **Example:** You configured DDNS but want to use an IP address for the **Unique Identifier URL** and the **Reply URL**. After you select the checkbox **Override DDNS/IP** and enter an IP address, the values of the **Unique Identifier URL** and the **Reply URL** change, because they are now based on the IP address, not the DDNS.

c. In the Azure portal > **Basic SAML Configuration** window, click **Save**.

8. In the **Data received by the SAML Identity Provider** section, select and configure the applicable option:

   - **Import Metadata File**

     a. In the Azure Portal >**SAML Certificates** section, next to **Federation Metadata XML**, click **Download**.

        Your computer downloads the metadata file.

     b. In the Quantum Spark WebUI > **Data received from SAML Identity Provider** section, next to **Metadata file**, click **Upload**.

     c. On your computer, select the metadata file and click **Open**.

- **Insert manually**
  1. In the Azure portal > **Set up [NAME OF YOUR APPLICATION]** section, copy the **Microsoft Entra Identifier**.
  2. In the Quantum Spark Gateway WebUI > **Data received from the SAML Identity Provider** section, paste the **Microsoft Entra Identifier** you copied from the Azure portal.
  3. In the Azure portal > **Set up [NAME OF YOUR APPLICATION]** section, copy the **Login URL**.
  4. In the Quantum Spark Gateway WebUI > **Data received from the SAML Identity Provider** section, paste the **Login URL** you copied from the Azure portal.
  5. In the Azure portal >**SAML Certificates** section, next to **Certificate (Base64)**, click **Download**.

     Your computer downloads the certificate file.
  6. In the Quantum Spark Gateway WebUI > **Data received from SAML Identity Provider** section, next to **Certificate**, click **Upload**.
  7. On your computer, select the certificate file and click **Open**.

9. In the Quantum Spark Gateway WebUI, click **Save**.
10. There are two possible deployment scenarios:
    - The Quantum Spark Gateway is already installed and has an existing Remote Access community with a different authentication method, and the administrator wants to change the method to "**SAML User**."
      1. Instruct members of the Remote Access community to disconnect from the site and connect again. Select "**SAML User**" as the preferred login option.
      2. The user, on connecting to the Gateway, is redirected to **Azure** to enter their Azure credentials.
      3. On verification, the Remote Access User gets access to corporate resources.

- The Quantum Spark Gateway is already installed but has no Remote Access community and the administrator creates it for the first time.

  a. Instruct members of the Remote Access community to create the site with the Quantum Spark Gateway as the URL. ("**SAML User**" is already set as the default authentication method).

  b. The user, on connecting to the Gateway, is redirected to Azure to enter their Azure credentials.

  c. On verification, the Remote Access User gets access to corporate resources.

For more information, see:

- *Remote Access VPN Clients for Windows Administration Guide* > "Getting Started with Remote Access Clients" > "Helping Users Create a Site"
- *Endpoint Security VPN for macOS Administration Guide* > "Helping Your Users" > "Helping Users Create a Site".

## Advanced Configuration

### Override the global "Route Internet traffic connected clients through this Security Gateway" configuration

In the basic configuration, the global setting of **Route Internet traffic from connected clients through this Security Gateway** applies to remote users who authenticate with Microsoft Entra ID.

In the advanced configuration, you can override the global setting of **Route Internet traffic from connected clients through this Security Gateway** for specific groups in Microsoft Entra ID.

For more information about **Route Internet traffic from connected clients through this Security Gateway**, see *"Configuring Advanced Remote Access Options" on page 399*.

Do this procedure for one or more groups in Microsoft Entra ID.

**Step 1: In the Microsoft Azure portal, create an app registration**

1. Put the relevant Microsoft Entra ID users into a group (example: `VPN_Users`) and assign this group to the SAML application you created for the Quantum Spark Gateway.
2. In the Azure Portal, click **App registrations**.

   The **App registrations** homepage opens.
3. Click **All applications**.
4. Click the application you created for the Quantum Spark Gateway.

   The **App registrations** page for the application opens.
5. From the left menu, expand **Manage** > click **App roles**.
6. Click **Create app role**.

   The **Create app role** sliding window opens.
7. In the **Display name** field, enter a name for the app role. We recommend to make this the same as the name of the group (in our example: `VPN_Users`).
8. In the **Value** field, enter the name of the group (in our example: `VPN_Users`).
9. Enter a Description for the app role.
10. Select the checkbox below **Do you want to enable this app role?**
11. Click **Apply**.

#### Step 2: In the Microsoft Azure portal, assign a role to the group

1. In the upper left, click **Home**.
2. Click **Enterprise Applications**.
3. Click the name of the application you created for the Quantum Spark Gateway.
4. From the left menu, expand **Manage** > click **Users and Groups**.
5. Select the checkbox to the left of the name of the relevant group.
6. Click **Edit assignment**.
7. Select the group for which you created the app registration.
8. Click **Select a role**.
9. Select the role (in our example: `VPN_Users`) you assigned to the group.
10. Click **Save**.
11. Click **Assign**.

#### Step 3: In the Microsoft Azure portal, add a claim to the SAML application you created for the Quantum Spark Gateway

1. In the upper left, click **Home**.
2. Click **Enterprise Applications**.
3. Click the name of the application you created for the Quantum Spark Gateway.
4. From the left menu, expand **Manage** > click **Single sign-on**.
5. In the **Attributes & Claims** section, click **Edit**.
6. Click **Add new claim**.
7. For **Name**, enter `group_attr`.
8. For **Source**, select **Attribute**.
9. For Source attribute, select `user.assignedroles`.
10. Click **Save**.

### Step 4: In the Quantum Spark Gateway WebUI, create a group for users who authenticate with Microsoft Entra ID

1. Go to the **VPN** view > **Remote Access** section > **Remote Access Users** page
2. Near the **Add** button, click the downward arrow > **Active Directory** > **Azure AD Group**.
3. In the **Name** field, enter the group name as configured in Microsoft Entra ID.

   ℹ **Important** - On the Quantum Spark Gateway, this name must always start with the prefix "`EXT_ID_`".
   Example:
   If the Azure AD group is called "`VPN_Users`", then you must enter "`EXT_ID_VPN_Users`".
4. Click **Save**.

### Step 5: In the Quantum Spark Gateway WebUI, edit the group to override the "Route Internet traffic connected clients through this Security Gateway" configuration

1. Go to the **VPN** view > **Remote Access** section > **Advanced** page
2. In the table, click the name of a group you selected for users who authenticate using Microsoft Entra ID.

   The **Edit [NAME OF THE GROUP]** window opens.
3. Select **Override global settings**.
4. Do one:
   - Select **Route all traffic for this Azure AD group through VPN** to override the global setting. For members of the group, all traffic goes through the VPN tunnel.
   - Leave the **Route all traffic for this Azure AD group through VPN** blank to override the global setting. For members of the group, only traffic to resources behind the Quantum Spark Gateway goes through the VPN tunnel.
5. Click **Save**.

# Configuring Advanced Remote Access Options

In the **VPN** > **Remote Access Advanced** page you can configure more advanced settings to determine VPN remote access users' behavior.

You can also add bookmarks (HTML links or RDP links) for specified URLs or computers when you connect through SSL VPN (see below). The next time you log in, your bookmarks are shown.

## Office Mode

Remote access VPN clients connect through a VPN tunnel from their homes to the appliance and from there they can gain access into the organization's resources.

The appliance assigns each remote access user an IP address from a specified network so that the traffic inside the organization is not aware that it originated from outside the organization.

This technology is called Office Mode and the network used for supplying the IP addresses is configurable.

**To configure the Office Mode network**

1. Enter the **Office Network address** and **Office Subnet Mask**.
2. Click **Apply**

   The default setting for office mode is 172.16.10.0/24.

**To assign a VPN certificate**

1. In the **Advanced** page > Certificate authentication section, select one of these options:
   - Automatically use the last installed certificate.
   - Manually choose a VPN certificate - Select a certificate from the list of uploaded certificates in the drop-down menu.
2. Click **Apply**.

**To route all traffic from VPN remote access clients through the gateway**

1. Select the **Route Internet traffic from connected clients through this gateway** checkbox.
2. Starting from R81.10.10, you can select the **Restrict VPN Remote Access implied rule** checkbox to disable implied rules and restrict Remote Access VPN according to the Access Policy.
3. Click **Apply**.

Normally, only traffic from the VPN clients into the organization's encryption domain is encrypted and sent through the VPN tunnel to the gateway. Selecting the above checkbox causes all traffic from the VPN clients to be encrypted and sent to the gateway. Traffic to locations outside the organization are enforced in this case by the outgoing access Policy. For more information, see **Access Policy Firewall Blade Control** and **Policy** pages.

**Notes:**

- This setting does not apply to traffic from SSL Network Extender clients.
- In R81.10.15 and higher, this setting applies to traffic from users who authenticate with a SAML Identity Provider only if you create an advanced configuration of the SAML connection. See *"Configuring SAML Authentication for Remote Access VPN" on page 390*.

**To configure a local encryption domain manually for remote access users only**

The local encryption domains are the internal networks accessible by encrypted traffic from remote access VPN users. By default, the local encryption domain is determined automatically by the appliance. Networks behind LAN interfaces and trusted wireless networks are part of the local encryption domain.

Optionally, you can manually create a local encryption domain to be used by remote access users only instead. It is possible to configure a different manual local encryption domain for VPN remote access and VPN site to site. See **VPN** > **Site to Site Blade Control** page.

1. Click on the local encryption domain link: **automatically according to topology** or **manually**. The link shown is a reflection of what is currently configured.
2. Select **Define local network topology manually**.
3. Click **Select** to show the full list of available networks and choose the relevant checkboxes.
4. Click **New** if the existing list does not contain the networks you need. For information on creating a new network object, see the **Users & Objects** > **Network Objects** page.
5. Click **Apply**.

   The **Remote Access Local Encryption Domain** window opens and shows the services you selected.

## DNS Servers for Remote Access users

You can define up to three DNS servers for Remote Access clients. By default, the **Office mode first DNS for clients** is set to this gateway.

**To use a different DNS Primary server**

1. Click **Configure manually**.
2. In **Office mode first DNS for clients**, enter the IP address of a server to use as the DNS server.
3. Click **Apply**.

# DNS Domain Name

You can set a DNS domain name that the Remote Access clients' devices automatically use to attempt to resolve non-FQDN domains. By default, the suffix is automatically configured to take the DNS domain name configured in the DNS page.

**To configure a manual DNS domain name**

1. Click **Configure manually**.
2. In **DNS domain name**, enter the DNS domain name suffix to use.
3. Click **Apply**.

**To configure the DNS domain name to be the same as the defined DNS domain name**

1. Click **Configure automatically**.
2. Click **Apply**.

   The DNS domain name shows the text "Same as DNS domain name".

# SSL VPN bookmarks

**To configure SSL VPN bookmarks**

1. Click **Add** > **New Local User/Users Group/Active Directory Group** > **SSL VPN Bookmarks** tab.

   A new window opens.
2. Enter new bookmarks or select existing bookmarks.

   **Note** - If you select **Global bookmark**, this bookmark is always shown.
3. Click **Apply**.

### To set SSL VPN bookmarks

1. In **SSL VPN bookmarks,** click **New** to create new bookmarks.

   A new window opens.

2. Enter these details:

   - **URL**

     **Note** - If you select **Global bookmark**, then all users see this bookmark.

   - **Type** - Link or RDP (remote desktop protocol)
   - **Label** - The bookmark name
   - **Tooltip** - Description

3. Click **Apply**.

If you select RDP as the bookmark type, you must enter the user name and password in the **RDP Advanced Settings**. These credentials are sent to the end user.

**Note** - Select **Show characters** to see the password characters.

You can also specify the screen size of the remote desktop.

The default mode is full screen.

### To manage SSL VPN bookmarks

1. Click on a bookmark.
2. Click **Edit** or **Delete**.
3. Click **Apply**.

# Configuring the Site to Site VPN Blade

In the **VPN** > **Site to Site Blade Control** page you can activate the appliance's ability to create VPN tunnels with remote sites. Site to Site VPN can connect two networks separated by the Internet through a secure encrypted VPN tunnel. This allows for seamless secure interaction between the two networks within the same organization even though they are physically distant from each other.

On this page you can activate the blade to allow site to site connectivity. You can view how many sites are already defined and configure basic access policy from the remote sites into the specific network accessible by this gateway.

The remote site can be accessible through another Check Point appliance (recommended) or a 3rd party VPN solution.

- ZScaler
- strongSwan (authentication based on X.509 certificates)

  **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

Once defined, access to the remote site is determined by the incoming/internal/VPN traffic Rule Base as seen in the **Access Policy** > **Firewall Policy** page. This is due to the fact that the remote site's encryption domain is considered part of the organization even though traffic to it is technically outgoing to the Internet (since it is now VPN traffic).

**To enable or disable the VPN Site to Site blade:**

1. Select **On** or **Off**.
2. Click **Apply**

**Note** - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in the next synchronization between the gateway and Cloud Services.

A warning icon is shown if the blade is active but no VPN sites are defined. Click **VPN Sites** to add a VPN site or see how many VPN sites are defined. The full list of the sites is located in **VPN** > **Site to Site VPN Sites**.

**To configure the default access policy from remote VPN sites:**

1. Select or clear the **Allow traffic from remote sites (by default)** checkbox. It is not recommended to clear this checkbox, as the remote site is usually part of your organization.
2. Select or clear the **Log remote sites traffic (by default)** checkbox.
3. Click **Apply**

### Local Encryption Domain

The local encryption domain defines the internal networks accessible by encrypted traffic from remote sites and networks, that traffic from them to remote sites is encrypted. By default, the local encryption domain is determined automatically by the appliance. Networks behind LAN interfaces and trusted wireless networks are part of the local encryption domain. Optionally, you can manually create a local encryption domain instead. See the **VPN** > **Site to Site Advanced** page for instructions.

# Harmony Connect

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

From your Quantum Spark Appliance, you can set up a VPN connection with Harmony Connect to provide security and other services for your Security Gateway.

First, you must enable the IKEv2 Key Type for FQDN in *"Advanced Settings" on page 246*.

**To establish a connection from your appliance with Harmony Connect:**

1. In the **VPN Site to Site** page, select one of these options to activate Harmony Connect:
   - Create a new VPN site which creates a new instance of a VPN site inside Harmony Connect and then creates tunnels to establish the connection.
   - Connect to an existing VPN site and create the tunnels.

   Enter the required information and click **Apply**.

   The activation details are supplied by your Harmony Connect provider.
2. Follow the steps to establish the connection.

   This may take a few minutes.

For more information on how to set up this connection, see these:

- *Harmony Connect Administration Guide*.
- *Harmony Connect for SMB Gateways Integration Guide*.

# Configuring VPN Sites

In the **VPN** > **Site to Site** > **VPN Sites** page you can configure remote VPN sites. All configured VPN sites appear in the table.

For more on how to configure site to site VPN, go to **VPN** > **Site to Site** > **Blade Control**.

When you add a new VPN site, these are the tabs where you configure these details:

- **Remote Site** - Name, connection type, authentication method (preshared secret or certificate), and the Remote Site Encryption Domain.
- **Encryption** - Change the default settings for encryption and authentication details.
- **Advanced** - Enable permanent tunnels, disable NAT for this site, configure encryption method, and additional certificate matching.

**To add a new VPN site:**

1. Click **New**.

   The **New VPN Site** window opens in the **Remote Site** tab.

2. Enter the **Site name.**
3. Select the **Connection type**:
   - **Host name or IP address** - Enter the **IP address** or **Host name**.

     If you select IP address, and it is necessary to configure a static NAT IP address, select **Behind static NAT** and enter the IP address.

     **Note** - Behind static NAT applies to IPv4 addresses only.

- **High Availability** or **Load Sharing** - When you select this option, you must configure a probing method on the **Advanced** tab. The probing method monitors which IP addresses to use for VPN: ongoing or one at a time.

  Load Sharing mode - Configure a list of backup IP addresses to distribute data.

  High Availability mode:

  - Configure a list of backup IP addresses in case of failure.
  - **Primary IP address** - Configure one of the existing IP addresses as the primary, or add an **IP address** and set it as the primary.

  The status of VPN sites whose hosts or IP addresses are in High Availability or Load Sharing mode are displayed in the **Responsiveness** column in the table. For example, 0 of 2 is responsive.

- **Only remote site initiates VPN** - Connections can only be initiated from the remote site to this appliance. For example, when the remote site is hidden behind a NAT device. In this scenario, this appliance only responds to the tunnel initiation requests. This requires a secure method of remote site authentication and identification.

4. Select an authentication method. This must match the authentication you used to configure this appliance as the other gateway's remote site.

   - **Preshared secret** - If you select this option, enter the same **password** as configured in the remote gateway and **confirm** it.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)

   - **Certificate** - The gateway uses its own certificate to authenticate itself. For more information, see **VPN** > **Internal Certificate**.

5. **Select the Remote Site Encryption Domain.**

   Configure the conditions to encrypt traffic and send to this remote site.

   - **Define remote network topology manually** - Traffic is encrypted when the destination is included in the list of network objects. Click **Select** to select the networks that represent the remote site's internal networks. Click **New** to create network objects.

- **Route all traffic through this site** - All traffic is encrypted and sent to this remote site. You cannot configure more than one remote site.

  When **Route all traffic** is configured, you can exclude a network object from the VPN traffic.

  **To exclude network objects or specific IP addresses:**

  a. Click **Exclude networks**.

  b. In the **Remote site route topology exclusions** table:

     - To add a new Network Object and IP address, click **New**.

     - To remove an object from the exclusions table, select the object name and click **Remove**.

  c. Click **Apply**

- **Encrypt according to routing table** - If you use dynamic routing, encrypt traffic based on source or service and destination. You must create a virtual tunnel interface (VTI) in the **Device** > **Local Network** page and associate it with this remote site. You can then use this VTI to create routing rules. Traffic that matches these routing rules is encrypted and routed to the remote site.

- **Hidden behind external IP of the remote gateway** - The remote site is behind NAT and traffic is initiated from behind the remote site to this gateway. When you select this option, it is not necessary to define an encryption domain.

6. **Exclude networks** - Select this option to exclude networks from the specified encryption domain. This may be useful if two gateways are in the same community and protect the same parts of the network.

7. Click **Apply**

On the **Encryption** tab you can change the default settings.

There are built in encryption settings' groups that only need to match in this configuration and in the remote site.

- **Default (most compatible)**
- **VPN A** - According to RFC 4308.
- **VPN B** - According to RFC 4308.
- **Suite-B GCM-128** or **Suite-B-GCM-256** - According to RFC 6379.
- **Custom** - Select this option to decide (manually) which encryption method is used (optional).

In the **Advanced** tab:

ⓘ **Note** - When you finish the new VPN site configuration, click **Save**.

