QUANTUM

29 July 2025

WATCHTOWER

User 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 WatchTower User 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
29 July 2025	Added 2500 series to supported models
23 February 2025	Updated: ■ *"About WatchTower" on page 7*
25 October 2023	Updated list of supported appliance models
06 May 2021	Updated appliance models, rebranding to Quantum Spark appliances
19 January 2020	v1.52
27 October 2019	v1.51
12 September 2019	v1.50
10 July 2019	v1.30
20 June 2019	v1.27
16 May 2019	v1.26
30 April 2019	v1.25
4 April 2019	v1.21
19 March 2019	First release of this document v1.01

Table of Contents

About WatchTower

Enhance your Check Point network security with the ability to monitor your network and quickly mitigate security threats on the go with your mobile phone.

If you use the Quantum Spark 1500 gateways, download the Check Point Quantum Spark WatchTower app for your mobile device to manage your network security on the go.

The intuitive app provides real-time monitoring of network events, alerts you when your network is at risk, enables you to quickly block security threats, and configure the security policy for multiple Quantum Spark gateways.

Main features include:

- Network Security snapshot - view the devices connected to your network and any potential security threats.
- Security alerts - get real-time notification of malicious attacks or unauthorized device connections.
- On-the-spot threat mitigation – quickly block malware-infected devices and view infection details for further investigation.
- Security policy configuration – remote management of your security policy via WebUI.
- Customized push notifications - set top-priority security events.
- Prioritized event notifications – view all events or by category, drill down for more information.
- Simple management of multiple gateways - configure the security settings for multiple gateways.

Supported Quantum Spark appliance models:

- 1500 series
- 2500 series - 2530 / 2550, 2560 / 2570, 2580

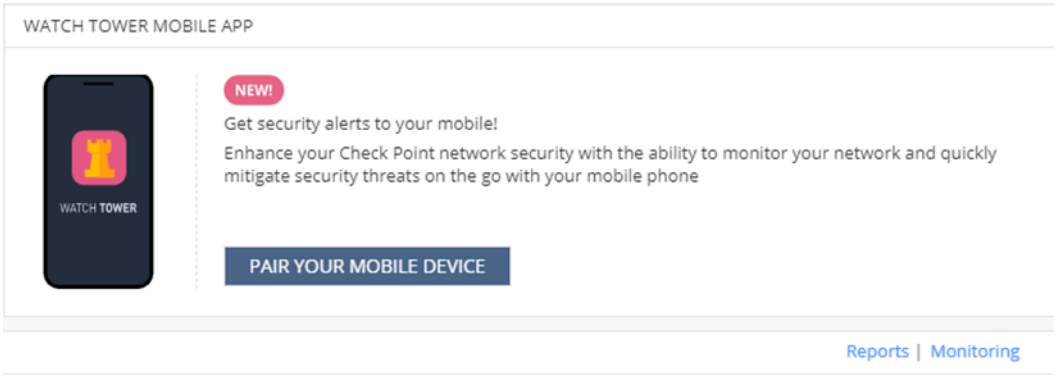
Important - The minimum supported firmware versions:

- Quantum Spark R82.00.X family - R82.00.00
- Quantum Spark R81.10.X family - R81.10.05 (see sk179615)
- Quantum Spark R80.20.X family - R80.20.00 (see sk165734)
- SMB R77.20.X family - R77.20.86 (see sk97766)

Introduction

Check Point WatchTower app lets you connect to your locally managed Security Gateway from your mobile device. You can receive notifications and react to real time events, review statistics and events, and access the Security Gateway WebUI.

Check Point WatchTower app is available in both Apple's AppStore and Google Play. Download and install the app on either an iOS or Android device.



Requirements

To use Check Point WatchTower, you must have a Locally Managed Quantum Spark Security Gateway deployed and configured.

Supported Quantum Spark appliance models:

- 1500 series
- 2500 series - 2530 / 2550, 2560 / 2570, 2580

Important - The minimum supported firmware versions:

- Quantum Spark R82.00.X family - R82.00.00
- Quantum Spark R81.10.X family - R81.10.05 (see sk179615)
- Quantum Spark R80.20.X family - R80.20.00 (see sk165734)
- SMB R77.20.X family - R77.20.86 (see sk97766)

Supported operating systems for the WatchTower app:

- iOS - version 9 and higher
- Android - version 6 and higher

Signing Up

A Check Point WatchTower account allows you to access, manage, and monitor multiple gateways from your mobile device with a single sign on.

When you open the app for the first time, you must create a WatchTower account in the Check Point cloud.

To create a Check Point WatchTower account:

1. From your mobile phone, access the WatchTower app and enter this information:
   - **Full name**.
   - **Email address**.
   - **Privacy** - Read and tap **I agree**.
   - **Terms of use** - When you sign up, you automatically agree to the terms of use.

     A window opens with the message that a confirmation mail was sent. and a field for the registration code.
2. In the field, enter the 6 digit registration code from the email.
3. Set your (complex) password.
4. Begin the process to add a Security Gateway.

Optional - Set up to log in with touchID or face recognition (either on the **Preferences** page or in the popup from the mobile OS).

The next time you log in to WatchTower, enter the password for your account.

If the sign up fails:

Verify that your mobile device is connected to the Internet and try again (might be a momentary disconnection).

Forgot My Password

To get a new password:

1. On the sign-in page, tap **Forgot your password?** at the bottom of the screen and follow the instructions.

   The reset-password page appears (waiting for confirmation).

2. A reset password message is sent to your email inbox. Copy the 6 digit registration code and enter it in the relevant field.

3. Enter a new password.

Pairing

Pairing is when you make a connection between the Security Gateway and your mobile device.

When you generate a pairing code in the Security Gateway WebUI, the Security Gateway automatically enables the **Reach My Device** feature in WebUI (**Device** view > **System** section > **DDNS and Device Access** page) and in Gaia Clish.

You can also enable and disable the **Reach My Gateway** service in WatchTower from the **Settings** page. If the **Reach My Gateway** service is disabled, the app can only connect locally to the Security Gateway (only from the Security Gateway's local/wireless network) and not through the Internet.

Pairing methodologies:

- Scan a QR code.
- Tap an invite link (opens the app) sent to your phone.
- Manual process.

Paring with a QR code

1. In the Security Gateway WebUI, go to the **Device** view > **System** section > **Administrators** page and click **Mobile Pairing Code**.

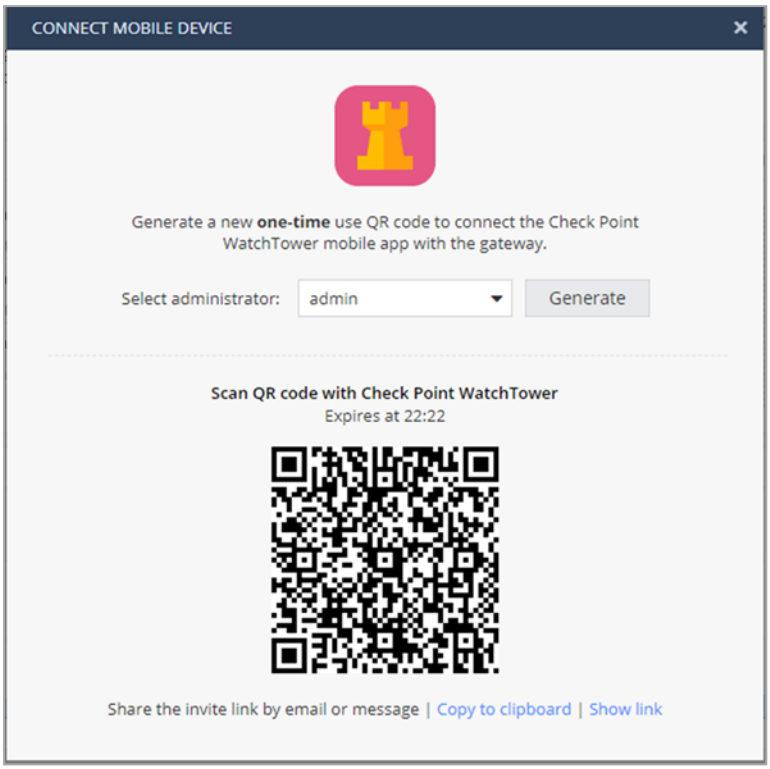
   Note - The **Pairing** button also appears on the **Overview** page.

2. This WebUI page generate and shows a QR code.
3. In WatchTower, tap **Add Gateway** and scan the QR code.

   You are redirected to the login page.

   Notes:
   - The QR code can only be used one time.
   - The QR code is temporary. The default time before expiration is 1 hour.

Example:



Paring with an Invite Link

1. In the Security Gateway WebUI, go to the **Device** view > **System** section > **Administrators** page and click **Mobile Pairing Code**.

   Note - The **Pairing** button also appears on the **Overview** page.