- **Settings**
  - Select to configure if the remote site is a Check Point Security Gateway. To enable permanent VPN tunnels, Select the checkbox.
  - Select to disable NAT for this site. The original IP addresses are used even if hide NAT is defined.
- **Encryption method**

  Select the IKE version:

| IKE Version | Notes |
|---|---|
| **IKEv1** | • The modes for IKE negotiation are Main Mode and Aggressive Mode.<br>For IKE negotiation, the Main Mode uses six packets, and the Aggressive Mode uses three packets.<br>We recommend you use the Main Mode, which is more secure.<br>By default, **Enable aggressive mode** is *not* selected and the Main Mode is used.<br>Enable the Aggressive Mode only if necessary, and the other side of the VPN tunnel does not support the Main Mode. (Third party gateways primarily do not work in the Main Mode.)<br>The Aggressive Mode is used to create a tunnel and one of the gateways is behind NAT. In this case, a pre-shared secret does not provide enough data for authentication in the Main Mode. Authentication must be done using a certificate and a gateway (peer) ID, or a secondary identifier couple that is available in the Aggressive Mode. The secondary identifier method is also available in IKEv2.<br>• If you select **Enable aggressive mode for IKEv1**:<br>◦ **Use Diffie-Hellman group** - Determines the strength of the shared DH key used in IKE phase 1 to exchange keys for IKE phase 2. A group with more bits ensures a stronger key but lower performance.<br>◦ **Initiate VPN tunnel using this gateway's identifier** - When this gateway's IP address is dynamic and the authentication method is the certificate and the peer ID, you must enter the **Gateway ID**. For **Type**, select domain name or user name. |
| **IKEv2** | When you create a tunnel and one of the gateways is behind NAT without a certificate (uses a pre-shared secret), with IKEv2 protocol you can use a secondary identifier couple to allow authentication.<br>In this case, the pre-shared secret is not enough.<br>If you select **Create IKEv2 VPN tunnel using these identifiers**, configure these settings:<br>• **Peer ID** - Enter the identifier.<br>• **Gateway ID** - Select **Use global identifier** or **Override global identifier** (enter the new identifier). |

| IKE Version | Notes |
|---|---|
| **Prefer IKEv2, support IKEv1** | Configure the fields as explained for the first two options.<br>• **Additional Certificate Matching** (does not apply when you use a pre-shared secret):<br>When you select certificate matching in the **Remote Site** tab, you first need to add the CA that signed the remote site's certificate in the **VPN** > **Certificates Trusted CAs** page.<br>In the **Advanced** tab, you can select to match the certificate to **Any Trusted CA** or an **Internal CA**.<br>You can also configure more matching criteria on the certificate.<br>• **Probing Method**<br>This section is shown only when you select High Availability or Load Sharing for the connection type in the **Remote Site** tab.<br>When the remote site has multiple IP addresses for VPN traffic, the correct address for VPN is discovered through one of these probing methods:<br>◦ **Ongoing probing** - When a session is initiated, all possible destination IP addresses continuously receive RDP packets until one of them responds. Connections go through the first IP to respond (or to a primary IP if a primary IP is configured and active for High Availability), and stay with this IP until the IP stops responding. The RDP probing is activated when a connection is opened and continues a background process.<br>◦ **One time probing** - When a session is initiated, all possible destination IP addresses receive an RDP session to test the route. The first IP to respond is chosen, and stays chosen until the VPN configuration changes. |

**Notes:**

- For more information on installing the certificate, see *"Managing Installed Certificates" on page 215*.
- The initiator's gateway ID must be set in the responder gateway as the peer ID.
- The Remote Access blade must be enabled for peer ID to work.
- On the gateway that is not behind NAT, for **Connection type**, select **Only remote site initiates VPN**.
- When you configure the remote site, do not select behind static NAT.

An initial tunnel test begins with the remote site. If you have not yet configured it, click **Skip**. The VPN site is added to the table.

Locally managed gateways can be part of these site to site communities:

- **VPN mesh community** - All gateways are connected to each other, and each gateway handles its own internet traffic. Encrypted traffic is passed from networks in the encryption domain of one gateway to the networks in the encryption domain of the second gateway.
- **VPN star community** - One gateway is the center and routes all traffic (encrypted and internet traffic of the remote peer) to the internet and back to the remote peer. The peer gateway is a satellite and is configured to route all its traffic through the center.

**To configure a gateway as the center:**

1. Select the VPN site from the list.
2. Click **Edit**.

   The **Edit VPN Site** window opens.
3. In the **Remote Site** tab:
   - For **Connection type**, enter the IP address which is the public IP of the remote peer (satellite gateway).
   - In the **Encryption domain**, select the networks of the satellite gateway that will participate in the VPN.
4. In the **Advanced** tab, select **Allow traffic to the internet from remote site through this gateway**.
5. Click **Apply**

   This gateway is now designated as the center. Hide NAT is done automatically in the center gateway.

**To configure a gateway as a satellite:**

1. Select the VPN site from the list.
2. Click **Edit**.

   The **Edit VPN Site** window opens.
3. In the **Remote Site** tab:
   - For **Connection type**, enter the IP address which is the public IP of the remote peer (center gateway).
   - In the **Encryption domain**, select **Route all traffic through this site**.
4. Click **Apply**

   This gateway is now designated as a satellite.

You can configure more than one satellite gateway to route all traffic through the center gateway.

If you try to configure two gateways to be the center, an error message shows.

If you do not configure one gateway as a center, the site to site VPN acts like a mesh community and each gateway continues to handle its own traffic.

**To run a tunnel test with a remote site:**

Check Point uses a proprietary protocol to test if VPN tunnels are active. It supports any site-to-site VPN configuration.

Tunnel testing requires two Security Gateways and uses UDP port 18234. Check Point tunnel testing protocol does not support 3rd party Security Gateways.

1. Select an existing site from the list.
2. Click **Test**.

**To edit a VPN site:**

1. Select the VPN site from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

**To delete a VPN site:**

1. Select the VPN site from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

**To disable or enable the VPN site:**

1. Select the VPN site from the list.
2. Click **Disable** or **Enable**.

### VPN Community Use Cases

**Q1:** A system administrator is responsible for 6 gateways and wants to share network resources between the satellite branches. Which type of VPN community is preferable?

**A1:** A star VPN community is preferable as every gateway does not have to create a VPN tunnel with all of the others. Instead, the 5 satellite peer gateways will each create one site to site star VPN community to the center gateway. Only the star gateway (center) must create a site to site from itself to each of the remote peers.

**Q2:** A center gateway handles all the traffic in the VPN community. When the gateway reboots, all the other gateways' internet traffic is affected, and they lose access to the remote peer encryption domain until the center gateway comes back up. How can the administrator avoid this downtime?

**A2:** In this case, a mesh community is better as each gateway can handle its own internet traffic and is not affected by any other gateway.

# Configuring Advanced Site to Site Community Settings

**Note** - This page is relevant only if Cloud Services is turned on.

In the **VPN** > **Site to Site Community** page you can see details of the community members configured for this appliance by Cloud Services. The information here is read-only and you cannot update details. The settings configured by Cloud Services for the **VPN** > **Site to Site** software blade are used by the community members.

The Community page shows:

- The name of the community configured by the Cloud Services Provider.
- A table with the sites that are part of the community.

**To test the VPN connection for a site:**

1. Select the site.
2. Click **Test**.

   If the test succeeds, a success message is shown. Click **OK** to close it.

   If the test does not succeed, click **Details** for more information. If applicable, click **Retry**.

**To see the details of a site configured by Cloud Services:**

Select a site and click **View Details**.

The View Site Details window opens and shows:

- Remote site details - Name, host or IP address, authentication method (preshared secret or certificate), and the Remote Site Encryption Domain
- Encryption settings - IKE (Phase 1) and IPsec (Phase 2) settings
- Advanced settings - Encryption method and certificate matching

For descriptions of the fields in the site details tabs, see *"Configuring VPN Sites" on page 407*.

# Viewing VPN Tunnels

In the **VPN Tunnels** page, you can see current VPN tunnels opened between this gateway and remote sites. Some sites are configured so tunnels are established only when necessary and some are configured with permanent tunnels. When the appliance is managed by Cloud Services, this table also shows the tunnels for the gateways in the community.

The table below shows the details of each tunnel configured:

| Field | Description |
|---|---|
| **Status** | Indicates if a tunnel is up or is pending traffic to become active. |
| **Site Name** | The VPN site name. |
| **From** | The external interface the tunnel uses. |
| **Peer Address** | Host name or IP address of the tunnel's destination gateway. |
| **Tunnel Creation Time** | Date the tunnel was created. |
| **Tunnel Expiration Time** | Date the tunnel expires. |
| **Community Name** | If the gateways are part of a community configured by Cloud Services, the community name with which the tunnel is associated.<br>Visible when the Quantum Spark gateway is configured in the Quantum Spark Management service in Infinity Portal. |
| **My Encryption Domain** | Indicates the tunnel's selectors (subnets/hosts) allowed from the source gateway. |
| **Peer's Encryption Domain** | Indicates the tunnel's selectors (subnets/hosts) allowed from the destination gateway. |
| **Phase 2 Methods** | Encryption and authentication methods used for the tunnel. |
| **Connections Per Instance** | The number of connections associated with the tunnel per instance. This lets you know if a tunnel is over-utilized. |

**To filter the list:**

In the **Type to filter** box, enter the filter criteria.

### To refresh the list:

Click **Refresh** to refresh manually this page with updated tunnel information.

### To delete all Security associations for a selected peer:

Click **Delete all SAs for the selected peer**.

**Note** - This page is available from the **VPN** and **Logs & Monitoring** tabs.

# Configuring Advanced Site to Site Settings

In the **VPN** > **Site to Site Advanced** page you can configure global advanced options that define how the appliance connects to remote sites.

The configuration options on this page answer these configuration questions:

- When to open a connection with a remote site - See "Configuring a Local Encryption Domain" below. In addition, the remote site's encryption domain is configured per site. See the **VPN** > **Site to Site VPN Sites** page.
- How the appliance connects to remote sites - See "Configuring the Appliance's Outgoing Interfaces for VPN usage below.

## Configuring a Local Encryption Domain

In domain-based VPN, traffic is encrypted when it originates in one Encryption Domain and is transmitted to a different domain.

The local Encryption Domain defines:

- The internal networks that encrypted traffic from remote sites and networks can get access.
- That traffic from the Encryption Domain to remote sites is encrypted.

By default, the local encryption domain is determined automatically be the appliance. Networks behind LAN interfaces and trusted wireless networks are part of the local Encryption Domain. Optionally, you can manually create a local Encryption Domain if necessary.

**To configure a local Encryption Domain manually:**

1. Click the link **defined automatically according to topology**.
2. Select **Define local network topology manually**.
3. Click **Select** to show the full list of available networks and select the applicable checkboxes.
4. Click **New** if the existing list does not contain the necessary networks required.

   For information on how to create a new network object, see the **Users & Objects** > **Network Objects** page.
5. Click **Apply**.

The Site to Site Local Encryption Domain window opens and shows the services you selected.

## Configuring the Appliance Interfaces

Link Selection is used to:

- Specify which interface is used for incoming and outgoing VPN traffic.
- Determine the best possible path for the traffic.

In addition, with the Link Selection mechanisms, the administrator can select which source IP addresses are used for VPN traffic.

The default configuration to select an outgoing interface and source IP address is for the device to determine them automatically. Alternatively, you can change the default settings and select other means to determine:

- The appliance's outgoing interface
- The appliance's source IP address

**To configure the appliance's outgoing interfaces and source IP address for VPN:**

1. In the **Link Selection** > **Outgoing interface selection** section, select a method to specify the outgoing interface:
   - **According to the routing table** - The OS's routing table finds the interface link with the lowest metric (highest priority) through which to send traffic based on the remote site's IP addresses.
   - **Route based probing** - This method also consults the routing table for the link with the lowest metric. But, before choosing an interface link to send traffic, all routing possibilities are examined. This is to make sure that the link is active. The gateway selects the best match (highest prefix length) active route with the lowest metric (highest priority). This method is recommended when there is more than one external interface.
2. In the **Source IP address selection** section, select an option to configure the source IP address used by the Security Gateway, when it initiates or responds to VPN traffic. This IP address is normally used by the remote sites to connect to this Security Gateway:
   - **Automatically chosen according to outgoing interface**.
   - **Manually configured** - Enter an IP address that is always used as the source IP address of a VPN tunnel.

## Configuring the IKE ID Type for the IKEv2 Main Mode (MM) Negotiation with 3rd-party VPN Peers

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.10 version.

The purpose of the IKEv2 ID Type exchanged during the IKEv2 Main Mode (MM) negotiation (Packet 5 and Packet 6) is to provide an ID, based on which the remote peer searches for the local peer in its database.

The ID Type is not necessary for IKEv2 Main Mode (MM) negotiation between Check Point Security Gateways. However, it is necessary for most 3rd-party VPN gateways. It is important to make sure both sides authenticate using the same ID Type and ID values.

Quantum Spark Spark gateways can configure IKEv2 ID Type to one of these:

- An FQDN (this is the default).
- An IP address (determined dynamically, based on the OS routing) - in R81.10.10 and higher.

**To see the current configuration:**

1. Connect to the command line on the Quantum Spark appliance.
2. Log in.
3. If your default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```

4. Examine the value of the Registry parameter:

   ```
   ckp_regedit -p SOFTWARE\\CheckPoint\\VPN1 | grep
   BestRoutingSenderIP
   ```

   Explanation:

   - If the output shows the value "False", then the Quantum Spark gateway configures IKEv2 ID Type to an FQDN
   - If the output shows the value "True", then the Quantum Spark gateway configures IKEv2 ID Type to its IP address

**To configure IKEv2 ID Type to an FQDN:**

**Important** - Schedule a maintenance window.

1. Connect to the command line on the Quantum Spark appliance.
2. Log in.

3. If your default shell is Gaia Clish, then go to the Expert mode:

```
expert
```

4. Configure the required value for the Registry parameter:

```
ckp_regedit -a SOFTWARE/CheckPoint/VPN1 BestRoutingSenderIP
False
```

5. Examine the value of the Registry parameter:

```
ckp_regedit -p
SOFTWARE\\CheckPoint\\VPN1 |
grep BestRoutingSenderIP
```

6. Restart all Check Point services (this interrupts all traffic):

```
cpstop ; cpstart
```

**To configure IKEv2 ID Type to an IP address based on the OS routing:**

**Important** - Schedule a maintenance window.

1. Connect to the command line on the Quantum Spark appliance.
2. Log in.
3. If your default shell is Gaia Clish, then go to the Expert mode:

```
expert
```

4. Configure the required value for the Registry parameter:

```
ckp_regedit -a SOFTWARE/CheckPoint/VPN1 BestRoutingSenderIP
True
```

5. Examine the value of the Registry parameter:

```
ckp_regedit -p
SOFTWARE\\CheckPoint\\VPN1 |
grep BestRoutingSenderIP
```

6. Restart all Check Point services (this interrupts all traffic):

```
cpstop ; cpstart
```

# Tunnel Health Monitoring

To test if a VPN tunnel is active, click the down arrow next to the Tunnel Health monitoring method and select one of these:

- **Tunnel test (Check Point Proprietary)** - The VPN tunnel is constantly monitored by periodically sending tunnel test packets, which act as a keepalive mechanism. When responses to the packets are received, the VPN tunnel is considered “up.” If no response is received within a specified time period, the VPN tunnel is considered “down.”

  **Notes**:
  - For testing to occur, you must:
    1. Select the **Tunnel test** option in the **Tunnel health monitoring method** in the **Site to Site Advanced Settings** page.
    2. Select the **Enable permanent tunnels** checkbox in the **Advanced** tab of the **Edit VPN Site** window for this site.
  - Tunnel testing only occurs between Check Point Security Gateways.

- **DPD (Dead Peer Detection)** allows you to monitor permanent tunnels over IKE traffic (IKEv1) and over IPsec traffic (IKEv2)/ DPD minimizes the number of messages required to confirm the availability of a peer.

  When set, a peer that is configued as DPD receives DPD Hello requests at regular intervals if there is no incoming IPsec traffic for 10 seconds.

# Managing Trusted CAs

In the **VPN** > **Certificates Trusted CAs** page you can add CAs used by remote sites' certificates to enable a VPN or WebUI certificate. A certificate shown by the remote site must be signed by a CA that is trusted by the appliance. Trusted CAs include both intermediate and root CAs.

This page also shows the built in Internal CA that by default creates the certificates for this appliance. It can also be used to sign remote sites' certificates. You can also export the internal CA to add it to a remote site's trusted CA list.

When Cloud Services is turned on and the appliance is configured by a Cloud Services Provider, the CA of the Cloud Services Provider is downloaded automatically to the appliance. The Cloud Services Provider CA is used by community members configured by Cloud Services.

**Note** - If you turn Cloud Services off, the Cloud Services Provider CA is removed.

### Recommended configurations

When you use certificate based site to site VPN with only one remote site, we recommend you export each site's Internal CA and add it to the other site's Trusted CA list.

When you use certificate based site to site VPN with multiple remote sites, in a mesh configuration, we recommend for all sites to use one CA to sign their internally used certificates on appliances that support creating signing requests. You must also add the same CA to all sites' Trusted CAs list. That CA can be an external CA service like Verisign (for a fee) or simply use this appliance's Internal CA. See below how to use it to sign external requests.

### To add a trusted CA:

1. Click **Add**.
2. Click **Browse** to upload a CA's identifier file (a .CRT file).
3. A **CA name** is suggested, but you can enter another name if preferred.

   Click **Preview CA details** to see further information from the .CRT file.
4. Click **Apply** The CA is added to the Trusted CA list.

### To edit a trusted CA's configuration:

1. Select the CA from the list.
2. Click **Edit**.
3. Select the necessary options regarding CRL (Certificate Revocation List):
   - **Retrieve CRL from HTTP Server(s)** - HTTP can be used to access the CA for CRL retrieval. When cleared, this appliance does not attempt to validate the remote site's certificate's CRL.
   - **Cache CRL on the Security Gateway** - Select how often is a new updated CRL is retrieved.
     - **Fetch new CRL when expires** - Upon expiration of the CRL.
     - **Fetch new CRL every X hours** - Regardless of CRL expiration.
4. Click **Details** to see full CA details.
5. Click **Apply**

### To delete a trusted CA:

1. Select the trusted CA from the list and click **Delete**.
2. Click **OK** in the confirmation message.

### To export the Internal CA (or other previously imported CAs):

1. Select the Internal CA in the table.
2. Click **Export**.

   The Internal CA's identifier file is downloaded through your browser and is available to be imported to the remote site's trusted CA list.
3. You can also export other trusted CAs you've added to the list if necessary by selecting them and clicking Export.

**To sign a remote site's certificate request by the Internal CA:**

1. Click **Sign a Request**.
2. Click **Browse** to upload the signing request file as created in the remote site.

   In third party appliances, make sure to look in its Administration Guide to see where signing requests are created.

   **Note** - The file must be in a path accessible to the appliance. After you click **OK** in the file browsing window, the file is uploaded. If it is correctly formatted, it is signed by the Internal CA and the **Download** button is available.

3. Click **Download**.

   The signed certificate is downloaded through your browser and is available to be imported to the remote site's certificates list.

# Managing Installed Certificates

On the **Installed Certificates** page, you can create and manage appliance certificates or upload a P12 certificate. Uploaded certificates and the default certificates are displayed in a table. To see certificate details, click the certificate name.