2. A QR code and the invite link are generated and displayed.

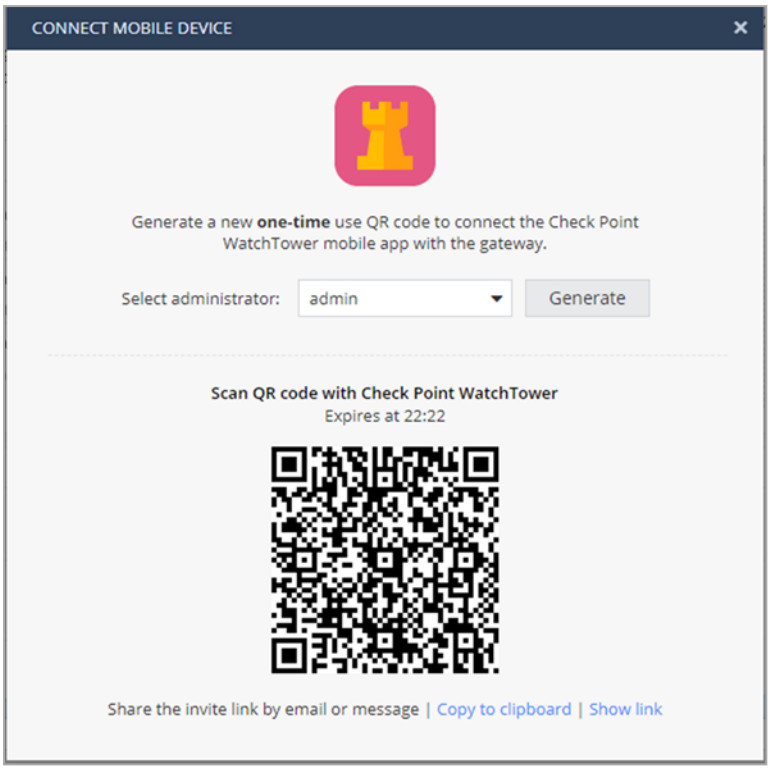
3. Click **Copy to clipboard**.

   You can now paste the link and send it to your mobile device.

   - If WatchTower is already installed, the link opens the Security Gateway login page. After you log in, the app is paired to the Security Gateway.
   - If WatchTower is not installed, you are redirected to the relevant App Store.

The invite link is temporary. The default time before expiration is 1 hour.

Example:



Manual Pairing

To allow pairing, your mobile device must be connected to the wireless network of the Security Gateway, or to an external wireless network that is connected to the LAN of the Security Gateway.

If you pair the Security Gateway and the app manually, you must configure these settings in the Security Gateway WebUI > **Device** view:

- In the **Network** section > on the **Wireless** page, configure a **Standard** wireless network.
- In the **System** section > on the **Administrator Access** page, in the **Select the sources from which to allow administrator access** section, select **Trusted Wireless**.

Alternatively, all you need is an external WiFi transmitter connected to the Security Gateway through a LAN port.

To manually pair your mobile device to the Security Gateway:

1. Open the WatchTower app.
2. Create a mobile account if you did not do so already.
3. On the **Connect to your Security Gateway** page, enter these credentials:
   - **Wireless** - The wireless network to which you are currently connected. To access a different wireless network, tap **Change**.
   - **Gateway IP address**. If you use a port other than the standard 4434, you must add the port to the IP address.

     For example: `192.168.1.1:<Port_Number>`
   - **Administrator Name**
   - **Password**
4. Tap **Connect**.

Troubleshooting

If the Security Gateway pairing fails:

1. Verify that your mobile device is connected to the Internet and try again (might be a momentary disconnection).

   You can also move to cellular (3G/4G) to evade the wireless if it is disconnected from the Internet.
2. Verify that this Security Gateway is not already connected to your app.
3. Generate a new QR code and try again (the temporary QR code may be expired).

   Note - If there is a problem in connectivity to the **Reach My Gateway** service, the QR code generation fails with a relevant message.

Reach My Gateway

When you generate a pairing code, the Quantum Spark Security Gateway automatically enables the **Reach My Device** feature in WebUI (**Device** view > **System** section > **DDNS and Device Access** page) and in Gaia Clish.

To access "Reach My Gateway" in WatchTower:

On the **Settings** page, tap the  icon.

To enable and disable the "Reach My Gateway" service:

Move the slider.

For manual pairing:

When you connect to the Security Gateway for the first time, you connect through wireless. All subsequent connections are through the Internet if **Reach My Gateway** is enabled.

If **Reach My Gateway** is disabled, the app continues to connect through local wireless only. This means you cannot access the Security Gateway from a different physical location.

Multiple Gateways

To pair a Security Gateway with an invite link:

1. Tap the invite link.
2. Enter the password for the Security Gateway.
3. Tap **Connect**.

To pair a Security Gateway with a QR code:

Note - The QR code can only be used one time. To add more than one Security Gateway at a time, you must generate a new QR code for each Security Gateway.

1. Tap the icon in the upper left corner of the screen.
2. In the window that opens, tap **All Gateways**.
3. Tap the **+** icon.
4. The QR scanner appears.
5. After the scan, enter the password for the Security Gateway.
6. Tap **Connect**.

To pair a Security Gateway manually:

In manual pairing, to add another Security Gateway, your mobile device must be connected to the wireless network of the Security Gateway.

1. Tap the icon in the upper left corner of the screen.
2. In the window that opens, tap **All Gateways**.
3. Tap the **+** icon.
4. The QR scanner appears (if camera permissions were granted to the app). Tap **Manual login**.
5. Verify you are connected to the wireless of the Security Gateway. Otherwise, tap **Change**.
6. Enter the **Gateway IP address**, **Port**, and other credentials including the admin password.
7. Tap **Connect**.

To delete a paired Security Gateway:

1. Tap **All Gateways**.
2. Tap the name of the Security Gateway you want to delete.
3. Tap the  icon at the top right corner of the screen.

   A menu opens.
4. Select **Delete**.

   You can also tap **Remove from list**. This removes the Security Gateway from the list of connected Security Gateways on the mobile app. The Security Gateway continues to send notifications to your mobile device until you delete the admin for that device in the Security Gateway WebUI.

If your Security Gateway is not connected:

On the **My Gateways** page, tap the Security Gateway name and then tap **Connect** under the Security Gateway icon.

These are your options:

- Connect to the Internet.
- Connect to your local network/WiFi.
- Remove the Security Gateway from the device list on the app.

  Note - You may still receive push notifications from the Security Gateway.
- Delete the Security Gateway.

If a Security Gateway is unreachable:

1. Verify that your Security Gateway is connected to the Internet.
2. On the **Settings** page, verify that the **Reach My Gateway** service is enabled.
3. Verify that the **Reach My Gateway** prefix was not changed since the pairing between the app and the Security Gateway (on the **Device** view > **System** section > **DDNS and Device Access** page).

Managing Protected Devices

WatchTower lets you manage the devices behind your Security Gateway. You can:

- Block a device.
- Edit a device's access to other internal networks and to the Internet.
- Show related events for a specific device.
- Assign contacts for a specific device - Save the contact information for the device owner. If you are notified about an event for that device, you can notify the contacts.

To see device information:

1. On the **Home** page, tap **Protected Devices**.

   The list of protected devices appears.

2. Select a specific device.

   The information screen for that device opens and displays:

   - Device name.
   - Device type.
   - Hardware.
   - IP address.
   - MAC address.
   - Interface.
   - Bandwidth and signal strength between the WiFi of the Security Gateway and the device (1500 appliances with R80.20 firmware and higher only).

If you received a notification of an infected device, you can block the infected device, but the admin must clean/remove the infection from the device.

To remove the infection icon from the device:

In the options menu, tap **I fixed it**.

Note - A device is marked as infected by its IP address. If that particular infected device is no longer connected to your network, after a while the original IP address is no longer reserved to it. In such a case, another device that connects to the Security Gateway may be assigned with this specific IP address and mistakenly be identified as an infected device.

To block a device:

1. Tap the device name.
2. Tap **Block Device**.

Note - A blocked device is only blocked from the specific network to the Internet and to other networks. If the device can connect through another network of that Security Gateway, it can still reach any device on the same network/switch and ping out to the Internet.

In the Security Gateway WebUI, you can manage your devices on the **Active Devices** page.

In WatchTower, go to **Home** > **Protected Devices** to see the list of devices that use the Security Gateway's network. You can filter by device type:

- All
- Office (desktop, laptop, printers)
- Mobile
- Other

To edit a device:

1. In the list of protected devices, select the device.

   The device details appear.
2. In the upper right corner of the screen, tap the  icon for options.
3. To modify the device information, tap **Edit**. You can:
   - Add a comment.
   - Change the device type or edit other information - Move the slider next to **Customized hardware details**.
4. Tap **Save**.

Note - A long press on the name of a protected device opens the options to edit, block/unblock etc

To copy device information to a clipboard:

When the device details are displayed, a long press on the field's content shows the option to edit or copy the information.

To show events for a specific device:

1. In the list of protected devices, select the device.

   The device details appear.

2. In the upper right corner of the screen, tap the  icon for options.

3. Tap **Show Device Events**.

   The **Events** page opens.

4. For an infected device, tap the **Show Events** link.

If you receive a permission error for actions in WatchTower:

Check your admin type on the Security Gateway and verify that you have the relevant permissions. For example, a read-only admin does not have permissions to execute any operation. A networking admin has permissions to execute networking related operations only.

To assign contacts for a device:

1. Open the device details page for the specific device.

2. Tap the  icon in the upper right corner of the screen.

3. Tap **Assign Contact**. If a contact is already assigned, it shows as **Change Contact**. You can also remove a contact assignment.

   A pop-up shows this message: **WatchTower would like to access your contacts**.

4. Tap **OK**.

5. Select the contact.

6. If the contact has multiple entries for phone number and email, select one for each and tap **OK**.

WatchTower Interface

This section describes the different screens of the WatchTower app and what you can do in each.

Home

The top portion of the **Home** page shows 3 clickable items:

- **Internet** (globe icon) - Shows external network with details and status of the Internet connection and VPN tunnels.
- **Gateway name** (Check Point Security Gateway icon) - Shows **Gateway details** including firmware, Security Gateway model and MAC address. You can also connect to the Security Gateway WebUI from this page.
- **Local network** (network icon) - Shows the internal network status with wireless and LAN details.