You can upload a certificate signed by an intermediate CA or root CA. All intermediate and root CAs found in the P12 file are automatically uploaded to the trusted CAs list.

**Note** - This page is available from the **Device** and **VPN** tabs.

On the **VPN Remote Access Blade Control** page, after you enable the SSL VPN feature, you can select and assign a certificate from the list of the installed certificates (with the exception of the Default Web Portal certificate). You can also do this on the **Remote Access Advanced** tab.

On the **Device** > **Device Details** page, you can select and assign a Web portal certificate from the list of installed certificates (with the exception of the Default certificate).

Installed certificates are used in site-to-site VPN, SSL VPN, and the Web portal.

When Cloud Services is turned on and the appliance is configured by Cloud Services, the Cloud Services Provider certificate is downloaded automatically to the appliance. The Cloud Services Provider certificate is used by community members configured by Cloud Services.

**Note** - If you turn Cloud Services off, the Cloud Services Provider certificate is removed.

**These are the steps to create a signed certificate:**

1. Create a signing request.
2. Export the signed request (download the signing request from the appliance).
3. Send the signing request to the CA.
4. When you receive the signed certificate from the CA, upload it to the appliance.

**To create a new certificate to be signed by a CA:**

1. Click **New Signing Request**.
2. Enter a **Certificate** name.
3. In the **Subject DN** enter a distinguished name (e.g. `CN=myGateway`).
4. **Optional:** - Click **New** to add alternate names for the certificate.

   Select the **Type**, enter the **Alternate name** and click **Apply**.
5. Click **Generate**.

The new signing request is added to the table and the status shows "Waiting for signed certificate".

**Note** - You cannot edit the request after it is created.

If the new signing request is signed by the Internal CA and the Organization Name is not defined in the DN, the Internal CA automatically generates the Organization Name.

**To export the signing request:**

Click **Export**.

**To upload the signed certificate when you receive the signed certificate from the CA:**

1. Select the signing request entry from the table.
2. Click **Upload Signed Certificate**.
3. Browse to the signed certificate file (*.crt).
4. Click **Complete**.

The status of the installed certificate record changes from "Waiting for signed certificate" to "Verified".

**To upload a P12 file:**

1. Click **Upload P12 Certificate**.
2. Browse to the file.
3. Edit the **Certificate name** if necessary.
4. Enter the certificate **password**.
5. Click **Apply**

# Managing Internal Certificates

In the **Certificates Internal Certificate** page you can view details of an internal VPN certificate. You can also view and reinitialize the certificate used by the internal CA that signed the certificate and can be used to sign external certificates.

**Note** - This page is available from the **Device** and **VPN** tabs.

When you create an internal VPN certificate, when a certificate that is signed by the internal CA is used, the CA's certificate must be reinitialized when the Internet connection's IP addresses change.

To avoid constant reinitialization, we recommend you use the DDNS feature. See **Device** > **DDNS**. When DDNS is configured, you only need to reinitialize the certificate once. Changes in the DDNS feature configuration by default automatically reinitialize certificates.

**To reinitialize certificates:**

1. Click **Reinitialize Certificates**.

   The Reinitialize Certificates window opens.

2. Enter the **Host/IP address**.

   Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.

3. Select the number of years for which the Internal VPN Certificate is valid. The default is 3. The maximum value allowed is 20.

4. Click **Apply**

**Note** - The internal VPN certificate expiration date cannot be later than the CA expiration date.

### To replace an internal CA certificate:

1. Click **Replace Internal CA Certificate**.
2. Click **Browse** to select the CA certificate file that includes the private key.
3. Enter the **Certificate name** and private key's password to allow the device to sign certificates with the uploaded CA.
4. Enter the **Host/IP address**.

   Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.
5. Click **Apply**

### To export an internal CA certificate:

Click **Export Internal CA Certificate** to download the internal CA certificate.

### To sign a remote site's certificate request by the internal CA:

1. Click **Sign a Request**.
2. Click **Browse** to upload the signing request file as created in the remote site.

   In third party appliances, make sure to look in its Administration Guide to see where signing requests are created.

   The file must be in a path accessible to the appliance. After you click **OK** in the file browsing window, the file is uploaded. If it is correctly formatted, it is signed by the Internal CA and the **Download** button is available.
3. Click **Download**.

   The signed certificate is downloaded through your browser and is available to be imported to the remote site's certificates list.

# Managing Users and Objects

This section describes how to set up and manage users (User Awareness, users, administrators, and authentication servers) and network resources.

## Working with User Awareness

In the **User Awareness** page you can turn the blade on or off and use the configuration wizard to configure sources to get user identities for logging and configuration purposes.

User Awareness lets you configure the Quantum Spark Appliance to show user based logs instead of IP address based logs and enforce access control for individual users and user groups.

### Workflow

1. Turn on the User Awareness Software Blade.
2. Click the **Configuration wizard** to enable and configure the blade.
3. Select the identification methods to get information about users and user groups and configure the identity sources.
4. After initial configuration, you can select the **Active Directory Queries**, **Browser-Based Authentication**, or **Identity Collector** checkboxes in the **Policy Configuration** section and click **Configure** for more advanced settings.
5. After the gateway acquires the identity of a user, you can enforce user-based rules on the network traffic in the Access Policy.

### Identity Sources

User Awareness can use these sources to identify users:

- **AD Query** (Active Directory Queries) - Seamlessly queries the Active Directory servers to get user information.

  The Quantum Spark Appliance registers to receive security event logs from the AD domain controllers when the security policy is installed. This requires administrator privileges for the AD server. When a user authenticates with AD credentials, these event logs are generated and are sent to the Security Gateway. The Quantum Spark Appliance can then identify the user based on the AD security event log.

- **Browser-Based Authentication** - Uses a portal to authenticate either locally defined users or as a backup to other identification methods.

- Browser-Based Authentication uses a web interface to authenticate users before they can access network resources or the Internet. When users try to access a protected resource, they must log in to a web page to continue. This identifies locally defined users or users that were not successfully identified by other methods.
- You can configure the Browser-Based Authentication to appear for all traffic. This identification method is commonly configured to appear when you access only specific network resources or the Internet to avoid the overhead required from end users when they identify themselves.
- For traffic that is not HTTP based, you can also configure that all unidentified users are blocked from accessing the configured resources or Internet until they identify themselves first through the Browser-Based Authentication.

- **Identity Collector** - Collects information about identities and their associated IP addresses and sends it to the Security Gateway for identity enforcement.

  ℹ **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

## Enabling User Awareness

1. Select the **On** or **Off** option.

   ℹ **Note** - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

2. Click the **Configuration wizard** link.

   The **User Awareness Wizard** opens.

3. Select one or more user identification methods and click **Next**.
4. Follow the rest of the steps and click **Finish**.
5. After initial configuration, you can select the **Active Directory Queries** or **Browser-Based Authentication** checkboxes under Policy Configuration and click **Configure** to configure more advanced settings.

## Active Directory Queries:

If you have an existing Active Directory server, click **Use existing Active Directory servers**.

**To add a new Active DirectoryDomain:**

1. Select **Active Directory Queries** and click **Configure**.

   The **Active Directory Queries** window opens.

2. Select **Define a new Active Directory** server.
3. Enter:
   - **Domain**
   - **IPv4 address**
   - **IPv6 address**
   - **User name**
   - **Password**
   - **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually.
4. To select user groups from specific branches, select the checkbox **Use user groups from specific branch only**.

   Click **Add** and enter a branch path in the **AD Branch** field.
5. Click **Apply**

You can also add a new AD Domain in the **Users & Objects** > **Authentication Servers** page.

### Configuring User Awareness to use NTLMv2 protocol for Active Directory Queries

**Follow one of these procedures:**

**In WebUI:**

1. Connect to the WebUI on the Quantum Spark Gateway / each Cluster Member.
2. Click the **Device** view > **Advanced section** > **Advanced Settings** page.
3. In the top search field, enter: `ntlm`
4. Double-click the parameter **User Awareness - Use NTLMv2 protocol for Active Directory Queries**.
5. Select **Use NTLMv2 protocol for Active Directory Queries**.
6. Click **Save**.

**In Gaia Clish**:

1. Connect to the command line on the Quantum Spark Gateway / each Cluster Member.
2. If the default shell is the Expert mode, go to Gaia Clish:

   ```
   clish
   ```

3. Run:

```
set user-awareness advanced-settings use-ntlmv2 true
```

## Browser-Based Authentication

### Blocking unauthenticated users

1. To block access for unauthenticated users when the portal is not available, select **Block unauthenticated users when the captive portal is not applicable**.

   This configuration option forces users using non-HTTP traffic to log in first through Browser-Based Authentication.

2. Select if unidentified users are redirected to Captive Portal for **All traffic** or **Specific destinations**.

   In most cases, all traffic is not used because it is not a seamless identification method.

3. Under Specific destinations, select **Internet** or **Selected network objects**.

   If you select **Selected network objects**, select the objects from the list or create new objects.

4. Click **Finish**.

### To edit settings and configure portal customization for Browser-Based Authentication

1. Under **Policy Configuration**, select **Browser-Based Authentication** and click **Configure**.
2. In the **Identification** tab, you can edit settings configured in the wizard if necessary.
3. In the **Customization** tab, select the relevant options:
   - **Users must agree to the following conditions** - You can require that users agree to legal conditions. In the text box, enter the conditions that are shown to the user.
   - **Upload** - Lets you upload a company logo. **Browse** to the logo file and click **Apply**. The logo is shown in the **Displayed Logo** section.
   - **Use Default** - Uses the default logo.
4. In the **Advanced** tab:
   - **Portal Address** - Keep the default setting which is the address the Captive Portal runs on the Quantum Spark Appliance or enter a different portal address.

- **Session timeout** - Sets for how long an authenticated user can access the network or Internet before they have to authenticate again.
- **Enable Unregistered guests login** - Allow an unregistered, guest user to be identified in the logs by name and not only by IP address.

  An unregistered user is an unmanaged non-AD user, typically a partner or a contractor. To gain access, guests enter their company name, email address, phone number (optional), and name.

  Configure the **Guest Session timeout**. This is the number of minutes for which a guest user can access network resources. The default timeout is 180 minutes.

  Guest access is logged. The name of the guest shows in the **User** column of the **Logs and Monitoring** tab. The other details show in the full log entry.

  Guest access is logged. The name of the guest shows in the **User** column of the **Logs and Monitoring** tab. The other details show in the full log entry.
- **Force quick cache timeout if user closes portal window** - When the portal is closed, the user is logged out within 5 - 10 minutes.

5. Click **Apply**

# Identity Collector

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

Quantum Spark Locally Managed appliances support Identity Collector as an Identity Source in versions R81.10.05 and higher.

**To configure the Identity Collector**

1. In the **Policy Configuration** section, select **Identity Collector** and click **Configure**.

   The **Authorized Clients** window opens.
2. For each client, enter this information:
   - **IPv4 address** - The IP address of the client.
   - **Secret** - Password
     - **Optional** - Click **Show** to display the secret.
3. Click **Apply**

For more information about **Identity Collector** configuration, see *Identity Awareness Clients Administration Guide*.

**Note** - This page is available from **Access Policy** > **User Awareness Blade Control** and **Users & Objects** > **User Awareness**.

# Configuring Local Users and User Groups

In the **Users & Objects** > **Users** page you can create local users and user groups. To use these objects in the Access Policy, make sure to activate User Awareness.

User objects are used to define the different terms under which users can operate. These include:

- The time frame during which users are allowed to access the network.
- If users can work remotely.

**To add a new local user:**

1. Click **New** > **Local User**.
2. Enter a **User name**, **Password**, and **Comments** (optional).

   The password can be up to 100 characters.

   **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)
3. For temporary or guest users, click **Temporary user**.

   Enter the expiration date and time.
4. To give the user remote access permissions, select **Remote Access permissions**.
5. Click **Apply**

   The user is added to the table on the page.

**To add a new local users group with remote access permissions:**

1. Click **New** > **Users Group**.
2. Enter a **Group name**.
3. To give the group remote access permissions, select **Remote Access permissions**.
4. To select initial users to add to the group, click the relevant checkboxes from the user list or click **New** to create new users.

   You can see a summary of the group members above the user list.
5. To remove a user, click the X next to the user name.
6. Click **Apply**

   The group is added to the table on the page.

**To automatically delete expired local users:**

1. Go to **Device** > **Advanced Settings**.
2. Select **User Management**.
3. Click **Edit**.

   The **User Management** window opens.
4. Click the checkbox for **Automatically delete expired local users**.
5. Click **Apply**

   Expired local users are automatically deleted every 24 hours (after midnight).

**To edit a user or group:**

1. Select the user or group from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

**To delete a user or group:**

1. Select the user or group from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

   The user or group is deleted.

# Configuring Local and Remote System Administrators

The **Device** > **Administrators** page lists the appliance administrators. Here you can:

- Create new local administrators.
- Configure the session timeout.
- Limit login failure attempts.
- Generate a QR code to connect the mobile application with the appliance for the first time.
- Regenerate keys.

Administrators can also be defined in a remote RADIUS server and you can configure the appliance to allow them access. Authentication of those remotely defined administrators is done by the same RADIUS server.

**Note** - This page is available from the **Device** and **Users & Objects** tabs.

## Administrator Roles:

- **Super Administrator** - All permissions. Super Administrators can create new locally defined administrators and change permissions for others.
- **Read Only Administrator** - Limited permissions. Read Only Administrators cannot update appliance configuration but can change their own passwords or run a traffic monitoring report from the **Tools** page.
- **Networking Administrator** - Limited permissions. Networking Administrators can update or modify operating system settings. They can select a service or network object but cannot create or modify it.
- **Mobile Administrator** - Mobile administrators are allowed all networking operations on all interfaces. They can change their own passwords, generate reports, reboot, change events and mobile policy, active hosts operations and pairing. They cannot login from or access the WebUI.
- **Remote Access Administrator** - Limited permissions. Remote access administrators can manage the VPN remote access configuration. They can add, edit and delete VPN remote access users and servers.
- **Access Policy Administrator** - Limited permissions. Access policy administrators can manage the Firewall settings; Applications and URL filtering settings; and the Firewall access policy. They can also create, edit, and delete network objects, services and custom applications.
- **Self-serve Administer** - Create this role in the Spark Management application in the Infinity Portal. Log in to your local gateway as a Self-serve Administrator to access the Self-serve portal.

Two administrators with write permissions cannot log in at the same time. If an administrator is already logged in, a message shows. You can choose to log in with Read-Only permission or to continue. If you continue the login process, the first administrator session ends automatically.

The correct Administrator Role must be configured to perform the operations listed below. If not, a **Permission Error** message shows.

## Local Administrators

**To create a local administrator:**

1. Click **New**.

   The **Add Administrator** page opens.

2. Enter the administrator details:

   **Note** - To enable Two-Factor Authentication (available starting from the R81.10.10 release), all administrators must have both an email address and a phone number configured. Click **Test** to verify that you can receive messages at both the email address and phone number.

   - **Name**. The hyphen (-) character is allowed in the administrator name.
   - **Password** and then **Confirm password**.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)

   - **Email address**.

     **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

   - **Phone number**. - Include the country code and do not include “+” at the beginning of the phone number. For example, "44123456789" where "44" is the country code.

     **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.

   - **Administrator role** Select from the pull-down menu.
   - **Enforce password change upon the next login**. . The next time the administrator logs in, this message appears: "Your password has expired and must be changed."

     After the password is changed, the checkbox is clear. You can reselect to enforce password change at any time.

3. Click **Save**.

   The name and Administrator Role is added to the table. When logged in to the WebUI, the administrator name and role is shown at the top of the page.

**Note** - If Two-Factor Authentication is not enabled, defining an email address and phone number is **optional**. However, you must have either an email address **or** a phone number defined to:

- Receive Security alert notifications by email or SMS. See *"Notifications" on page 60*
- To reset your password on the Login page of the WebUI (see below).

**To edit the details of locally defined administrators:**

1. Select the administrator from the table and click **Edit**.
2. Make the relevant changes.
3. Click **Apply**

**To delete a locally defined administrator:**

1. Select an administrator from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

**Note** - You cannot delete an administrator who is currently logged in.

**To reset password:**

**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.08 version.

You can securely reset your password when you log in to your Security Gateway.

**Note** - You must have an email address or phone number configured as part of the administrator details.

1. In the **Login** page, enter the **User Name** and click **Forgot my password.**
2. The **Find Your Account** screen appears. Enter your **Username** and your **Email** or **Phone numbe**r, and click **Next**.

   You receive a message with a security code (One Time Password).
3. Enter the security code and click **Next**.
4. Create and enter your new password in the applicable field.

   **Note** - The password must contain a minimum of 6 characters.
5. In the **Confirm password** field, Enter the password again.

6. Click **Next**
7. A message on the screen confirms your password was successfully changed.
8. Click **Next** to proceed to the **Login** page.

# Remote Administrators

**Note** - In R81.10.10, Two-Factor Authentication is not supported when RADIUS or TACACS is configured for administrator access.

**To allow access for administrators defined in a remote RADIUS server:**

1. Make sure administrators are defined in the remote RADIUS server.
2. Make sure a RADIUS server is defined on the appliance. If there is no server, click the **RADIUS configuration** link at the top of this page. You must configure the IP address and shared secret used by the RADIUS server.
3. When you have a configured RADIUS server, click **Edit permissions**.

   The **RADIUS Authentication** window opens.
4. Select **Enable RADIUS authentication for administrators**.

   **Use roles defined on RADIUS server** is selected by default.
5. Configure the role for each user on the RADIUS server. See additional details below.

   **Note** - A user without role definition will get a login error.
6. If you select **Use default role for RADIUS users**, select the **Administrators Role**:
   - Super Admin
   - Read only
   - Networking Admin
   - Mobile Admin
7. To define groups, click **Use specific RADIUS groups only** and enter the RADIUS groups separated by a comma.
8. Click **Apply**

**To set the Session Timeout value for both local and remotely defined administrators:**

1. Click **Security Settings**.

   The **Administrators Security Settings** window opens.

2. Configure the session timeout (maximum time period of inactivity in minutes). The maximum value is 999 minutes.

3. To limit login failure attempts, click the **Limit administrators login failure attempts** checkbox.

4. Enter the number of **Maximum consecutive login attempts** allowed before an administrator is locked out.

5. In **Lock period**, enter the time (in seconds) that must pass before a locked out administrator can attempt to log in again.

6. To enforce password complexity on administrators, click the checkbox and enter the number of days for the password to expire.

   **Note** - We strongly recommend the use of complex passwords. Password must contain at least 12 characters - uppercase, lowercase, numeric, and non-alphanumeric characters. Allowed alphanumeric characters: `! @ # % ^ & * ( ) - _ + : ;`

7. Click **Apply**

# Pairing a Mobile Device

To connect the mobile application with the appliance for the first time:

1. Click **Mobile Pairing Code**.

   The **Connect Mobile Device** window opens.

2. Select an administrator from the pull down menu.

3. Click **Generate**.

   This generates a QR code to connect the Check Point WatchTower mobile application with the appliance for the first time.