The lower portion of the **Home** page shows the number/amount of:

- **Security updates available** - Tap to open the **Security updates** page which shows the Software Blades and their status (up to date, update available, and **Update now**). It also shows when is the next daily update. In case of schedule update failure, a relevant error message is shown.
- **Protected Devices**
- **Malware Events** - During the past 7 days.
- **Traffic Scanned** - During the past 7 days.

Tap each one for more information.

Tap the tabs at the bottom of the page to access the **Events**, **Statistics**, and **Settings** pages.

Tap the  icon in the upper left hand corner of the screen to access the **Preferences**, Help and your list of Security Gateways.

Preferences

From the **Home** page, tap the  icon in the upper left corner of the screen and then tap the gear icon to access the **Preferences** page.

On the **Preferences** page, you can select the language for the WatchTower interface.

Note - Only English is supported for the input language.

The language for push notifications is set per Security Gateway, in the Security Gateway WebUI > **Home** view > **Monitoring** section > **Notifications** page.

You can also configure:

- **Login with biometric ID**. Move the slider to the right to enable login to WatchTower using fingerprint or face recognition.
- **Connect from anywhere**. Connect to the Security Gateway from the Internet or allow access in accordance with what was defined in the Security Gateway WebUI > **Device** view > **System** section > **Administrator Access** page. If this feature is disabled, WatchTower can only connect to the Security Gateway through the Security Gateway's local network.
- **Allowed idle time**. Select the maximum amount of idle time before the app locks. After this period, you must re-authenticate to continue using the app. The default is 5 minutes.
- **Number of events**. Define the number of events displayed in WatchTower. The default is 50 and can be increased up to 200.
- **Appearance**. Control the light/dark mode:
  - Light - Dark text on white/light background (default).
  - Dark - White text on dark background.
  - Automatic - According to the OS settings.

In addition, you can access the **Terms of use** and **Privacy policy** from this page.

To clear all account information:

Tap the  icon in the top right corner and tap **Reset Account**.

To logout:

Tap the  icon in the top right corner and tap **Logout**.

To return to the Home page:

- iOS users: Tap **Dismiss**.
- Android users: Press the back button.

Gateway Details

You can access this page from the **Home** or **Settings** pages.

This page shows the Security Gateway details, including:

- Firmware. You can also see what firmware is available and can schedule a firmware upgrade.
- Security Gateway model
- MAC address

Tap the ▪▪▪ icon in the upper right corner for more options, including:

- **Additional Gateway Settings...**
- **Schedule Upgrades**
- **Assign Contact...**
- **Share Gateway Pairing URL** - Tap to share a link to manage your Security Gateway by another admin or mobile device.
- **Reboot**
- **Help**

To assign owners or contacts for a Security Gateway:

1. On the **Gateway Details** page, tap the ▪▪▪ icon in the upper right corner of the screen.
2. Tap **Assign Contact...**. If a contact is already assigned, it shows as **Change Contact**. You can also remove a contact assignment.

   A pop-up shows this message: WatchTower would like to access your contacts.
3. Tap **OK**.
4. Select the contact.

If the contact has multiple entries for phone number and email, select one for each and tap **OK**.

Events

On the **Events** page, you can filter according to type:

- **All**
- **Security**
- **Attention**
- **Info**

Tap the event to see the **Event details**.

The events list displays the last 50 events by default. To change this, tap the  icon in the upper left corner and go to **Preferences** > **Number of events**.

Note - On the **Home** > **Protected Devices** page, you can select a specific device and see its related events.

To configure push notifications:

Go to **Settings** > **Notifications**.

Notes:

Notes:

- All events appear on the **Events** page, even if no push notifications are sent for that type of event.
- A reconnected device event is triggered when a device is connected after it was idle for more than a week. To change the default idle time, go to **Settings** > **Notifications**.
- An infected device event that was already handled still appears in the events list. If you open the event details, you see that the problem is fixed.

Statistics

The **Statistics** page shows the scanned traffic. You can filter for a specific time period:

- 1 hour
- 24 hours
- 7 days
- 30 days

Statistic Cards

- **Scanned Traffic** - How much traffic was scanned. Peaks are shown in orange. This card always appears, even if there is no data to present.
- **Scanned files/infected files** – How many files were scanned and how many were found to be infected.

  Infection details are not included in the card.

  This card does not appear if there is no data to present or if the Threat Emulation (SandBlast) blade is disabled.
- **Malware Events** - The total number of malware events that were detected and blocked by Anti-Bot and Anti-Virus, and the top, most common malware types that were found.

  The numbers to the left are the malware severity (1-5, with 5 as the highest severity).

  The malware links are to the **Check Point Research** site with information about this malware and remediation steps (if needed).

  This card always appears, even if there is no data to present.

  The **Malware Events** statistics card shows malware events, not compromised devices. Any malware events are blocked and handled by the Security Gateway. If there any compromised devices, a red panel appears in the **Home** tab and redirects to the list of compromised devices.
- **Attacks** - The total number of protections that were triggered by IPS (Intrusion Prevention System) and the top, most common protection types that were triggered.