For more information about the mobile application, see the *WatchTower App User Guide*.

# Configuring a RADIUS Server for non-local Quantum Spark Appliance users

Non-local users can be defined on a RADIUS server and not in the Quantum Spark Appliance. When a non-local user logs in to the appliance, the RADIUS server authenticates the user and assigns the applicable permissions. You must configure the RADIUS server to correctly authenticate and authorize non-local users.

**Notes:**

- The configuration of the RADIUS Servers may change according to the type of operating system on which the RADIUS Server is installed.
- If you define a RADIUS user with a null password (on the RADIUS server), the appliance cannot authenticate that user.

**Configuring a Steel-Belted RADIUS server for non-local appliance users**

1. Create the dictionary file `checkpoint.dct` on the RADIUS server, in the default dictionary directory (that contains `radius.dct`). Add these lines in the `checkpoint.dct` file:

```
@radius.dct
MACRO CheckPoint-VSA(t,s) 26 [vid=2620 type1=%t% len1=+2
data=%s%]
ATTRIBUTE CP-Gaia-User-Role CheckPoint-VSA(229, string)  r
ATTRIBUTE CP-Gaia-SuperUser-Access CheckPoint-VSA(230,
integer)  r
```

2. Add these lines in the `vendor.ini` file on the RADIUS server (keep in alphabetical order with the other vendor products in this file):

```
vendor-product = Quantum Spark Appliance
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```

3. Add this line in the `dictiona.dcm` file:

`"@checkpoint.dct"`

4. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

`CP-Gaia-User-Role = <role>`

Where *<role>* allowed values are:

| Administrator Role | Value |
|---|---|
| Super Admin | `adminRole` |
| Read only | `monitorrole` |
| Networking Admin | `networkingrole` |
| Mobile Admin | `mobilerole` |

#### Configuring a FreeRADIUS server for non-local appliance users

1. Create the dictionary file `dictionary.checkpoint` in the `/etc/freeradius/` on the RADIUS server.

   Add these lines in the `dictionary.checkpoint` file:

   ```
   # Check Point dictionary file for FreeRADIUS AAA server
   VENDOR CheckPoint 2620
   ATTRIBUTE   CP-Gaia-User-Role          229   string
   CheckPoint
   ATTRIBUTE   CP-Gaia-SuperUser-Access   230   integer
   CheckPoint
   ```

2. Add this line in the `/etc/freeradius/dictionary` file

   ```
   "$INCLUDE dictionary.checkpoint"
   ```

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   ```
   CP-Gaia-User-Role = <role>
   ```

   Where *<role>* is the name of the administrator role that is defined in the WebUI.

| Administrator Role | Value |
|---|---|
| Super Admin | `adminRole` |
| Read only | `monitorrole` |
| Networking Admin | `networkingrole` |
| Mobile Admin | `mobilerole` |

### Configuring an OpenRADIUS server for non-local appliance users

1. Create the dictionary file `dict.checkpoint` in the `/etc/openradius/subdicts/` directory on the RADIUS server:

   ```
   # Check Point Gaia vendor specific attributes
   # (Formatted for the OpenRADIUS RADIUS server.)
   # Add this file to etc/openradius/subdicts/ and add the line
   # "$include subdicts/dict.checkpoint" to
   /etc/openradius/dictionaries
   # right after dict.ascend.
   $add vendor 2620 CheckPoint
   $set default vendor=CheckPoint
        space=RAD-VSA-STD
        len_ofs=1 len_size=1 len_adj=0
        val_ofs=2 val_size=-2 val_type=String
        nodec=0 noenc=0
   $add attribute 229 CP-Gaia-User-Role
   $add attribute 230 CP-Gaia-SuperUser-Access val_type=Integer
   val_size=4
   ```

2. Add this line in the `/etc/openradius/dictionaries` file immediately after `dict.ascend`:

   ```
   $include subdicts/dict.checkpoint
   ```

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   ```
   CP-Gaia-User-Role = <role>
   ```

   Where *<role>* is the name of the administrator role that is defined in the WebUI.

   | Administrator Role | Value |
   |---|---|
   | Super Admin | `adminRole` |
   | Read only | `monitorrole` |
   | Networking Admin | `networkingrole` |
   | Mobile Admin | `mobilerole` |

**To log in as a Super User:**

A user with super user permissions can use the Quantum Spark Appliance shell to do system-level operations, including working with the file system.

1. Connect to the Quantum Spark Appliance platform over SSH or serial console.
2. Log in to the Gaia Clish shell with your user name and password.
3. Run: `expert`
4. Enter the Expert mode password.

**Important**:

- To configure the Expert mode (Bash) as the default shell, run this command (**not recommended**):
  ```
  bashUser on
  ```
- To configure the Gaia Clish as the default shell, run this command (**recommended**):
  ```
  bashUser off
  ```

# Managing Authentication Servers

On the **Users & Objects** view > **User Management** section > **Authentication Servers** page you can define and view different authentication servers where users can define both an external user database and the authentication method for users in that database.

You can configure these types of authentication:

- **RADIUS server** - Define the details of a primary and secondary RADIUS server. The Quantum Spark Appliance can connect to these servers and recognize users defined in them and authenticated by them.

  **Note** - In R81.10.10, Two-Factor Authentication is not supported when RADIUS or TACACS is configured for administrator access.

- **TACACS+ server** - TACACS+ is an access control mechanism that enables user authentication and authorization of users by a separate server on the network.

  **Notes:**
  - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.
  - The **VPN** view > **Remote Access** section > **Authentication Servers** page does not show the section **TACACS+ Servers**.

- **Active Directory Domain** - Define the details of the Active Directory domain that contains your organization's user information. The User Awareness feature can use these details to provide seamless recognition of users for logging purposes and user based policy configuration. This can be used for VPN remote access user authentication. When this is the case, additional configuration is necessary in the **VPN** view > **Remote Access** section > **Remote Access Users** page.

# Configuring RADIUS Servers

RADIUS servers can be used for:

- Defining a database of users with remote access privileges. Such users are both defined and authenticated by the RADIUS server.
- Defining administrators. See the **Users & Objects** > **User Management** section > **Administrators** page.

**To add a RADIUS server**

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. In the section **RADIUS Servers**, click **Configure**.
3. In the **Primary** tab, enter this information:
   - **IP address** - The IP address of the RADIUS server.
   - **Port** - The port number through which the RADIUS server communicates with clients. The default is 1812.
   - **Shared secret** - The secret (pre-shared information used for message "encryption") between the RADIUS server and the Quantum SparkAppliance.

     Select **Show** to see the shared secret.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)
   - **Timeout (seconds)** - A timeout value in seconds for communication with the RADIUS server. The timeout default is 3 seconds.

   **Note** - Click **Clear** if you want to remove information you entered in **IP address** and **Shared secret**.
4. On the **Secondary** tab, repeat Step 2 for a Secondary RADIUS server if applicable.
5. Click **Apply**

   The primary and secondary servers (if defined) are added to the RADIUS section on the page.

### To edit a RADIUS server

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. Click the IP address link of the RADIUS server you want to edit.
3. Make the necessary changes.
4. Click **Apply**

### To delete a RADIUS server

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. Next to the RADIUS server you want to delete, click the **Remove** link.

### To configure a RADIUS server administrator

1. Click the **Users & Objects** view > **Users Management** section > **Administrators** page.
2. In the line **Administrator RADIUS authentication is**, click **Edit permissions**.
3. Select **Enable RADIUS authentication for administrators**.
4. Select one of these:
   - **Use roles defined on RADIUS server**
   - **Use default role for RADIUS users**
     a. In the **Default Administrators Role**, select the applicable role.
     b. **Optional:** Select **For Administrators use specific RADIUS group only**.

        Enter the applicable RADIUS groups.
5. Click **Apply**

**To configure remote access permissions for users defined on the RADIUS server**

1. Click the **Users & Objects** view > **Users Management** section > **Administrators** page.
2. Click the link in the sentence **Remote access permissions for RADIUS users are disabled**.
3. Select **Enable RADIUS authentication for User Awareness, Remote Access and Hotspot**.
4. **Optional:** Select **For Remote Access use specific RADIUS groups only**.

   Enter the applicable RADIUS groups.
5. Click **Apply**
6. Configure the remote access permissions for RADIUS users in the **VPN** view > **Remote Access** section > **Remote Access Users** page.

# Configuring TACACS+ Servers

**Notes:**

- In the R81.10.X releases, this feature is available starting from the R81.10.05 version.
- TACACS+ is used for administration only and not for Remote Access authentication.

**To add a TACACS+ server**

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. In the section **TACACS+ Servers**, click **Configure**.
3. In the **Primary** tab, enter this information:
   - **IP address** - The IP address of the TACACS+ server.
   - **Port** - The port number through which the TACACS+ server communicates with clients. The default is 49.
   - **Shared secret** - The secret (pre-shared information used for message "encryption") between the TACACS+ server and the Quantum Spark Appliance.

     Select **Show** to see the shared secret.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)
   - **Timeout (seconds)** - A timeout value in seconds for communication with the TACACS+ server. The timeout default is 3 seconds.

   **Note** - Click **Clear** if you want to remove information you entered in **IP address** and **Shared secret**.
4. On the **Secondary** tab, repeat Step 2 for a Secondary TACACS+ server if applicable.
5. Click **Apply**

**To delete a TACACS+ server**

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. Next to the TACACS+ server you want to delete, click the **Remove** link.

#### To configure a TACACS+ server administrator

1. Click the **Users & Objects** view > **Users Management** section > **Administrators** page.
2. In the line **Administrator TACACS+ authentication is**, click **Edit permissions**.
3. Select **Enable TACACS+ authentication for administrators**.
4. Select one of these:
   - **Use roles defined on TACACS+ server**
   - **Use default role for TACACS+ users**

     In the **Default Administrators Role**, select the applicable role.
5. Click **Apply**

# Configuring Active Directory Servers

### To add an Active Directory domain

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. In the section **Active Directory** section, click **New**.
3. Enter this information:
   - **Domain** - The domain name.

     You cannot create another object with the same **Domain** as an existing Active Directory domain object.
   - **IP address** - The IP address of one of the domain controllers of your domain.
   - **User name** - The user must have administrator privileges to ease the configuration process and create a user based policy using the users defined in the Active Directory.
   - **Password** - The user's password.

     **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)
   - **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually.

     For example: CN=John James,OU=RnD,OU=Germany,O=Europe,DC=Acme,DC=com
4. Select **Use user groups from specific branch only** if you want to use only part of the user database defined in the Active Directory.
   a. Click **New**.
   b. Enter the branch in the Branch full DN in the text field.
   c. Click **Apply**
5. Click **Apply**

### To edit an Active Directory domain

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. In the section **Active Directory** section, select the Active Directory domain.
3. Click **Edit**.
4. Make the applicable changes.

   You cannot change the **Domain**.
5. Click **Apply**

### To delete an Active Directory domain

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. In the section **Active Directory** section, select the Active Directory domain.
3. Click **Delete**.
4. Click **OK** in the confirmation message.

### To change synchronization mode with the defined Active Directories

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. In the section **Active Directory** section, click **Configure**.
3. Select the applicable option:
   - **Automatic synchronization**
   - **Manual synchronization**

     **Note** - With this option, you can synchronize the user database known to the appliance in all locations that this user database can be viewed. For example:
     - The **Users & Objects** view > **User Management** section > **Users** page.
     - The **Access Policy** > view > **Firewall** section > **Policy** page > **Source** picker.
       You cannot select a user from the Active Directory, only an Active Directory user group.
       You can select a local user.
4. Click **Apply**

### To configure remote access permissions for all users defined in Active Directory

By default, users defined in the Active Directory are not given remote access permissions. Instead, in the **VPN** > **Remote Access** section > **Remote Access Users** page all users defined locally or in Active Directories can be selected to be granted remote access permissions per user.

1. Click the **Users & Objects** view > **Users Management** section > **Authentication Servers** page.
2. In the section **Active Directory** section, click the link in the sentence **Remote access permissions for Active Directory users are set in**.
3. Select **All users in Active Directory**.

   With this option, it is not necessary to go to the **VPN** view > **Remote Access** section > **Remote Access Users** page and select specific users.

   Note that most Active Directories contain a large list of users and you might not want to grant them all remote access permissions to your organization.

   Usually you keep the **Selected Active Directory user groups** option and configure remote access permissions on the **VPN** view > **Remote Access** section > > **Remote Access Users** page.
4. Click **Apply**

# Managing Applications & URLs

In the **Users & Objects** > **Applications & URLs** page you can define application groups, custom applications, and view the full list of available applications. You can then use them in the access policy together with the applications and URLs that are in the Application Database. A custom application group lets you define multiple categories and/or sites to use in the access policy Rule Base.

To configure the access policy, click the **applications default policy** link or click the **Applications Blade Control page** link.

For more information about all built in applications and categories, click the **Check Point AppWiki** link at the top of the page.

**Note** - When URL Filtering is selected in the **Access Policy** > **Firewall Blade Control** page, rules containing URLs and custom applications are enforced.

### What is a custom application?

Most applications are browser based. A custom application can be defined using a string or regular expression search on URLs.

### What is a category?

Each URL is inspected by the Check Point Cloud using the URL Filtering and can be matched to one or more built in categories (for example, phishing sites, high bandwidth, gambling, or shopping, etc.).

### The Application and Categories List

A list of applications and categories is shown according to a filter that is shown above the list. There are 4 filters:

- **Common** - Commonly used applications, custom applications, and categories.
- **Custom** - Only custom applications.
- **Categories** - Only categories.
- **All**

A tag icon is shown next to categories and dedicated application icons are shown next to applications.

In the Application Database, each application is assigned to one primary category based on its most defining aspect. It also has additional categories which are characteristics of the application. For example, Pinterest - its primary category is social networking and its additional categories are share photos and SSL protocol. If a category is in a rule, the rule matches all applications that are marked with the category.

If new applications are added to an additional category that is in the access policy Rule Base, the rule is updated automatically when the database is updated.

### To search for a category or application:

1. Filter the list to show the required view.
2. Enter the text of the category of application in the Filter box.

   As you type, the list is filtered.

### To create a custom URL:

1. Select **New** > **URL**.
2. Enter the URL.
3. Click **Apply**

   You can use the URL in a rule.

### To create a custom application:

1. Select **New** > **Application**.
2. Enter a name for the custom application.
3. Select a **Primary category** from the list.
4. Select **All URLs are regular expressions** if you want to use regular expressions instead of partial strings. Regular expressions use **PCRE syntax** (for example, to block www.malicioussite.com using a regular expression you can use **.*\.malicioussite\.com**)
5. Click **New** to add a partial string or regular expression that the appliance will detect in the URL and then Click **OK**.
6. Do step 5 to add more related strings or regular expressions. The custom application will be matched if one of the strings or expressions is found.
7. Click the **Additional Categories** tab to select more categories if necessary.
8. Click **Apply**

   You can use the application in a rule.

**To create a custom applications group:**

1. Select **New** > **Applications Group**.
2. Enter a **Group name**.
3. Select the applications and categories to add as group members. To filter the selection list by common, categories, custom, or all, click the link.

   The group members window shows a quick view of the selected items. You can quickly remove a selected item by clicking the x next to it.
4. If necessary, click **New** to add a custom application or URL to the list. For information on creating a custom application, see above.
5. Click **Apply**

   You can use the custom application group in a rule.

# Managing System Services

The **Users & Objects** > **Services** page lists the system services configured in the system. In this page you can add new services, edit services, and delete services.

You use service objects to easily define the different network protocols. This is usually with IP protocol and ports (used by the TCP and UDP IP protocols).

These objects can be used to define your security policy, as well as policy based routing rules. Many service objects are predefined with the system and cannot be deleted. Those predefined "system services" represent the appliance's ability to perform deep inspection on those services for connectivity and security reasons. The system services sometimes have additional configuration options.

**To create a new service:**

1. Click **New**.
2. In the **Service** tab, enter information in the fields that apply to the type of service you select. Note that not all fields may show:
   - **Name** - Enter the service's name.
   - **Type** - Select the service type from the list:
     - **TCP**
     - **UDP**
     - **ICMP** - Select this option if it is necessary to represent a specific option within the ICMP protocol. Note that this is an advanced option.
     - **Other** - Select this option to represent any IP protocol other than TCP or UDP.
   - **Ports** - Enter the port(s) if you selected Type - TCP or UDP. Enter a specific port number or port range.
   - **IP Protocol** - Enter the IP protocol, if in the **Type** field you selected **Other**.
   - **ICMP type** and **ICMP code** - Enter the ICMP type and code that you want the service object to represent as listed in RFC 792. This option is only relevant, if in the **Type** field you selected **ICMP**.
   - **Comments** - Enter an optional comment.

- **Disable inspection for this service** – Select this checkbox to disable deep inspection of traffic matching this service. This option is only available for built-in services.

3. In the **Advanced** tab, enter information in the fields that apply to the type of service you selected. Note that not all fields may show depending on the service type.

   **General**

   - **Session timeout (in seconds)** - Time in seconds before the session times out.
   - **Use source port** - Select this option and enter a port number for the client side service. If specified, only those source port numbers are accepted, dropped, or rejected when inspecting packets of this service. Otherwise, the source port is not inspected.
   - **Accept replies** (relevant for non-TCP services) - When cleared, server to client packets are treated as a different connection.
   - **Match** (a highly advanced option to be used only by Check Point Support).

   **Connection handling**

   - **Keep connections open after policy has been installed** - Even if they are not allowed under the new policy. If you change this setting, the change does not affect open connections, but only future connections.
   - **Synchronize connections on cluster** - Enables state-synchronized High Availability or Load Sharing on a cluster. Of the services allowed by the Rule Base, only those with Synchronize connections on cluster are synchronized as they pass through the cluster. By default, all new and existing services are synchronized.
   - **Start synchronizing X seconds after the connection was initiated** - For TCP services, enable this option to delay telling the Quantum Spark Appliance about a connection so that the connection is only synchronized if it still exists in X seconds after the connection is initiated. Some TCP services (HTTP for example) are characterized by connections with a very short duration. There is no point in synchronizing these connections because every synchronized connection consumes gateway resources, and the connection is likely to have finished by the time a failover occurs.

### Aggressive aging

This feature can be configured from the **Device** > **Advanced** page. When the appliance is under load, older connections are removed from memory faster to make room for new connections.

- **Enable aggressive aging** - Select this option to manage connections table capacity and reduce gateway memory consumption to increase durability and stability.
- **Aggressive aging timeout (in seconds)** - Time in seconds before the session times out.

4. Click **Apply**

### To edit a service:

1. Select a service from the list.
2. Click **Edit**.
3. Make the necessary changes. Note that not all fields can be edited.
4. Click **Apply**

### To delete a service:

1. Select the service from the list. Note that you can only delete a user defined service.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

### To filter for a specified service:

1. In the **Type to filter** box, enter the service name or part of it.
2. As you enter text, the list is filtered and shows matching results.

### Built-in System Services

Some built-in services represent Check Point's ability to perform deep inspection of the specific protocol. These system services cannot be deleted. When you edit them, the ports which you configure decide when the deep inspection occurs and you can add or change default ports. Some system services have additional configuration which affect the way the deep inspection is performed.

- **HTTP** - The IPS settings tab lets you configure how and when HTTP deep inspection is performed. Select the relevant options.
- **HTTPS** - The URL Filtering settings tab lets you categorize HTTPS sites by information in certificates.
- **FTP** - The Firewall settings tab lets you configure how the firewall automatically detects data connections. You can select one of these options:
  - Any - The Firewall detects and allows FTP data connections in all modes.
  - Active - The Firewall detects and allows FTP data connections in active mode only.
  - Passive - The Firewall detects and allows FTP data connections in passive mode only.
- **PPTP_TCP** - The IPS settings tab lets you configure how PPTP deep inspection is performed.
  - Action on malformed connections - Choose the action to perform on connections when parsing has failed.
  - Tracking - Choose the type of log to issue when parsing fails.
  - Enforce strict PPTP parsing - Select this to enforce strict adherence to the protocol.
- **SNMP** - The Firewall settings tab lets you configure the firewall to enforce a read-only mode in SNMP.
- **SSH** - The Firewall settings tab lets you configure the firewall to block older version of the SSH protocol (1.x).
- **Citrix** - The Firewall settings tab lets you configure which protocol to support on the configured ports. The default port 1494 is commonly used by two different protocols - Winframe or Citrix ICA.

# Managing Service Groups

The **Users & Objects** > **Service Groups** page lists the service groups defined in the system. In this page you can add new service groups, and edit or delete existing service groups.

We recommend you define service groups to configure the security policy. If the security policy is configured with groups and not specified objects, it is much easier to maintain the policy over time. If you decide to add new service objects to the system, you only need to add them to the relevant groups and your policy automatically applies.

There are built in service groups for common services.

Some of these service groups also contain additional configuration for the inspection of the specific protocol.

### To create a new service group:

1. Click **New**.

   The New Service Group window opens.

2. Enter a **Name** for the group and **Comments** (optional).
3. Click **Select** to show the full list of available services and select the relevant checkboxes.
4. Click **New** if the existing list does not contain the services you need. For information on creating a new service object, see the **Users & Objects** > **Services** page.
5. Click **Apply**

   The New Service Group window opens and shows the services you selected.

6. You can also click **New** from the New Service Group window.
7. To remove a service object from the group list, select it and click **Remove**.
8. Click **Apply**

   The service group is added to the list of groups.

### To edit a service group:

1. Select a group from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**

**To delete a service group:**

1. Select the group from the list. Note that you can only delete a user defined service group.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

**To filter for a specified service group:**

1. In the **Type to filter** box, enter the service group name or part of it.
2. As you enter text, the list is filtered and shows matching results.

**Built-in System Service Groups**

Some built-in service groups represent Check Point's ability to perform deep inspection of a specific protocol. Such system service groups cannot be deleted. They contain a list of built in services which you can restore if you edit the content of such groups by clicking **Reset**.

Some system service groups have additional configuration which affect the way the deep inspection is performed.

**DNS** - The Firewall settings tab lets you configure NAT support over DNS. Note that this option affects the performance of DNS traffic and is normally not needed unless your organization uses both NAT and an internal DNS server accessible to the Internet. The IPS settings tab lets you configure how and when DNS deep inspection is performed. Select the relevant options.

# Network Objects and Groups

Starting from R81.10.15, the **Users & Objects** view > **Network Resources** section > **Network Objects** is a unified objects and groups page to create and manage network objects and groups. This replaces the separate **Managing Network Objects** and **Managing Network Object Groups** pages used in version R81.10.10 and lower.

On this page you can add, edit, and delete network objects and groups.

**Important** - You can create a maximum of 1000 objects in total. For example, 500 host objects, 300 network objects, and 200 Domain Name objects.

For each object or group, the columns in the table display the name, type, information (for example, IP address or range of an object) and starting from R81.10.05, where it is used, for example the specific rules in the Access Policy.

**Note** - Starting in version R81.10.17, the "Where in use" feature is turned off by default.
To enable this feature, go to *"Advanced Settings" on page 246* > **WebUI settings and customizations - Enable where in use** and change the value to `true`.

Use the **Search** field at the upper right corner of the page to search for an object. The table display highlights the group in which the object is found.

For each group, when you hover over one of the objects within the group, you can see specific information about the object such as its type, IP addresses and in which group it is used.

The most common use for network objects is to define a security policy and exceptions to it. These objects can be used as hosts for the internal DNS service and their IP addresses can be configured as fixed for the internal DHCP service.

You can make a new access policy rule in the **Access Policy** > **Firewall** > **Policy** page and use one of the network objects or groups as the source or destination. The **Manual Rules** table on the **Access Policy** page displays the objects in the relevant rule. The **Where Used** column in the **Network Objects** table shows also displays the access policy rule you just created.

**To create a new network object on the Network Objects page:**

1. Click **New** and select **Network Object**.
2. In the **New Network Object** window, select **Type**:
   - **Network** - Represents a network.
   - **Single IP** - Represents a device with a single IP address (host object). Select or clear these options as necessary:
     - **Allow DNS server to resolve this object name** - When the gateway is the DNS server for your internal networks, the name of the server / network object is translated to its IP address.
     - **Exclude from DHCP service** - The internal DHCP service does not distribute the configured IP address of this server / network object to anyone.
     - **Reserve IP address for DHCP service for MAC** - The internal DHCP service distributes the configured IP address only to this server / network object based on its MAC address.
     - Enter the **MAC address** - This is required for IP reservation. When you create the object from the Assets page, the MAC address is detected automatically.
   - **IP Range** - Represents a range of IP addresses. Enter the **Start IP** and **End IP**. Select or clear this option as necessary:

     **Exclude from DHCP service** - The internal DHCP service does not distribute the configured IP range to anyone.

- **Wildcard** - Represents IP addresses that share a common pattern. For example, all IP hosts with the IP address 250 on different networks: 192.168.*.250 / 24

  **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.08 version Build 996001739.

  a. In the New Network Object window, enter the **Name** (mandatory field).

  b. In versions R81.10.15 and lower, enter the **Wildcard IP** address. This is the wildcard pattern and shows the "*" in a particular position in the IP address. For example, 172.168.*.110

  c. Click **Save**.

  **Limitations:**

  - IPv6 addresses are not supported.
  - In the wildcard IPv4 address, the asterisk octet always has the IPv4 subnet mask octet 255.

    Examples:

    - IPv4 address with a wildcard: X.X.*X
    - IPv4 address with a wildcard: X.*.X.X

    In both examples, the IPv4 subnet mask that the Access Policy applies is 255.255.255.255

- **Domain Name** - This text string maps to the alphanumeric IP addresses used to access a Domain. For example, the Domain Name for Google is "google.com". The actual website (domain) address is an IP address but DNS allows you to enter a Domain Name to be routed to the exact website.

  **Note** - The Domain Name object must exactly match the Domain name.

- **Device** - Enter the MAC address. **Optional**: Select **Bypass host with this MAC by SSL Inspection**.

  If you select to **Use custom hardware name**, enter the **Device type**, **Hardware**, and **Operating system**

3. Enter the **Name** and **IP address**.
4. Depending on the object type, you may need to configure additional fields.
5. Click **Save**.

Starting from R81.10.15, you can also create a new network object on the *"Configuring the Remote Access Blade" on page 355* page > **Allow or block selected objects** section.

**To create a new Network Object Group on the Network Objects page:**

1. Click **New** and select **Network Object Group**.
2. In the **New Network Object Group** window, enter a **Name** for the group.
3. **Optional:** Add a comment.
4. Select existing objects to add to this group or click **New** to create a new object.
5. Click **Save**.

**To use an object in an Access Policy rule:**

1. In WebUI, click the **Access Policy** view > **Firewall** section > **Policy** page.
2. Add a new rule or edit an existing rule.
3. In the **Source** column or the **Destination** column, select the object.
4. Configure other columns in this rule.
5. Click **Save**.

## Editing, Deleting and Filtering Network Objects

**To edit a network object:**

1. Select a network object from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Save**.

**To delete a network object**

1. Select the network object from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

**To filter for a specified network object**

1. In the **Type to filter** box, enter the name of the network object or part of it.
2. As you enter text, the list is filtered and shows matching results.

### To add a new network object and bypass SSL inspection based on the host MAC address (Locally Managed only)

1. Click **New**.

   The **New Network Object** window opens.

2. In **Type**, select **Device**.
3. In **Host MAC address**, enter a custom value or select from the menu.
4. Select **Bypass host with this MAC by SSL inspection**.
5. In **Object name**, enter the applicable text.
6. Click **Apply**

**Note** - You can also do this on the **Home** > **Assets** (starting from R81.10.10) or **Active Devices** page. Click **Save as** and select **Device type Network Object**.

# Managing Network Object Groups

Starting from R81.10.15, this no longer exists as a separate page on the appliance WebUI. To create and manage network objects and groups, see the **Unified Network Object and Groups Page**.

The **Users & Objects** > **Network Object Groups** page lists the network object groups defined in the system. In this page you can add new network object groups, edit network object groups, delete network object group, and see where the network objects are in use.

We recommend you define groups for network objects to configure the security policy. If you configure security policy with groups and not specified objects, it is much easier to maintain the policy over time. When new network objects are added to the system, you only need to add them to the relevant groups and your policy automatically applies.

**To create a new network object group:**

1. Click **New**.

   The New Network Object Group window opens.

2. In **Name**, enter the applicable text.
3. **Optional:** In **Comments**, enter the applicable text.
4. Click **Select** to show the full list of available network objects and choose the relevant checkboxes.
5. Click **New** if the existing list does not contain the network object you need.

   For information on creating a new network object, see the **Users & Objects** > **Network Objects** page.

6. Click **Apply**

   The New Network Object Group window opens and shows the services you selected

7. You can also click **New** from the New Network Object Group window.
8. To remove a network object from the group list, select it and click **Remove**.
9. Click **Apply**

   The network object group is added to the list of groups.

### To edit a network object group:

1. Select a group from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**

### To delete a network object group:

1. Select the group from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

### To filter for a specified service group:

1. In the **Type to filter** box, enter the network object group name or part of it.
2. As you enter text, the list is filtered and shows matching results.

# Logs and Monitoring

This section describes the security and system logs. It also describes various monitoring tools.

## Viewing Security Logs

The **Logs & Monitoring** > **Logs** > **Security Logs** page shows the last 100 log records.

To load more records, continue scrolling down the page. The log table is automatically refreshed.

### To search for a security log

Enter your query in the **Enter search query** search field on the right side of the screen and click the search icon 🔍.

### If you require assistance to create a query:

1. Click the **Query Syntax** icon ? next to the search field.
2. The Query Syntax window opens and shows examples for:
   - General Search - A simple string or an IP address.

     Example: `203.0.113.64`
   - Focused Search - <Field-Name>:<criteria>. The Field Name can be the name of a table column or a field from the log details.

     Example: `action:drop` or `source port:22`
   - You can use operators in your search. Examples:

```
[NOT] text1 AND [NOT] text2 … AND [NOT] textn
[NOT] text1 OR [NOT] text2 … OR [NOT] textn
[NOT] field1:value1 AND [NOT] field2:value2 … AND [NOT]
fieldn:valuen
[NOT] field1:value1 OR [NOT] field2:value2 … OR [NOT]
fieldn:valuen
```

**Notes**:

- Search is not case-sensitive.
- Make sure there is no space between the field name and the search criteria.

### To limit the number of logs to search:

1. Click the **Settings** tab.
2. In the **Security Logs Settings** window, select the checkbox **Limit the number of logs to search**.
3. In the **Maximum number of logs to search** field, use the arrows to select the desired number.
4. Click **Save**.

### To see the security log record

1. Select a log entry from the list.
2. Click **View Details** or double-click the entry.

   The log record opens.

### To refresh the security log data

Click the **Refresh** icon 🔄.

### To stop local logging:

When necessary, you can stop local logging for better performance. This removes the overhead of creating and maintaining logs. No new logs are generated until you set the resume option.

1. Select **Actions** > **Stop local logging**.
2. To resume, select **Actions** > **Resume local logging**.

   **Note** - In version R81.10.08 and lower, select **Options** instead of **Actions**.

### Storing Logs

Logs can be stored locally on the appliance's non-persistent memory or on an external SD card (persistent). Logs can also be sent to an externally managed log server (see **Log Servers** page).

When you insert an SD card, it mounts automatically and then local logs are saved to it. Before you eject an SD card, make sure to unmount it. Select **Actions** > **Eject SD card safely**.

**Note** - In firmware versions R81.10.00 and higher, SD cards are formatted with the `ext4` file system. In older firmware versions, SD cards are formatted with the `FAT32` file system. If you upgrade to a version R77.20.85 or higher, the file system on the SD card remains `FAT32` for backward compatibility.

### To delete logs from local log storage

1. In **Logs & Monitoring** > **Logs** > **Security Logs** page, click **Clear logs**.

   A confirmation window opens.

2. Click **Yes** to delete logs.

   The logs are deleted, and the logs grid reloads automatically.

**Note** - Logs are deleted from the external SD card (if inserted) or from the local logs storage. Logs are not deleted from the remote logs server.

The logs are deleted, and the logs grid reloads automatically.

### Exporting Security Logs

To export the security logs, see *"Configuring External Log Servers" on page 480*.

# Viewing System Logs

The **Logs & Monitoring** > **System Logs** page shows up to 500 systems logs (syslogs) generated from the appliance at all levels except for the debug level. These logs should be used mainly for troubleshooting purposes and can also give the administrator notifications for events which occurred on the appliance.

These are the syslog types:

- **Info** - Informative logs such as policy change information, administrator login details, and DHCP requests.

  **Audit logs** show each operation of the administrator from the WebUI, Gaia Clish, Mobile, or Quantum Spark Portal.

  **CPOSD** logs show new configurations.

- **Notice** - Notification logs such as changes made by administrators, date, and time changes.
- **Warning** - Logs that show a connectivity or possible configuration failure. The problem is not critical but requires your attention.
- **Error** - System errors that alert you to the fact that a specific feature is not working. This can be due to misconfiguration or connectivity loss which requires the attention of your Internet Service Provider.

**To download the full log file:**

1. Click **Download Full Log File**.
2. Click **Open** or **Save**.

**To refresh the system logs list:**

Click **Refresh**.

**To clear the log list:**

1. Click **Clear Logs**.
2. Click **OK** in the confirmation message.

**To search system logs table:**

Enter keyword for the log in the text search field.

# Viewing Audit Logs

Audit Logs are records for actions on the Quantum Spark appliance, such as login, logout, and configuration change s(in the appliance settings, in objects, in rules, and more).

By default, these Audit Logs are only saved locally.

To view the Audit Logs, go to the **Logs & Monitoring** view > **Logs** section > **Audit Logs** page.

Starting in R81.10.15, you can configure the appliance to send these local Audit Logs to Quantum Spark Management.

**Advantages:**

- **Centralized Monitoring** - View all audit logs in a dedicated monitoring page within the SMP. This centralized view allows for easy tracking of all changes made to the system components and objects.
- **Comprehensive Tracking** - Monitor changes related to users, administrators, security rules, allow lists, block lists, internet objects, IP addresses, MAC addresses, VPN operations, and more. Any modifications to critical security settings and configurations are logged and can be reviewed for accountability and security purposes.
- **Enhanced Security and Compliance** - Ensure that all administrative actions are logged, providing a detailed record for compliance audits and security reviews. This helps you detect unauthorized changes and enables you to take corrective actions promptly.
- **Operational Transparency** - Provide a transparent view of all administrative operations, making it easier to troubleshoot issues and understand the impact of specific changes.

**Known Limitations:**

- Export of Audit Logs supports only configuration changes in WebUI and Gaia Clish.
- Export of Audit Logs for changes in the Dynamic Routing settings you make in Gaia Clish is not supported.
- Export of Audit Logs for users' login / logout is not supported.

### To export Audit Logs to Quantum Spark Management:

**Note** - The Quantum Spark gateways must be connected to the Quantum Spark Management service in Infinity Portal.

1. On each Quantum Spark gateway, connect to the command line.
2. Log in to Gaia Clish.

3. Enable the export:

   ```
   set logs-config send-audit-on-db-change true
   ```

   To disable, configure the value "`false`".

For more information, see the *Quantum Spark Management Administration Guide* > Chapter "Logs and Events" > Section "Working with Audit Logs".

# Configuring External Log Servers

The **Logs & Monitoring** > **Log Servers** page lets you configure external log servers for security and system logs for additional logging storage.

**Note** - You cannot configure external log servers when Cloud Services is turned on.

## External Check Point Log Server

You can use an external Check Point Log Server that is managed by a Security Management Server for storing additional logs.

**Use cases for an external Check Point Log Server:**

- Extend the log retention time. For example, currently, when your gateway is managed by Quantum Spark Portal, you can retain logs for 3 months. If you configure an external Log Server, you can retain the logs for a year.
- Export the logs format to a 3rd party mechanism for data mining.

**Do these steps before you configure an external Check Point Log Server from this page in the WebUI:**

1. Identify the Log Server you want to send logs to.
2. Identify the Security Management Server that manages the Log Server.
3. Open SmartConsole on this Security Management Server.
4. Run the Security Gateway wizard to define and create a Security Gateway object that represents this appliance with the these details:

   In the **General Properties** window, select:

   - **Gateway platform** - Select your appliance
   - **Gateway IP address - Dynamic IP address**

   In the **Trusted Communication** window, from **Gateway Identifier** select **MAC address** or **First to connect**.
5. Install the database on the Security Management Server and other related objects.

**To configure an external Check Point Log Server:**

1. Under **Check Point Log Server**, click **Configure**.

   The External Check Point Log Server window opens.

2. Enter the **Management Server IP address**.

   This IP address is used only to establish trusted communication between the appliance and the Security Management Server.

3. In **SIC name**, enter the SIC name of the Log Server object defined in SmartConsole.

   These are the options to get this name:

   - **Option 1:**

     a. Connect with Database Tool (GuiDBEdit Tool) (see sk13009) to the Security Management Server.

     b. From the **Tables** tab, expand **Table** > **Network Objects**.

     c. In the right pane, locate the Log Server object.

     d. In the bottom pane, locate **sic_name**.

   - **Option 2:**

     Run this CLI command on the Log Server in the Expert mode (use SSH or console connection):

     ```
     $CPDIR/bin/cpprod_util CPPROD_GetValue SIC MySICname 0
     ```

   Copy the SIC name value and paste it into the SIC name field on this page.

4. In **Set SIC One-time Password**, enter the same password that was entered for the Security Management Server and then enter it again in the **Confirm SIC One-time Password** field.

   **Note** - You cannot use these characters in a password or shared secret: { } [ ] ` ~ | ' " \ (maximum number of characters: 255)

5. If the Log Server is not located on the Security Management Server, select **Log server uses different IP address** and enter the IP address.

6. Click **Apply**

   **Important**:
   - After successful configuration of the external log server, any changes you make in the WebUI configuration on this page requires reinitialization of the SIC in SmartConsole. If you do not reinitialize SIC in SmartConsole, connectivity to the log server can fail.
   - To see the logs, you must connect with SmartConsole to the dedicated Log Server (and not the Security Management Server).

**To configure a new external Check Point Log Server when the gateway is connected to Quantum Spark Portal (Cloud):**

After you initiate traffic from resources behind the gateway, open the Check Point Log Server to verify that you see the logs.

# Syslog Server Configuration

You can configure a gateway to send logs to multiple syslog servers. - Only one secure syslog server is supported.

**To configure a syslog server:**

1. Under **Syslog Servers**, click **Configure**.

   The Syslog Server window opens.

2. Select **Protocol**:

   - **UDP** - Send security logs or system logs (not secured).
   - **TLS Over TCP (secured)** - Send system or security logs from gateways in a secured and encrypted fashion.

3. Enter a **Name** and **IP address**/ **Host Name**.
4. Enter a **Port** number.
5. Select **Enable log server**.
6. **Optional** - Select **Show obfuscated fields**. Obfuscated packets are shown as plain text.
7. Select **Forwarded logs**:

   - System logs
   - Security logs

8. Click **Upload** to upload a Trusted CA Certificate.
9. Click **Apply**

# Secured Syslog

### Use Case

A system administrator wants to send system and/or security logs from the organization's gateways in a secured and encrypted fashion. Therefore, he selects TLS Over TCP as the protocol. UDP is not secure.

**Notes:**

- Only one remote TLS server is supported.
- You can upload a CA certificate to establish trust with the remote syslog server.
- The TLS server must be configured using its domain name. Only UDP allows you to configure the server by IP address.
- The configured domain name must be identical to the domain name in the server's certificate.
- Both system and security logs are supported.

**To configure additional syslog servers:**

Click **Add a syslog server...**.

**To edit the syslog server:**

1. Click the **Edit** link next to the server's IP address.
2. Edit the necessary information.
3. Click **Apply**

**Note** - When more than one server is defined, the syslog servers appear in a table. Select the syslog server you want to edit and click **Edit**.

**To delete the syslog server:**

1. Select the syslog server.
2. Click **Delete**.

# Notifications

See *"Notifications" on page 60*.

# Managing Active Devices

**Important** - This page is only relevant for versions up to R81.10.08. Starting in R81.10.10, **Active Devices** and **Wireless Active Devices** are replaced by the **Home** > **Assets** page.

The **Active Devices** page shows a list of the devices identified in internal networks. You can access this page from the **Logs and Monitoring** tab > **Status** section and from the **Home** tab > **Monitoring** section.

The table shows these columns:

- **Name** - Hostname of the device.
- **IP address** - IP address of the device.

  **Note** - If a device has both IPv4 and IPv6 addresses, there is a single entry in the table.

- **MAC Address** - MAC Address of the device.
- **Device Details** - Type of the device.
- **Blocked** - Indicates whether the device is blocked from network activity.
- **Interface** - Name of the appliance interface, to which the device is connected.

## Blocking a Device Manually

Click the device to select it and click **Block**.

# Toolbar Buttons

- **Filter** - Filter the list by servers, active devices, or known devices.
- **Refresh** - Refresh the information in the list.
- **Details** - Select a row in the list and click **Details** to show additional properties of the device.
- **Save as** - Save a selected device as a network object or server.

  When you select this option, the **New Network Object** (see *"Network Objects and Groups" on page 466*) window or **New Server Wizard** (see *"Defining Firewall Servers" on page 267*) opens.

  Enter the information in the fields and click **Apply**. Use these objects to reserve IP addresses to MAC addresses in the DHCP server and also add this object name as a device in the local DNS service. Network objects and server objects can be used in the security configurations, for example in the Access Policy and IPS exceptions

  A server object also allows you to configure access and NAT if applicable as part of the object. If access and/or NAT are configured, automatic access rules are created in the Access Policy Rule Base.
- **Start/Stop Traffic Monitor** - Gather upload and download packet rates for active devices.

  This operation may affect performance. To stop, click **Stop Traffic Monitoring**.
- **Revoke Certificate** - Revokes the certificate assigned to the device.

## Revoking the Hotspot Access

The display shows the devices connected to the gateway through a Hotspot.

You can revoke the Hotspot access for one or more devices.

This disconnects the device from the gateway and requires the device to log in again through the Hotspot.

**To revoke the Hotspot access:**

1. Click the record for the relevant device.
2. Click **Revoke Hotspot Access**.

   The access for that device is revoked. You must log in again through the Hotspot to reconnect the device to the gateway.

**Notes:**

- This page is available from the **Home** and **Logs & Monitoring** tabs.
- If there is no IPv6 activity in a dual stack host, the Active devices do not show the IPv6 address.

## Adding a New Network Object to Bypass SSL Inspection Based on the Host MAC Address

1. Click the device to select it.
2. From the toolbar, click **Save as** and select **Device type Network Object**.
3. For **Host MAC address**, enter a custom value or select from the menu.
4. Select **Bypass host with this MAC by SSL inspection**.
5. In **Object name**, enter the applicable text.
6. Click **Apply**

**Note** - You can also do this from the **Users & Objects** > **Network Objects** page. Click **New**, and then for **Type**, select **Device**.

# Assets

Starting from R81.10.10, the **Home** >**Monitoring** > **Assets** page replaces the **Active Devices** and **Wireless Active Devices** pages.

The **Assets** page displays devices in the internal networks. When an asset is connected to the gateway, it automatically appears here.

The top of the page shows multiple counters:

- **Assets** - Total number of connected devices.
- **IoT Assets** - Relevant only when the IoT protection is enabled. For more information, see the *"IoT Protect" on page 300* page.
- **Manually blocked**.
- **Infected**.
- **Assets attempted to access unauthorized domains** - Assets which accessed or attempted to access a domain that is not under IoT policy in the last 7 days.
- **Not under IoT policy** - Relevant only when the IoT protection is enabled. For more information, see the *"IoT Protect" on page 300* page.

The graph icon on the far right shows the breakdown of the device types, such as IP camera, Media player, Scale, SmartTV, and Other.

You can filter to show a specific type of assets. For example, if you filter for IP camera, you see the number of IP camera types and the relevant vendors. You can see general information about the asset such as the traffic upload and download, and the policy. In the **Asset Details** tab, you can set the asset to bypass by Smart Accel, or bypass by SSL inspection. You can also create a network object directly from the **Assets** page.

All connected assets are displayed in a table with these columns:

- **Name** - Name of the device. The vendor icons appear next to the name.
- **IP Address**
- **Interface**
- **Vendor**
- **Device Type**

For each asset, click one of these options:

- Refresh
- **Actions**

    - **TCpdump Tool** - Opens a popup window in which you can capture traffic that passes through appliance interfaces. For more information, see *"Using System Tools" on page 507*.
    - **Reserve IP address** - Click **Add** to reserve an IP address for this asset. This creates a network object with the asset name.
    - **Export assets to a csv file** - Click the **Export to csv** button to create a csv file with all asset data.
    - **Block** - Prevent this asset from sending traffic.
    - **Delete** - Delete this asset from the list of connected devices.
    - **Monitoring** - Receive notifications if the asset is not answering to ping. You can do this per function or per asset.
    - **Recognize** - Run the recognition process for a single asset , all assets, or for unrecognized assets.
    - **Scan** - Scan the asset with one of these options: Ping, ARP, SNMP.
- Show WiFi data

On the **Assets** page, IoT assets that are **Not under IoT policy** are marked with this icon 💎 (relevant if the IoT blade is turned on).

**To see the Asset Details:**

1. Go to the **Home** > **Monitoring** > **Assets** page.
2. Click the table row with the asset name.
3. The **Asset Details** open in a popup window with these tabs:
    - **Asset Details** - Shows these fields: **Vendor**, **Model**, **Interface**, **Last seen**, **Download speed**, **Upload speed**, **View security logs**.
    - **IoT** - **Access from the Internet** (domains allowed to access your device) and **Policy**. If these options are grayed out, you cannot make any changes. Otherwise select from the pulldown menu).
    - **Override/Bypass** - Describes override and bypass behavior: **Asset description**, **Override** (select **Asset type** and **Vendor** from the pulldown menu), **Bypass** (select the applicable checkboxes to bypass by Smart Accel and to bypass by SSL Inspection.

**To see an asset's status:**

1. Go to the **Home** > **Monitoring** > **Assets** page.
2. Double -click the table row with the asset name.
3. Click the arrow next to **Status** to expand the section.
4. Select the **Filters** icon to see the number of assets in this category/rank:
   - **IoT** - Number of connected IoT devices.
   - **Manually blocked**
   - **Infected**
   - **Unauthorized** - Attempts to access unauthorized domains.
   - **Unprotected** - Number of devices not protected by the IoT protection policy,
   - **Low confidence** - You can protect an asset from the Assets page only if the Low confidence rank is less than 10. This means that the recognition service is not sure, for example, if the device is an IoT device.
   - **Override**
5. Click the arrow to expand the **Functions** section.
6. Click the arrow to expand the **Interface** section.

# Wireless Active Devices

**Important** - This page is only relevant for versions up to R81.10.08. Starting in R81.10.10, **Active Devices** and **Wireless Active Devices** are replaced by the **Home** > **Assets** page.

The **Logs & Monitoring** view > **Status** section > **Wireless Active Devices** page shows the devices connected to your gateway's wireless network.

The information for each connected device's network usage includes:

- **SSID** - Name of the WiFi network
- **Type** - Shows the connection type a device is connected with over WiFi.

  **Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.
- **Channel**
- **Frequency**
- **Signal Strength**
- **RSSI** - Received Signal Strength
- **Bandwidth**
- **IP Address**
- **MAC address**

# Paired Mobile Devices

The **Logs & Monitoring** > **Paired Mobile Devices** shows the mobile devices paired to the gateway.

**To revoke a pairing:**

1. Select the device name.
2. Click **Revoke**.
3. In the confirmation window that opens, click **Yes**.

# Viewing Infected Devices

In the **Infected Devices** page you can see information about infected devices and servers in the internal networks. You can also directly create an exception rule for a specified protection related to an infected or possibly infected device or server.

You can access this page from the **Threat Prevention** tab > **Threat Prevention** section, or from the **Logs and Monitoring** tab > **Status** section.

The Infected Devices table shows this information for each entry:

- **Icon** - Shows icons for the different classifications of infected devices and servers.

| Description | Host Icon | Server Icon |
|---|---|---|
| Infected device or server - When the Anti-Bot blade detects suspicious communication between the host or server and an external Command & Control center due to a specified triggered protection | 🖥 | 🗄 |
| Possibly infected device or server - When the Anti-Virus blade detects an activity that *may* result in host or server infection. For example:<br>• When you browse to an infected or a potentially unsafe Internet site, there is a possibility that malware was installed.<br>• When you download an infected file, there is a possibility that the file was opened or triggered and infected the host or server. | 🖥? | 🗄? |

- **Object name** - Shows the object name if the host or server was configured as a network object.
- **IP/MAC address** - Shows the IP and MAC address of the infected device.
- **Device/User Name** - Shows a device or user name if the information is available to the appliance through DHCP or User Awareness.
- **Incident type** - Shows the detected incident type:
  - Found bot activity
  - Downloaded a malware
  - Accessed a site known to contain malware
- **Severity** - Shows the severity of the malware:

  - Low
  - Medium
  - High
  - Critical

- **Protection name** - Shows the Anti-Bot or Anti-Virus protection name.
- **Last incident** - The date of the last incident.
- **Incidents** - Shows the total number of incidents on the device or server in the last month. If there is a large amount of records, the time frame may be shorter.

**To filter the infected devices list**

1. Click **Filter**.
2. Select one of the filter options:
    - **Servers only** - Shows only machines that were identified as servers (and not any machine/device).

      Servers are defined as server objects in the system from the **Access Policy** > **Servers** page.
    - **Possibly infected only** - Shows only devices or servers classified as possibly infected.
    - **Infected only** - Shows only devices or servers classified as infected.
    - **High and above severity only** - Shows devices and servers that are infected or possibly infected with malwares that have a severity classification of high or critical.

**To add a malware exception rule for a specified protection**

1. Select the list entry that contains the protection for which to create an exception.
2. Click **Add Protection Exception**.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the exception rule fields.
   - **Scope** - Select either **Any** or a specific scope from the list. If necessary, you can create a **New** network object, network object group, or local user.

     If it is necessary to negate a specified scope, select the scope and select the **Any Scope except** checkbox.

     For example, if the scope of the exception should include all scopes *except* for the DMZ network, select DMZ network and select the **Any Scope** except checkbox.

     **Note** - DMZ is not supported in 1530 / 1550 appliances.
   - **Action** - Select the applicable action to enforce on the matching traffic: **Ask**, **Prevent**, **Detect** or **Inactive**.

     See the **Threat Prevention** > **Threat Prevention Blade Control** page for a description of the action types.
   - **Log** - Select the tracking option: **None**, **Log**, or **Alert**.

     Logs are shown on the **Logs & Monitoring** > **Security Logs** page.

     An alert is a flag on a log. You can use it to filter logs.
4. **Optional** - Add a comment in the **Write a comment** field.
5. Click **Apply**

   The rule is added to **Malware Exceptions** on the **Threat Prevention** > **Exceptions** page.

**To view the logs of a specified entry:**

1. In the Logs and Monitoring tab, select the list entry for which to view logs.
2. Click **Logs**.

   The **Security Logs** page opens and shows the logs applicable to the IP/MAC address.

# Viewing VPN Tunnels

In the **VPN Tunnels** page, you can see current VPN tunnels opened between this gateway and remote sites. Some sites are configured so tunnels are established only when necessary and some are configured with permanent tunnels. When the appliance is managed by Cloud Services, this table also shows the tunnels for the gateways in the community.

The table below shows the details of each tunnel configured:

| Field | Description |
|---|---|
| **Status** | Indicates if a tunnel is up or is pending traffic to become active. |
| **Site Name** | The VPN site name. |
| **From** | The external interface the tunnel uses. |
| **Peer Address** | Host name or IP address of the tunnel's destination gateway. |
| **Tunnel Creation Time** | Date the tunnel was created. |
| **Tunnel Expiration Time** | Date the tunnel expires. |
| **Community Name** | If the gateways are part of a community configured by Cloud Services, the community name with which the tunnel is associated.<br>Visible when the Quantum Spark gateway is configured in the Quantum Spark Management service in Infinity Portal. |
| **My Encryption Domain** | Indicates the tunnel's selectors (subnets/hosts) allowed from the source gateway. |
| **Peer's Encryption Domain** | Indicates the tunnel's selectors (subnets/hosts) allowed from the destination gateway. |
| **Phase 2 Methods** | Encryption and authentication methods used for the tunnel. |
| **Connections Per Instance** | The number of connections associated with the tunnel per instance. This lets you know if a tunnel is over-utilized. |

**To filter the list:**

In the **Type to filter** box, enter the filter criteria.

### To refresh the list:

Click **Refresh** to refresh manually this page with updated tunnel information.

### To delete all Security associations for a selected peer:

Click **Delete all SAs for the selected peer**.

**Note** - This page is available from the **VPN** and **Logs & Monitoring** tabs.

# Viewing Active Connections

The **Logs & Monitoring** > **Connections** page shows a list of all active connections.

The list shows these fields:

- Protocol
- Source Address
- Source Port
- Destination Address
- Destination Port

### To filter the list:

In the **Type to filter** box, enter the filter criteria.

The list is filtered.

### To refresh the list:

Click the **Refresh** link.

# Access Points

The **Logs & Monitoring** > **Access Points** page shows the available access points around your gateway. The network information includes:

- Channel
- Frequency
- Security
- Signal strength
- Signal noise

**Use case:**

Use this information to decide which network to connect to, and change based on your needs.

In addition, this page displays the current wireless radio frequency and channel in use and the wireless networks configured.

# Viewing Monitoring Data

See *"Viewing Monitoring Data" on page 68*.

# Extended Monitoring

## Overview of Extended Monitoring

Quantum Spark Appliances do not have sufficient storage to keep all logs and monitoring data.

You can configure your Quantum Spark Appliance to upload the logs to Check Point cloud (the appliance uploads the logs to the Quantum Spark Management service in Infinity Portal).

When you need to review the data, your Quantum Spark Appliance download the applicable logs from Check Point cloud and shows them in WebUI.

## Requirements for Extended Monitoring

1. The Quantum Spark Appliance must run the firmware R81.10.15 or higher.
2. The Quantum Spark Appliance must be connected to Cloud Services with the option **"Use Cloud Capabilities"**.

   See *"Connecting to Cloud Services" on page 54*.

**Note** - If your Quantum Spark Appliance with the firmware R81.10.10 or lower was already connected to Quantum Spark Management, then after the firmware upgrade, the Extended Monitoring feature is available on your Quantum Spark Appliance.

## Description of the WebUI Page

The **Logs and Monitoring** view > **Monitoring** section > **Extended Monitoring** page shows three tabs with multiple sections:

- **Traffic** - with these sections:
  - **Sources by Bytes**
  - **Applications by Bytes**
  - **Destinations by Bytes**
  - **Services by Bytes**
- **Logs** - with these sections:
  - List of log records
  - **Statistics**
  - **Blade**
  - **Action**
  - **Interface Name**

  - **Origin**
  - **Service**
- **Remote Access** - with these sections:
  - Various widgets with data about the Remote Access VPN users and their traffic
  - **Top applications by traffic**
  - **Traffic over time**

## Viewing Log Records

You can review the logs in two places:

- In the Quantum Spark Management service > **Logs & Events** view.

  See the *Quantum Spark Management Administration Guide*.

- On your Quantum Spark Appliance > **Logs and Monitoring** view > section **Monitoring** > **Extended Monitoring** page.

  Each tab has the Search bar at the top:

  - On the left of the Search filed, you can click to select a preset time filter.
  - In the Search field, you can enter a string to filter the results in all sections (for example, enter an IP address).
  - On the right of the Search field, you can click the applicable button - to enable an automatic refresh or to refresh manually.

# Viewing Reports

See *"Viewing Reports" on page 73*.

# Dr. Spark

With the Dr. Spark feature, you can check the Quantum Spark Appliance performance, sizing and health status.

**Note** - The Dr. Spark feature is available as a separate tab starting from R81.10.08. In earlier versions, the Dr. Spark buttons are available on the *"Using System Tools" on page 507* page.

| Action | Description |
|---|---|
| **Generate the Dr. Spark Report** | Saves a report that shows if the appliance passed or failed various tests.<br>If the appliance fails a test, the report provides more details to describe why it failed.<br>**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.<br>**Procedure**<br>1. Click **Generate the Dr. Spark Report**.<br>A message next to the button shows the progress.<br>Do not move to another WebUI page.<br>2. When the task completes, the button changes to **Download Dr. Spark Report**.<br>3. Click **Download Dr. Spark** to download the report file.<br>Your web browser saves this file (`DrSpark_<YYYY-MM-DD_HH-MM-SS>.zip`) in the default download folder.<br>4. When the download completes, the button changes to **Generate the Dr. Spark Report**.<br>5. Extract the content of this ZIP archive.<br>6. Open the file **index.html** in a web browser.<br>Legend:<br>- ✓ - The appliance passed this test.<br>- ❗ - The appliance failed this test.<br>- ⓘ - General information for the administrator.<br>- ⓘ - This test was not applicable to this appliance. |
| **Download Last Report** | Prints the last report generated.<br>**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.08 version. |

| Action | Description |
|---|---|
| **Dr. Spark - Load** | Saves a short report with the data about the current Security Gateway performance.<br>**Note** - In the R81.10.X releases, this feature is available starting from the R81.10.05 version.<br>**Procedure**<br>1. Click **Dr. Spark - Load**.<br>A message next to the button shows the progress.<br>Do not move to another WebUI page.<br>2. When the task completes, the button changes to **Download Dr. Spark Load**.<br>3. Click **Download Dr. Spark** to download the report file.<br>Your web browser saves this file (`drSMB_diag_last_perf_run.txt`) in the default download folder.<br>4. When the download completes, the button changes to **Dr. Spark - Load**.<br>5. Use a text editor to view this report.<br>**Example Report**<br>`Gateway Performance:`<br><br>`Number of hosts: 0`<br>`Number of connections: 64`<br>`Connection rate: 69 per second`<br>`Throughput:`<br>` Receive: 8327 Kbps`<br>` Transmit: 3448 Kbps`<br>`Packet Rate:`<br>` Receive: 30 packets per second`<br>` Transmit: 27 packets per second`<br>`SSL is disabled`<br>`-----Blade Status-----`<br>`VPN-RA is enabled but no users are set up`<br>`VPN-S2S is enabled but no tunnels are up`<br>`NGTP is active`<br>`----CPU and Memory----`<br>`Available CPU: 99.61%`<br>`Available memory on the Gateway: 3943320 KB`<br>`Fw1 memory consumption: 11%`<br>`SFWD memory consumption: 181648 KB` |

# Offline installation procedure

If your Security Gateway is not connected to the Internet (versions R81.10.05 and higher), or if your Security Gateway runs R81.10.00, you can install the latest Dr. Spark tool in this way:

1. Download the installation script for your Quantum Spark appliance model to your computer:
   - For 2000 / 1900 / 1600 / 1800:

     https://support.checkpoint.com/results/download/123706
   - For 1500 / 1400 / 700:

     https://support.checkpoint.com/results/download/123700
2. Copy the script from your computer to the Quantum Spark appliance to the `/storage/` directory.
3. Connect to the command line on the Quantum Spark appliance.
4. If your default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```
5. Assign the 'execute' permission to the script:

   ```
   chmod +x /storage/doctor-smb.sh
   ```
6. Run the script:

   ```
   /storage/doctor-smb.sh
   ```
7. Run the Dr. Spark tool:

   ```
   drSMB diag <option>
   ```

   For the syntax, refer to *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances* > chapter "Working with Dr. Spark."

# Using System Tools

On the **Tools** page you can perform various actions to diagnose problems with the appliance.

The same **Tools** page is available in:

- The **Home** view > **Troubleshooting** section.
- The **Device** view > **System** section.
- The **Logs & Monitoring** view > **Diagnostics** section.

| Action | Available From | Description |
|---|---|---|
| **Monitor System Resources** | R81.10.00 | Opens a popup windows that shows:<br>- **CPU Usage History**<br>The information is refreshed automatically.<br>- **Memory Usage History**<br>Memory usage is calculated without memory that was allocated in advance to handle traffic and without cache memory.<br>This gives a more accurate picture of the actual memory usage in the appliance but it may differ from figures you receive from Linux tools.<br>The information is refreshed automatically.<br>- **Disk Usage**<br>Click the **Refresh** button for the most updated disk usage information.<br>Click the names of column to sort the output. |
| **Show Routing Table** | R81.10.00 | Opens a popup window that shows this information for each route:<br>- **Source**<br>- **Destination**<br>- **Service**<br>- **Gateway**<br>- **Metric**<br>- **Interface**<br>- **Origin** |

| Action | Available From | Description |
|---|---|---|
| **Show Router Configuration** | R81.10.05 | Opens a popup window where you select one of the categories, and the window shows the corresponding Gaia Clish commands:<br>- **BGP**<br>- **OSPF**<br>- **Inbound route filters**<br>- **Route redistribution** |
| **Run Command** | R81.10.10 | Opens a popup window in which you can select a predefined CLI command and see its output:<br>- **Policy status** (shows the status of different security policies)<br>- **Scan network** (shows the connected IoT devices)<br>- **Show diagnostics** (runs the Gaia Clish command "`show diag`").) |
| **Test Cloud Services Ports** | R81.10.00 | Opens a popup window that shows the result of the Cloud Services Connectivity Test<br>(the output of the Gaia Clish command "`test cloud-connectivity`"). |

| Action | Available From | Description |
|---|---|---|
| **Tcpdump Tool** | R81.10.00 | Opens a popup window, in which you can capture traffic that passes through appliance interfaces.<br>❗ **Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window. |

| Action | Available From | Description |
|---|---|---|
| | | |

| Action | Available From | Description |
|---|---|---|
| **Firewall Monitor Tool** | R81.10.10 | Opens a popup window, in which you can capture traffic that passes through appliance interfaces.<br>❗ **Warnings:**<br>■ When you use this tool, the CPU load increases. Schedule a maintenance window.<br>■ When you select the option "`-p all`", the CPU load increases significantly because this tool shows the information for each inspection chain module.<br>ℹ **Notes:**<br>■ The appliance runs the "`fw monitor`" command with the specified parameters. See the:<br>• *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances* > Chapter "Miscellaneous Commands" > Section "fw commands".<br>• *R81.10 CLI Reference Guide* > Chapter "Security Gateway Commands" > Section "fw" > Section "fw monitor".<br>■ Compared to the **Tcpdump Tool**:<br>• This tool shows how each packet passes through the Security Gateway inspection chain modules.<br>• This tool saves the captured traffic only in the plain-text format (filename is "`fw_monitor.log`").<br>■ You can view the captured traffic in real time or save it into a plain-text file.<br>■ When you start a new traffic capture and save it into a file, and a file with such name already exists, the appliance adds a running number to the default filename (this way, it does not overwrite an existing file).<br>■ The appliance captures traffic only on interfaces with a configured IP address.<br>■ The packet capture stops automatically if the WebUI session ends.<br>**Procedure:** |

| Action | Available From | Description |
|---|---|---|
| | | 1. Click the **Firewall Monitor Tool** button.<br>2. **Optional:** Configure the applicable filters:<br>a. In the **Monitor outgoing packets** field, enter how many outgoing packets to capture before the tool must stop the traffic capture.<br>b. In the **Monitor incoming packets** field, enter how many incoming packets to capture before the tool must stop the traffic capture.<br>c. Select "**-p all**" to see the information for each inspection chain module.<br>❗ **Warning** - The CPU load increases significantly.<br>d. Select "**grep**" to enter a free text filter.<br>▪ This field is case-sensitive.<br>▪ If the text must contains spaces, then you must enclose it in single quotes or double quotes.<br>▪ The tool captures the specified number of packets, and then filters the output to show only the relevant lines.<br>3. To save the captured traffic into a plain-text file:<br>Note - If you selected "**grep**", then the saved file contains only the relevant lines you see on the screen.<br>a. Click **Save** to download the file.<br>b. Your web browser saves this file (`fw_monitor.log`) in the default download folder. |

| Action | Available From | Description |
|---|---|---|
| **Firewall Ctl Tool** | R81.10.10 | Opens a popup window, in which you can see the kernel debug that shows which packets the Security Gateway drops.<br>**Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window.<br>**Notes:**<br>- The appliance runs the "`fw ctl zdebug -m fw + drop`" command. See the *R81.10 Quantum Security Gateway Guide* > Chapter "Kernel Debug".<br>- You can view the kernel debug output in real time or save it into a plain-text file.<br>- When you start a new kernel debug and save it into a file, and a file with such name already exists, the appliance adds a running number to the default filename (this way, it does not overwrite an existing file).<br>- The kernel debug stops automatically if the WebUI session ends.<br>**Procedure:**<br>1. Click the **Firewall Ctl Tool** button.<br>2. **Optional:** In the **Command timeout** field, enter the duration (in seconds) of the kernel debug.<br>3. **Optional:** In the "**grep**" field, enter the applicable filter:<br>- This field is case-sensitive.<br>- If the text must contains spaces, then you must enclose it in single quotes or double quotes.<br>- The tool captures the specified number of packets, and then filters the output to show only the relevant lines.<br>4. To save the kernel debug output into a plain-text file:<br>Note - If you entered a "**grep**" filter, then the saved file contains only the relevant lines you see on the screen.<br>a. Click **Save** to download the file. |

| Action | Available From | Description |
|---|---|---|
| | | b. Your web browser saves this file (`fw_ctl_zdebug_drop.log`) in the default download folder. |

| Action | Available From | Description |
|---|---|---|
| **VPN Debug Tool** | R81.10.10 | Opens a popup window, in which you can start a VPN debug.<br>❗ **Warning** - When you use this tool, the CPU load increases. Schedule a maintenance window.<br>ℹ **Notes:**<br>■ The appliance runs the "`fw ctl zdebug -m fw + drop`" command.<br>See the *R81.10 Quantum Security Gateway Guide* > Chapter "".<br>• *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances* > Chapter "Miscellaneous Commands" > Section "fw commands".<br>• *R81.10 CLI Reference Guide* > Chapter "Security Gateway Commands" > Section "fw" > Section "fw monitor".<br>■ You can view the kernel debug output in real time or save it into a plain-text file.<br>■ When you start a new kernel debug and save it into a file, the appliance adds a running number to the default filename (this way, it does not overwrite and existing debug file).<br>■ The kernel debug stops automatically if the WebUI session ends.<br>**Procedure:**<br>1. Click the **VPN Debug Tool** button.<br>2. Click the **Start Debugging** button.<br>3. Wait until you see the line "`VPN debugging in progress`".<br>4. Do **not** close this popup window (it will stop the VPN debug).<br>5. Replicate the VPN issue:<br>■ Remote Access VPN connection to this appliance.<br>■ Site to Site VPN connection to / from this appliance.<br>6. Click the **Stop Debugging** button.<br>7. Click **Download File** to download the archive with the required log files. |

| Action | Available From | Description |
|---|---|---|
| | | 8. Your web browser saves the archive file (`vpn_<YYYYMMDDHHMM>.tgz`) in the default download folder.<br>9. To have more information, also collect the CPinfo file - see the **Generate CPInfo File** below.<br>For the complete debug procedure, refer to sk62482. |
| **Display DSL Statistics** | R81.10.00 | Opens popup window that shows the DSL statistics.<br>Available only on DSL models. |
| **Generate CPInfo File** | R81.10.00 | Collects outputs of many commands and contents of various log files into an archive package.<br>This data helps Check Point Support understand the configuration and troubleshoot issues.<br>**Procedure:**<br>1. Click **Generate CPInfo File**.<br>A message next to the button shows the progress.<br>2. When the task completes, the button changes to **Download CPInfo File**.<br>3. Click **Download CPInfo File** to download the file.<br>4. Your web browser saves this file (`R81.10<Build>_<MMDDHHMM>.cpinfo.gz`) in the default download folder.<br>5. When the download completes, the button changes to **Generate CPInfo File**. |
| **Ping** | R81.10.00 | Opens a popup window that shows the result of the ping command to the specified IP address / hostname.<br>The appliance sends ICMP Requests to the specified destination. |
| **Trace** | R81.10.00 | Opens a popup window that shows the result of the traceroute command to the specified IP address / hostname.<br>The appliance sends ICMP Requests to the specified destination. |
| **Lookup** | R81.10.00 | Opens a popup window that shows the result of the DNS lookup for the specified IP address / hostname (the output of the Gaia Clish command "`nslookup`"). |

| Action | Available From | Description |
|---|---|---|
| **Download** | R81.10.00 | Opens sk159712 to download the Windows driver for a USB-C console socket.<br>**Explanation:**<br>When the mini-USB is used as a console connector, Windows OS does not automatically detect and download the driver needed for serial communication.<br>You must manually install the driver.<br>For more information, see sk182035. |

# SNMP

SNMP is a protocol for sending data and is used for monitoring. SNMP traps are alert messages sent as a result of monitoring conditions. SNMP trap receivers are configured to receive the alerts.

In the **Logs & Monitoring** > **SNMP** page you can do these actions:

- Turn the SNMP agent on or off
- Configure SNMP settings (system location, system contact, and community string for SNMP v1 and v2 authentication)
- Add SNMP v3 users
- Configure the settings for SNMP trap receivers
- Enable or disable SNMP traps that are sent to the trap receivers

SNMP must be set to **ON** to configure all SNMP settings (users, traps, and trap receivers).

### To enable or disable SNMP:

1. Change the **SNMP On/Off** slider position to **ON** or **OFF**.
2. Click **Apply**

### To configure SNMP settings:

Click **Configure**.

The **Configure SNMP General Settings** window opens. You can enable SNMP traps, configure system location and contact details, and enable SNMP versions in addition to v3.

### SNMP v3 Users

- To add a new SNMP v3 user, click **New**.
- To edit an existing SNMP v3 user, select the user from the list and click **Edit**.
- To delete an SNMP v3 user, select the user from the list and click **Delete**.

# SNMP Traps Receivers

SNMP trap receivers receive the alert messages. The trap receiver properties must be configured before a trap is sent.

**To add an SNMP trap receiver:**

1. Click **New**.
2. In the **Add SNMP Traps Receiver** window, enter the IP address.
3. For a **v2 trap receiver**, enter the community name.
4. For a **v3 trap receiver**, enter the name of the defined SNMP v3 user.

**To edit an existing SNMP trap receiver:**

Select the trap receiver from the list and click **Edit**.

**To delete an SNMP trap receiver:**

Select the trap receiver from the list and click **Delete**.

# SNMP Traps

You can enable or disable specified traps from the list and for some traps set a threshold value. The enabled traps are sent to the configured trap receivers.

**Prerequisites**: SNMP and SNMP traps must be enabled on the appliance.

## SNMP Traps for VPN Tunnels

SNMP trap for VPN tunnels provides better monitoring of VPN tunnel status. For this specific trap, users are alerted when VPN tunnels go down. Currently, only VPN tunnels configured as Permanent Tunnels are monitored.

This feature is **off** by default. When the feature is enabled, the VPN tunnels status is periodically checked. If a tunnel is detected as down, an SNMP trap is sent to the user.

## SNMP Traps for Hardware Sensors

SNMP traps for hardware sensors provide information on whether the sensor values are within their thresholds. Indicators are success or failure. These traps are on by default when SNMP traps are enabled and cannot be individually turned off or configured by the user.

### To enable an SNMP trap:

1. In the list of SNMP traps, double-click the name of the trap.

   The **SNMP Trap Configuration** window opens.

2. Click **Enabled**.

   The trap details, including the **monitored object**, **Trap OID** and **description**, show.

3. Click **Apply**

### To edit an SNMP trap:

1. Select the trap from the list and click **Edit**.
2. Select the **Enable trap** option to enable the trap or clear it to disable the trap.
3. If the trap contains a **value**, you can edit the threshold value when necessary.
4. Click **Apply**

# Advanced Configuration

This section contains information about advanced configuration, including upgrades and restoring factory defaults.

**Note** - Not all topics are relevant for all appliance models.

## Upgrade Using a USB Drive

This section explains how you can upgrade the appliance with a USB drive without a console connection to the appliance. For more information, see *"Upgrade Using Boot Loader" on page 527*.).

**Note** - A USB storage device used for clean installation of a new image on the 1500 series must be formatted with the FAT32 file-system.

### Installing a new firmware image from a USB drive

Check Point releases new firmware images every so often. You can install the new default image on the appliance using the image file and a USB drive. Note that you can also upgrade through the WebUI. If the new image supports it, you do not lose your previous settings. When you install the new default image using a USB drive, the appliance deletes your previous settings and creates a new factory default image.

#### To upgrade to a new firmware image from a USB drive:

1. Disconnect the Quantum Spark Appliance from the power source.
2. Place the firmware image file on a USB drive in the top folder. Do not rename the file.
3. Make sure the top folder of the USB drive does not contain any previous Boot loader or Firmware images (`u-boot*.bin` files, or `fw1*.img` files).
4. Connect the USB drive to the USB port on the Quantum Spark Appliance.
5. Connect the appliance to the power source. When the appliance is turned on, the Power LED on the front panel lights up in red for a short period.

   The LED then turns blue and starts to blink. This shows a boot is in progress and firmware is being installed.

   When the LED turns a solid blue, the appliance is ready for login.

   **Note** - The LED is red if there is an alert or error.

6. Remove the USB drive.
7. As this operation has removed your previous settings, refer to the *Quantum Spark Appliance Getting Started Guide* and reconfigure your appliance with the First Time Configuration Wizard.

**Notes:**

- When you upgrade with a USB drive, you also replace the saved factory defaults image of the appliance as this method installs the new default image on the appliance.
- Uboot update from a USB drive is currently not supported.

# Upgrade Using an SD Card

In the 1570 / 1590 appliances, you can use an SD card to upgrade to a new firmware image or auto-configuration file. When you install a new image with an SD card, the appliance deletes your previous settings and creates a new factory default image. Back up your settings so you can restore them after the installation is complete.

**Note** - The 1530 / 1550 appliance does not support SD cards.

**Note** - SD cards are formatted with `ext4`. In earlier versions, SD cards are formatted as FAT32. If you upgrade from an earlier version to R77.20.85 or higher, the SD remains with FAT32 for backward compatibility.

**To upgrade to a new firmware image from an SD card:**

1. Disconnect the Quantum Spark Appliance from the power source.
2. Place the firmware image on the SD card in the top folder. Do not rename the file.

   Make sure the top folder of the SD card does not contain any previous Boot loader or firmware images (`u-boot*.bin` files or `fwl*.gz` files).
3. Insert the SD card into the SD card slot on the Quantum Spark Appliance. If the operation does not succeed, this may be because the SD card slot does not recognize all devices.
4. Connect the appliance to the power source.

The installation begins with the image file. This takes several minutes.

If the file is valid, the Power LEDs start to blink blue to show progress.

When the installation is complete, the Power LED is solid blue. The appliance is ready for your input.

Restore your settings. For more information, see *"Backup, Restore, Upgrade, and Other System Operations" on page 156*.

**To upgrade using Gaia Clish commands:**

These are the file names that you can use:

- `autoconf.clish`
- `autoconf.`*`<MAC Address>`*`.clish`

*<MAC Address>* is the specified MAC address in this format: *XX-XX-XX-XX-XX*

You can create multiple configuration files for Quantum Spark Appliance gateways. The gateways run both files or only one of them. First the `autoconf.clish` configuration file is loaded. If there is a configuration file with the same MAC address as the gateway, that file is loaded second.

Use the **#** symbol to add comments to the configuration file.

# Boot Loader

If you are connected to the console port on the appliance and during the boot you press **CTRL+C**, the Gaia Embedded Boot Menu appears:

```
Welcome to Gaia Embedded Boot Menu:
1. Start in normal Mode
2. Start in debug Mode
3. Start in maintenance Mode
4. Restore to Factory Defaults (local)
5. Install/Update Image/Boot-Loader from Network
6. Restart Boot-Loader
7. Run Hardware diagnostics
8. Install DSL Firmware/Upload preset configuration file
Please enter your selection (press ENTER to finish):
```

When you are in Boot Loader, all interfaces are down and you can only activate them for options that require connectivity. At this point Check Point's services are not active.

| Boot Option | Description |
|---|---|
| `1. Start in normal Mode` | The default boot mode for the appliance.<br>**Note** - If there is an error and the appliance cannot boot properly in this boot mode, it reverts to the Maintenance mode and the Power LED turns a constant red. |
| `2. Start in debug Mode` | Boot mode that gives printouts of processes that are initialized during boot.<br>**Note** - If there is an error and the appliance cannot boot properly in this boot mode, it reverts to the Maintenance mode and the Power LED turns a constant red. |
| `3. Start in maintenance Mode` | Boot mode that gives access only to the file system (network interfaces, Check Point processes and the appliance's services are down). |
| `4. Restore to Factory Defaults (local)` | See *"Restoring Factory Defaults" on page 528*. |
| `5. Install/Update Image/Boot-Loader from Network` | See *"Upgrade Using Boot Loader" on page 527*. |

| Boot Option | Description |
|---|---|
| `6. Restart Boot-Loader` | Restarts the appliance. |
| `7. Run Hardware diagnostics` | Runs the hardware diagnostics on the appliance. |
| `8. Install DSL Firmware/Upload preset configuration file` | Uploads a preset configuration file. |

# Upgrade Using Boot Loader

**To upgrade the Quantum Spark Appliance using U-boot (boot loader):**

**Note** - In 1570 / 1590, Bootloader is supported only through the DMZ port and is not available through the LAN ports.

1. Connect to the console port on the appliance with (use the serial console connection on the back panel of the appliance).

2. Reboot the appliance.

3. During boot, when the applicable message appears, press **CTRL+C**.

   The Gaia Embedded Boot Menu appears:

   ```
   Welcome to Gaia Embedded Boot Menu:
   1. Start in normal Mode
   2. Start in debug Mode
   3. Start in maintenance Mode
   4. Restore to Factory Defaults (local)
   5. Install/Update Image/Boot-Loader from Network
   6. Restart Boot-Loader
   7. Run Hardware diagnostics
   8. Install DSL Firmware/Upload preset configuration file
   Please enter your selection (press ENTER to finish):
   ```

4. Press **5** to select the option **Install/Update Image/Boot-Loader from Network**.

5. You are asked if you want to load the image manually from a TFTP server, or if you want to use automatic mode with a BOOTP server.

6. If you select manual mode, you are asked to fill in the IP of the Quantum Spark Appliance, the IP of the TFTP server, and the image name.

7. If you select automatic mode, the procedure starts automatically to search for the BOOTP server.

8. While in the menu mode, press **CTRL+C** again to return to the Boot Loader menu.

   During the upgrade, the Power LED blinks blue to show progress. This takes up to a minute.

   When the upgrade is successfully completed, the Power LED is solid blue, and the appliance waits for you to press a key. Error in the upgrade process is indicated if the Power LED is red.

# Restoring Factory Defaults

The Quantum Spark Appliance contains a default factory image.

When the appliance is turned on for the first time, it loads with the default image.

As part of a troubleshooting process, you can restore the appliance to its factory default settings if necessary.

You can restore the appliance to the factory default image with the WebUI, Boot Loader, or a button on the back panel.

**Important** - When you restore factory defaults, you delete all information on the appliance and it is necessary to run the First Time Configuration Wizard.

**To restore factory defaults with the WebUI:**

1. In the Quantum Spark Appliance WebUI, click **Device** > **System Operations**. The System Operations pane opens.
2. In the Appliance section, click **Factory Defaults**.
3. In the pop-up window that opens, click **OK**.
4. While factory defaults are restored, the Power LED blinks blue to show progress.

   This takes some minutes. When this completes, the appliance reboots automatically.

**To restore factory defaults with the button on the back panel:**

1. Press the Factory Default button with a pin. Hold for at least 12 seconds.
2. When the Power LED is lit blue, release the button. The appliance reboots itself and starts to restore factory defaults immediately.
3. While factory defaults are restored, the Power LED blinks blue to show progress.

This takes some few minutes. When this completes, the appliance reboots automatically.

### To restore the Quantum Spark Appliance to its default factory configuration using U-boot (boot loader):

1. Connect to the console port on the appliance with (use the serial console connection on the back panel of the appliance).
2. Reboot the appliance.
3. During boot, when the applicable message appears, press **CTRL+C**.

   The Gaia Embedded Boot Menu appears:

   ```
   Welcome to Gaia Embedded Boot Menu:
   1. Start in normal Mode
   2. Start in debug Mode
   3. Start in maintenance Mode
   4. Restore to Factory Defaults (local)
   5. Install/Update Image/Boot-Loader from Network
   6. Restart Boot-Loader
   7. Run Hardware diagnostics
   8. Install DSL Firmware/Upload preset configuration file
   Please enter your selection (press ENTER to finish):
   ```

4. Enter **4** to select the option **Restore to Factory Defaults (local)**.
5. When the prompt appears "**Are you sure? (y/n)**", enter **y** to continue and restore the appliance to its factory defaults settings.

   While factory defaults are restored, the Power LED blinks blue to show progress. This takes up to a few minutes. When completed, the appliance boots automatically.

### To disable the reset to default:

Use this Gaia Clish command:

```
set additional-hw-settings reset-timeout 0
```

### To enable the reset to default:

Use this Gaia Clish command:

```
set additional-hw-settings reset-timeout 12
```

# Custom Default Image

As the default image is burned early in the lifecycle of the appliance, it sometimes becomes obsolete and lacks important security fixes or other updates. Therefore, you may want to replace it with a newer image.

If you select to install a custom default image, you can also preserve settings, policy, SIC, or the license as part of the default image.

**To update the default image:**

Run this Gaia Clish command:

```
update default-image from current-image preserve-settings yes
force yes
```

If you configure the value of "`preserve-settings`" to "`no`", you can only preserve the SIC and license.

If you configure the value of "`force`" to "`no`", the appliance asks you to confirm before it reboots.

For more information, see the *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

# SSH Authentication

Starting from R81.10.00, you can use RSA key authorization instead of password-based authentication when you log in over SSH.

**Warning** - This configuration does not survive a firmware upgrade.

## Procedure:

1. Create the RSA key and export its public key in the OpenSSH format.

- On the Check Point Gaia OS (or Gaia Embedded OS) use this command in the Expert mode:

   a. Run the applicable command:

   - **For versions earlier than R81.10.10 Build 3001**

     ```
     ssh-keygen -t rsa -b 4096
     ```

   - **For versions R81.10.10 Build 3001 and higher**

     ```
     ssh-keygen -t ecdsa -b 521
     ```

   **Notes:**
   - See https://linux.die.net/man/1/ssh-keygen
   - See https://www.ssh.com/academy/ssh/keygen
   - SSH-RSA is deprecated and is no longer supported in OpenSSH. We recommend that you use ECDSA or ED25519 (if your SSH client supports it)

   b. In this prompt, enter the required path and the file name for the RSA Private Key:

   ```
   Enter file in which to save the key
   (/home/admin/.ssh/id_rsa):
   ```

   **Note** - You can append several keys in this file.
   These keys are valid for all administrators configured on the Quantum Spark appliance.

   c. In this prompt, just press the Enter key:

   ```
   Enter passphrase (empty for no passphrase):
   ```

   d. In this prompt, just press the Enter key:

   ```
   Enter same passphrase again:
   ```

  Example from a Gaia OS server:

  **Note** - In this example, the "`/home/admin/MyKey`" file is the RSA Private Key, and the "`/home/admin/MyKey.pub`" file is the RSA Public Key.

```
[Expert@HostName:0]# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_
rsa): /home/admin/MyKey
Enter passphrase (empty for no passphrase): Press the
Enter Key
Enter same passphrase again: Press the Enter Key
Your identification has been saved in /home/admin/MyKey.
Your public key has been saved in /home/admin/MyKey.pub.
The key fingerprint is:
SHA256:iru...   ...   ...   ...   ...   ...bKrY
admin@HostName
The key's randomart image is:
+---[RSA 4096]----+
|B=*. ..          |
|.B =o...         |
|  *o=.  .        |
|   O.. .         |
|..* = . S        |
|...@ = *         |
| E= O * .        |
|    = * .        |
|  ..B..          |
+----[SHA256]-----+
[Expert@HostName:0]#
```

- On a Linux OS, you can use the "`openssl`" command or any other applicable tool.

  Do not configure a passphrase.

  **For versions earlier than R81.10.10 Build 3001:**

  ```
  openssl genrsa -out /var/log/MyKey.private 4096
  openssl rsa -in /var/log/MyKey.private -out
  /var/log/MyKey.public -outform PEM -pubout
  ```

  **For versions R81.10.10 Build 3001 and higher:**

  ```
  openssl ecparam -name secp521r1 -genkey -noout -out
  /var/log/MyKey.private
  openssl ec -in /var/log/MyKey.private -pubout >
  /var/log/MyKey.public
  ```

- On a Windows OS, you can use the "PuTTYgen" tool.

  Do not configure a passphrase.

  In the PuTTY built-in help, refer to the chapter "Using public keys for SSH authentication".

2. Transfer the file with the public key from the Linux-based server to your computer:

| Example | RSA Private Key | RSA Public Key |
|---|---|---|
| For Gaia OS | /home/admin/MyKey | /home/admin/MyKey.pub |
| For Linux OS | /var/log/MyKey.private | /var/log/MyKey.public |

3. Connect to the command line on the Quantum Spark Appliance.
4. Log in.
5. If the default shell is Gaia Clish, then go to the Expert mode:

```
expert
```

6. Create the required directory:

```
mkdir -v /storage/.ssh
```

7. Configure the required permissions on this directory:

```
chmod 700 /storage/.ssh
```

8. Transfer the file with the public key (in the above example for Gaia OS- "MyKey.pub") from your computer to the Quantum Spark Appliance to this directory:

```
/storage/.ssh
```

9. Rename the file with the public key to "authorized_keys":

```
mv -v /storage/MyKey.pub /storage/.ssh/authorized_keys
```

10. Edit file "/pfrm2.0/etc/sshd_config" file:

a. Back up the current file:

```
cp -v /pfrm2.0/etc/sshd_config{,_BKP}
```

b. Edit the current file:

```
vi /pfrm2.0/etc/sshd_config
```

c. Change this line:

```
AuthorizedKeysFile          none
```

to this line:

```
AuthorizedKeysFile          /storage/.ssh/authorized_keys
```

d. Save the changes in the file and exit the editor.

11. Reboot the Quantum Spark Appliance.

12. In your SSH client, configure the SSH session to use the RSA or ECDSA (depending on your version) Private Key file.

    Refer to the documentation for the SSH client.

    **Note** - For PuTTY, it is necessary to convert the Private Key file from the OpenSSH format to the PPK format:

    a. Start the `PuTTYgen` tool.
    b. From the top, click the **Conversions** menu.
    c. Click Import key.
    d. Select the Private Key file and click **Open**.
    e. In the bottom right corner, click **Save private key**.
       Do not configure a passphrase.

13. Connect with the SSH client (that uses the Private Key file) to the Quantum Spark Appliance.

    When prompted, enter the applicable username.

    There should not be a prompt for the password.

# Fonic Bypass

**Note** - This topic is only applicable for the 1595R Wired model.

The 1595R wired model has a FONIC (Fail Open Network Interface Card) bypass mechanism implemented between the DMZ and LAN4 ports.

The Bypass mechanism is automatically activated when one of these occurs:

- Power to the appliance is down.
- There is a critical software failure (using watchdog logic).

These are the two Bypass mechanism modes:

- **Active** - The connection between DMZ and LAN4 ports work as a normal system interface and drive data through the appliance, as long as the power is on and the software is valid. If the appliance power is off or the software has a critical problem that prevents it from maintaining a keep-alive mechanism, the Bypass circumvents the DMZ and LAN4 port connection and traffic bypasses the appliance.
- **Force-bypass** - "Bypass". The connection between the DMZ and LAN4 port is forcibly bypassed and the traffic bypasses the appliance regardless of the software status.

### To switch between Bypass-mechanism modes:

- Use Clish or WebUI (see below for details).

  Or

- Use the Bypass push button on the side of the 1595R appliance.

  In **Active** mode, pressing the button for more than 5 seconds switches the mode to Force-Bypass.

  In **Force-Bypass** mode pressing the button for more than 5 seconds, switches the mode to Active.

The Bypass LED indicates the current bypass status when power is on. When the LED is on, Bypass is activated. If the LED is off, Bypass is off.

**Note** - When using the button to switch modes, the status will not be saved in the configuration and the mode will switch back to the UI configured mode after a reset or power down.

**When the mode is set to Active**: After power is restored or after a reset, the appliance reboots and the system maintains the bypass between the DMZ/LAN4 ports until the Security Policy is activated. Once the Security Policy is activated, the system will set the Bypass to the mode configured by UI.

**When the mode is set to Bypass**: After power is restored or a hardware/software reset, the DMZ-LAN4 port connection is still bypassed until you reconfigure the mode and the software system is valid.

## Configuring Bypass mode in the WebUI

1. Go to **Device** > **Advanced Settings**.
2. In the search field, enter "fonic."
3. The **Fonic settings - Mode** attribute appears. Double-click the attribute name.
4. In the attribute window that opens, select or clear the checkbox to change the mode from **Active** to **Bypass** mode.
5. Click **Apply**.

## Configuring Bypass mode in Gaia Clish

### To display the current (Fonic) Bypass configured mode:

```
show fonic-settings advanced-settings
```

### To switch between Active and Bypass mode:

```
set fonic-settings advanced-settings mode
```

# RESTful API

## Enabling and disabling the REST API

**To enable REST API on the gateway, run this Gaia Clish command:**

```
set rest-api mode on
```

**To disable REST API on the gateway, run this Gaia Clish command:**

```
set rest-api mode off
```

## Request Structure

### HTTP Post

```
https://<gateway-ip>:<port>/web-api/<command>
```

The default port number is 4434.

### HTTP Headers

| Header | Description |
|---|---|
| `Content-Type` | application/json |
| `x-chkp-sid` | Session ID token as returned by the login command.<br>`The x-chkp-sid` header is mandatory in all API calls except the login API. |

### Request payload

Text in JSON format containing the different parameters.

Example:

```
https://192.168.1.1:4434/web-api/login
```

# Response Structure

Returned value on Success:

- HTTP status 200 (OK)
- A JSON string (content varies depending on which API is called)

Returned value on failure:

- HTTP status 500 (Internal Server Error), 400 (Bad Request), or 401 (Unauthorized)
- A JSON structure with the error details

# Versioning

HTTP Post with a specific version

```
https://<gateway-ip>:<port>/web-api/<version>/<command>
```

If no version is being sent, the latest supported version is used.

Example:

```
https://192.168.1.1:4434/web-api/v1/login
```

# REST API Commands

## (1) Login

### Description

1. Log in to the SMB appliance with your SMB admin username and password.
2. The SMB returns your session unique identifier.
3. Enter this session unique identifier in the `x-chkp-sid` header of each request.

### Request URL

```
POST https://<gateway-ip>:<port>/web-api/login
```

### Request Headers

| Header Name | Value | Description |
|---|---|---|
| `Content-Type` | application/json | Send JSON object to use the API Web Services. |

### Request Body

| Parameter Name | Value | Description |
|---|---|---|
| `user` (Required) | String | Administrator username |
| `Password` (Required) | String | Administrator password |

### Response

On Success, HTTP Return code: 200

| Header Name | Value | Description |
|---|---|---|
| `sid` | String | Session unique identifier for the `x-chkp-sid` header of each request. |
| `role` | String | The administrator role and permissions. |
| `read-only` | Boolean | True if the session is read only. |
| `api-server-version` | String | API server version. |
| `session-timeout` | Integer | Session expiration timeout in minutes. |

On Failure, HTTP Return code: 400, 401, 500

### Example Request

```
{
"user": "admin",
"password": "aa"
}
```

### Example Response

```
{
"sid": "9aa5770044797d7209f8ce9b0ef0fa0",
"role": "ROLE.SUPER",
"read-only": false,
"api-server-version": "v1",
"session-timeout": 10
}
```

## (2) Logout

### Description

Log out from the current session. After you log out, the session id is no longer valid.

### Request URL

```
POST https://<gateway-ip>:<port>/web-api/v1/logout
```

### Request Headers

| Header Name | Value | Description |
|---|---|---|
| `Content-Type` | application/json | Send JSON object to use the API Web Services. |
| `x-chkp-sid` | string token | Session unique identifier as the response to the login request. |

### Request Body

There is no request body.

### Response

On Success, HTTP Return code: 200

On Failure, HTTP Return code: 400, 401, 500

## (3) Generate-Report

### Description

Generate security report data according to the selected time frame:

`Hourly/Daily/Weekly/Monthly`

### Request URL

```
POST https://<gateway-ip>:<port>/web-api/generate-report
```

### Request Headers

| Header Name | Value | Description |
|---|---|---|
| `Content-Type` | application/json | Send JSON object to use the API Web Services. |
| `x-chkp-sid` | string token | Session unique identifier as the response to the login request. |

### Request Body

| Header Name | Value | Description |
|---|---|---|
| `type` (Required) | String | Report time frame.<br>Allow values: `{hourly, weekly, daily, monthly}` |

### Response

On Success, HTTP Return code: 200

| Header Name | Value | Description |
|---|---|---|
| `reportData` | Base64 string | Send data JSON in base64 format. |

On Failure, HTTP Return code: 400, 401, 500

### Example Request

```
{
"type": "daily",
}
```

### Example Response

```
[
{
"reportData": "<report_json_in_base64_format>"
}
]
```

## (4) Run-Clish-Command

### Description

Run a single Gaia Clish command.

### Request URL

```
POST https://<gateway-ip>:<port>/web-api/run-clish-command
```

### Request Headers

| Header Name | Value | Description |
|---|---|---|
| `Content-Type` | application/json | Send JSON object to use the API Web Services. |
| `x-chkp-sid` | string token | Session unique identifier as the response to the login request. |

### Request Body

| Header Name | Value | Description |
|---|---|---|
| `script` (Required) | String | A single clish command in base64 format. |

### Response

On Success, HTTP Return code: 200

| Header Name | Value | Description |
|---|---|---|
| `output` | String | Clish command output in base64 format. |

On Failure, HTTP Return code: 400, 401, 500

### Example Request

```
{
"script": " c2hvdyBwcm94eQ=="
}
```

### Example Response

```
{
"output":
"dXNlLXByb3h5OiAgICAgICAgICAgICAgICAgICAgdHJ1ZQpzZXJ2ZXI6IC
AgICAgICAgICAgICAgICAgICAgICAgICAxLjEuMS4xCnBvcnQ6ICAgICAgICAgICAgICAg
ICAgICAg
ICAgIDgwODAKCg=="
}
```

The script is:

```
show proxy
```

The output is:

```
use-proxy: true server: proxy.checkpoint.com port: 8080
```