  The numbers to the left are the protection severity (1-5, with 5 as the highest severity).

  The protection links are to the **Check Point Research** site with information about this protection.

  This card does not appear if there is no data to present or if the IPS blade is disabled.

- **Bandwidth usage of top used applications** - The pie chart at the top includes the traffic volume of only the top used applications. The portion of this traffic from the total scanned traffic (in percentage) is presented below the chart, followed by the list of the most used applications.

  This card does not appear if there is no data to present or if the Application Control blade is disabled.

- **Bandwidth usage of top users** - The pie chart at the top includes the traffic volume of only the top users. The portion of this traffic from the total scanned traffic (in percentages) is presented below the chart, followed by the list of the users who consume the most bandwidth.

  This card does not appear if there is no data to present or if the User Awareness blade is disabled.

On the **Home** tab > **Malware Events**, the top of the screen shows the report time frame settings.

The **Home** tab displays the **7 days** report data which is updated every four hours.

If you select the **1 Hour** or **24 Hours** time frame, you can see more recent events.

After you install or upgrade a Security Gateway, it takes time for the report data to be collected:

- **Hourly** - Up to 1 hour
- **Daily** - Up to 2 hours
- **Weekly** - Up to 4 hours
- **Monthly** - Up to 8 hours

Any existing data is deleted after an upgrade/install.

The statistics data displays what was collected since the last Security Gateway installation or upgrade. This means that the monthly and weekly reports may display data for a much shorter period of time, possibly even less than 1 day. Because their time frames are much shorter, the hourly and daily reports are not affected as much.

Reports

You can generate and share reports (in PDF format) of the statistics data for a specific time period.

To generate reports:

1. Tap the  icon in the upper right corner of the screen.
2. Tap **Generate Report**.

   Note - The report generation may take 20 to 30 seconds to complete. Tap **Run in background** to remove the loading page.

3. When the report is ready, a popup message appears. Tap **Open** to see the report.
4. To share, tap the  icon.

Settings

From **Settings**, you can access:

- **Notifications** (see *"Notifications" on page 32*)
- **Gateway Details** (see *"Gateway Details" on page 26*)
- **Administrators** (see *"Administrators" on page 33*)
- **Wireless Networks** (see *"Wireless Networks" on page 34*)
- **Local Network** (see *"Local Network" on page 35*)
- **Internet Connections** (see *"Internet Connections" on page 36*)
- **Reach My Gateway** - tap the icon (see *"Reach My Gateway" on page 16*)
- **VPN** (to Monitor VPN tunnel status)
- **Remote Access Users** (to monitor Remote Access VPN users)

To reboot the Security Gateway:

Note - You can also perform this action from the **Gateway Details** page.

1. Tap the icon in the upper right corner.
2. Tap **Reboot**.
3. Tap **Yes** to confirm.
4. Tap **OK**.

Notifications

On the **Notifications** page you can enable push notifications for:

- **Security Incidents** - Infected device detected, malicious file downloaded, malicious file blocked, malicious email received, malicious email blocked.
- **Networking Events** - New device, device reconnected, primary Internet restored, primary Internet down.
- **Operational Events** - New firmware available, license about to expire, license activated, license expired.

Options:

- On/off - Select to enable/disable push notifications.
- Shows previews.
- Language - Select the language for the notifications.

Administrators

You can access the **Administrators** page from the **Settings** tab.

The **Administrators** page shows the list of administrators.

To add an administrator:

1. Tap the ▪▪▪ icon.
2. Tap **Add administrator**.
3. Enter administrator details.
4. Tap **Done**.

To delete an administrator:

1. Do a long press on the specific administrator name.
2. Tap **Delete administrator**.

   Note - You cannot delete an admin who is currently logged in.

3. Tap **Done**.

To change the password for a specific administrator:

1. Tap the administrator name.

   Note - A long press on the name shows additional options.

2. Tap **Change password**.
3. Enter the new password.
4. Tap **Done**.

Wireless Networks

In **Wireless Networks**, you can edit the network settings or share the password for the network.

Tap the  icon in the upper right corner to:

- Add new WiFi.
- Change the radio settings.

When you see the WiFi details for a specific network, tap the  icon to:

- Disable Network.
- Edit Network.

  Note - One of the actions you can do here is copy the password to the clipboard.

- Change the password.
- Share the password.

Local Network

Shows the available local networks for example LAN, DMZ, etc. and all their details.

To disable/enable a network:

1. Tap the  icon in the upper right corner.
2. Tap **Disable/Enable Network**.

Internet Connections

From the **Home** tab, you can access the **Internet** page which shows the available Internet connections and their status (connected/disconnected and primary). Active connections have a green icon and disconnected ones show a red icon.

Tap the name to see the connection details:

- Connection type
- Interface name
- IP address
- Duration of the connection

To test the connection's upload/download speed and latency:

1. On the **Internet Connections** page, tap the  icon in the upper right corner.
2. Tap **Speed Test**.
3. The display shows the number of megabyes uploading/downloading per second.
4. Tap **Retry** to refresh the results.

You can monitor your device's Internet connection from your mobile device. You must first configure this on the Security Gateway WebUI **Home** view > **Overview** section > **System** page.

To configure connection monitoring:

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

   The **Edit Internet Connection** window opens.
2. In the **Connection Monitoring** tab, select or clear:
   - **Automatically detect loss of connectivity to the default gateway**. This pings the default Security 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.
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**.

To monitor your Internet connections from WatchTower:

1. Tap the connection name.

   The **Connection Details** page opens.

2. Tap **Probing servers** to see the list and details for:
   - Packet loss.
   - Failures
   - Min and Max Latency (seconds).
   - Jitter - Irregular time delay in the sending of data packets over a network.

Accessing the Security Gateway WebUI

To reach the Security Gateway WebUI:

1. In the **Settings** tab, tap the  icon in the top right corner.
2. In the menu that opens, tap **Additional Gateway Settings...**

You can also access the WebUI from the **Gateway Details** page:

Tap the  icon in the top right corner and select **Additional Gateway Settings...** from the drop-down menu.

FAQ

Managing Gateways

How can I switch between gateways?

1. Tap the icon at the top left corner and select a Security Gateway from the quick access list.

   Or

   Tap **All Gateways** to see the full list of your Security Gateways and select one. A details page opens.

2. Tap **Connect**.

How do I delete a gateway?

1. Tap the icon at the top left corner and tap All Gateways to see the full list of your Security Gateways.
2. Select the Security Gateway. The details page opens.
3. Tap the icon at the top right corner). An action menu opens.
4. Tap **Delete Gateway**.

   Note - When you tap **Delete Gateway**, the Security Gateway is removed. If you tap **Remove from List**, the Security Gateway is removed from the list of connected Security Gateways on the mobile app, but continues to send notifications until you go to the Security Gateway WebUI and delete the admin for that device.

How do I add a gateway?

See *"Multiple Gateways" on page 17*.

Security Gateway paring failed.

Do *one* of these procedures: (from simplest to more advanced):

1. Verify that your mobile device is connected to the Internet and try again (might be a momentary disconnection). You can also move to cellular (3G/4G) if there is a problem with your WiFi.
2. Verify that this Security Gateway is not already connected to your app.
3. Generate a new QR code and try again (The QR code can be used only once, or the temporary QR code validity may be expired).

Notes:

- If there is a problem in connectivity to the **Reach My Device** service, the QR generation process fails with a relevant message.
- The manual pairing procedure works only with the standard WebUI port (TCP 4434). Verify that this was not changed on your Security Gateway.

I upgraded/installed my gateway and all the statistics tabs are empty or not displayed. The Home tab statistic panels also do not display anything.

After you install or upgrade a Security Gateway, it takes time for the report data to be collected:

- Hourly – Up to 1 hour
- Daily – Up to two hours
- Weekly – Up to 4 hours
- Monthly – Up to 8 hours

Any existing statistics data is deleted after an upgrade/install.

I connected locally to my gateway (either manual pairing or connect locally anytime later) and a warning page appeared, asking me whether to trust the site or not… what do I do?

In this case, the Security Gateway does not have a formal signed certificate but a self signed one. Therefore, to verify that you are connecting to your specific Security Gateway, the app displays its certificate's fingerprint.

Compare this fingerprint with your Security Gateway's internal certificate's fingerprint to verify that you connected to your Security Gateway.

If verified, tap **Trust** to continue. If not, tap **Cancel** to stop the process.

While working with the app, a warning about an untrusted-site page suddenly appeared. What is this?

The application communicates securely with predefined trusted domains. If the certificate is not exactly the one the app expects, it handles it as if there is a security breach and blocks the connection. Note that even if the received certificate is valid, if it does not match exactly, the site is blocked.

I added a gateway using manual pairing and I cannot connect to it from the Internet, only locally from the wireless.

In the **Settings** page, check the **Reach My Gateway** service. If the **Reach My Gateway** is disabled, you cannot connect to the Security Gateway. **Reach My Gateway** is automatically activated if you use the QR code method for pairing.

I can't connect locally (through local wireless) to the gateway.

Verify these conditions:

1. You are connected to the Security Gateway's wireless network.
2. The Security Gateway IP address is correct.
3. If the Security Gateway's WebUI uses the standard port (TCP 4434).

   If not, you must add the port number in the URL:

   <*Gateway-IP-Address*>:<*Port*>

Security Gateway unreachable.

Verify that the **Reach My Device** service is reachable from your Security Gateway and test it by generating a pairing QR code.

1. Verify that your Security Gateway is connected to the Internet.

   Note - If there is a problem in connectivity to the **Reach My Device** service, the QR generation process fails with a relevant message.

2. Verify that the **Reach My Device** prefix was not changed since the pairing between the app and the Security Gateway (on the **Device** view > **System** section > **DDNS and Device Access** page).
3. If the WebUI port was changed after Security Gateway pairing, reboot the Security Gateway for WatchTower to reconnect.

I need to configure my gateway every time I enter the application.

This occurred occasionally in earlier versions of WatchTower (prior to v1.25). If you still experience this problem, delete and re-install WatchTower.

Managing Devices

When do you block a device?

If you receive notification of an infected device (appears on your mobile with a special icon), or if a new unknown device detected, you can block them.

Note - If there is an infection, you must take action to clean the device. The Security Gateway cannot clean the device, only block the device from the network to avoid spreading the infection.

After you clean the device, tap **I fixed it**. This automatically unblocks the device.

How do I get more information about an infected device?

If there is an infected device, a red banner appears at the top of the **Home** tab.

When you tap this banner, a list of the infected devices opens and includes:

- Device details
- Infection details

You can also access the same information from the **Events** tab.

I was notified that a new device was detected. How do I get more information?

The device details are shown in the **Events** page.

After the Security Gateway learns more information about this device, more details are available.

I blocked a device but it can still ping.

A blocked device is only blocked from the specific network to the Internet and other networks. If the device can connect through another network of the Security Gateway, it can still reach any device on the same network/switch and ping out to the Internet.

I blocked a device but it re-connected through another network.

A blocked device is blocked only from the specific network. It can still connect to other networks on the Security Gateway.

A device connected to my network and is suddenly displayed as infected, but it is not.

A device is marked as infected by its IP address. If that particular infected device is no longer connected to your network, after a while the original IP address is no longer reserved to it. In such a case, another device that connects to the Security Gateway may be assigned with this specific IP address and mistakenly be identified as an infected device. To remove the mistaken infection label, tap **I Fixed It**.

I don't see any device-reconnected events.

A reconnected device event is triggered when a device is connected after it was idle for over a week (default). You can configure the reconnected device settings in **Settings** > **Notifications** > **Device reconnected**.

Events and Push Notifications

I received a notification of an infected device. What do I do now?

You can block the infected device, but the admin must clean/remove the infection from the device.

To remove the infection icon from the device, in the options, tap **I fixed it**.

I was notified a malicious file was blocked. How do I get more information?

On the **Events** page, you can see the device and infection details.

I received an infected file notification but the malware events in the Home tab displays 0 malware events.

On the **Home** tab, tap **Malware Events**. The top of the screen shows the report time frame settings. The **Home** tab displays the **7 Days** report data which is updated every four hours. If you select the **1 Hour**, or **24 Hours** time frames, you can see more recent events.

I received an event notification a while ago and now I can't find it.

The events list is limited to the last 50 events

To change this limit:

1. Tap the  icon at the top left of the screen and tap **Preferences** > **Number of events**.
2. Increase the limit (up to 200 events).

I have several malware events. Does this mean my devices are compromised?

The **Malware Events** statistics card shows malware events, not compromised devices. Any malware events were probably blocked and handled by the Security Gateway.

If there are any compromised devices, a red panel appears in the **Home** tab and redirects to the list of compromised devices.

In the last 30 days report, I see smaller numbers than what I expected.

The **Statistics** data displays what was collected since the last Security Gateway installation or upgrade. This means the monthly and weekly reports may display data for a much shorter period of time, possibly (even less than 1 day). Because their time frames are much shorter, the hourly and daily reports are not affected as much.

I get push notifications in English even though my app is localized to a non-English language.

The push notifications are sent from the Security Gateway. You must set your preferred language in the in the Security Gateway WebUI > **Home** view > **Monitoring** section > **Notifications** page.

Miscellaneous

I forgot my password. How do I recover it, or get a new one?

See *"Forgot My Password" on page 11*.

Sign up failed.

Verify that your mobile device is connected to the Internet and try again (might be a momentary disconnection).

My app locks every time it's in the background on my phone. What can I do to prevent this?

On the **Preferences** page, you can select the maximum amount of idle time before the app locks, ranging from 15 minutes to 1 day (24 hours). The default is 30 minutes.

I received a permission error message for actions in the App.

Check your administration type on the Security Gateway and verify that you have the relevant permissions.

- Read-only admin - Does not have permissions to execute any operation.
- Networking admin - Has permissions to execute networking operations only.

I want to configure more security and network settings but they are not included in the app.

You must configure these in the Security Gateway WebUI:

1. Go to the **Settings** tab and tap the  icon (top-right of the screen).
2. Select **Gateway Web Interface**.
3. Enter the Security Gateway credentials.
4. The WebUI opens.
5. Configure your security and network settings.

I want to connect to another account, but the email cannot be changed.

WatchTower supports only one user account per installation. To connect or create a new account, you must reset the account or remove the app and reinstall it.

How can I share statistics data?

See *"Statistics" on page 28* > "To generate a report."